Rational points on varieties

Bjorn Poonen

Department of Mathematics, Massachusetts Institute of Technology, Cambridge, MA 02139-4307, USA

E-mail address: poonen@math.mit.edu

URL: http://math.mit.edu/~poonen/
2010 Mathematics Subject Classification. Primary 14G05; Secondary 11G35

Key words and phrases. Rational points, descent, étale cohomology, torsors, Brauer–Manin obstruction, descent obstruction
## Contents

### Preface

0.1. Prerequisites

0.2. What kind of book this is

0.3. The nominal goal

0.4. The true goal

0.5. The content

0.6. Anything new in this book?

0.7. Standard notation

0.8. Acknowledgements

### Chapter 1. Fields

1.1. Some fields arising in classical number theory

1.2. \( C_r \) fields

1.3. Galois theory

1.4. Cohomological dimension

1.5. Brauer groups of fields

Exercises

### Chapter 2. Varieties over arbitrary fields

2.1. Varieties

2.2. Base extension

2.3. Scheme-valued points

2.4. Closed points

2.5. Curves

2.6. Rational points over special fields

Exercises

### Chapter 3. Properties of morphisms

3.1. Finiteness conditions

3.2. Spreading out

3.3. Flat morphisms

3.4. Fppf and fpqc morphisms

### Chapter 4. Arithmetic schemes

4.1. Arithmetic schemes

4.2. Elliptic curves

4.3. Modular curves

4.4. Schemes over discrete valuation rings

4.5. Nonsingular projective varieties

4.6. Approximation theorems

Exercises

### Chapter 5. Local fields

5.1. \( p \)-adic fields

5.2. \( Z_p \) and \( Q_p \)

5.3. Local field duality

5.4. Completion

5.5. The Hasse-Weil theorem

Exercises
Preface

0.1. Prerequisites

A person interested in reading this book should have the following background:

- Algebraic geometry (e.g., Har77: up to Chapter II, §8 as a minimum, but familiarity with later chapters is also needed at times) — this is not needed so much in our Chapter I;
- Algebraic number theory (e.g., Cas67, Frö67 or Lan94, Part One or Neu99, Chapters I and II).
- Some group cohomology (e.g., AW67 or Mil13, Chapter 2).

0.2. What kind of book this is

The literature on rational points is vast. To write a book on the subject, an author must choose one of the following:

1. write thousands of pages to cover all the topics comprehensively,
2. focus on one aspect of the subject, or
3. write an extended survey serving as an introduction to many topics, with pointers to the literature for those who want to learn more about any particular one.

Our approach is closest to 3, so as to bring newcomers quickly up to speed while also providing more experienced researchers with directions for further exploration.

This book originated as the lecture notes for a semester-long course, taught during spring 2003 at the University of California, Berkeley, and fall 2008 and fall 2013 at the Massachusetts Institute of Technology. But it has grown since then; probably now it is about 50% too large for a single semester, unless students are willing to read much of it outside of class.

0.3. The nominal goal

Many techniques have been used to decide whether a variety over a number field has a rational point. Some generalize Fermat’s method of infinite descent, some use quadratic reciprocity, and others appear at first sight to be ad hoc. But over the past few decades, it was discovered that nearly all of these techniques could be understood as applications of just two cohomological obstructions, the étale-Brauer obstruction and the descent obstruction. Moreover, while this book was being written, it was proved that the étale-Brauer obstruction
and the descent obstruction are equivalent! The topics in this book build up to an explanation of this “grand unified theory” of obstructions.

0.4. The true goal

Our ulterior motive, however, is to introduce readers to techniques that they are likely to need while researching arithmetic geometry more broadly. Along the way, we mention open problems and applications that are interesting in their own right.

0.5. The content

Chapter 1 introduces fields of special interest to arithmetic geometers, and discusses properties and invariants (the $C_r$ property, cohomological dimension, and the Brauer group) that control the answers to some arithmetic questions about fields in general. Not all of Chapter 1 is needed in future chapters, but the Brauer group plays a key role later on (in Chapters 6 and 8).

Chapter 2 discusses aspects of varieties with particular attention to the case of ground fields that are not algebraically closed. Ultimately we aim to treat global fields of positive characteristic as well as number fields, so we do not require our ground field to be perfect. Among other topics, this chapter discusses properties of varieties under base extension (e.g., irreducible vs. geometrically irreducible), the functor of points of a scheme, closed points and their relation to field-valued points, and genus change of curves under field extension. A final section introduces the main questions about rational points that motivate the subject, such as the questions of whether the local-global principle and weak approximation hold.

Chapter 3 begins with morphisms of finite presentation in order to discuss spreading out (e.g., extending a variety over a number field $k$ to a scheme over a ring of $S$-integers in $k$). But the heart of the chapter is an extended introduction to smooth and étale morphisms, going beyond the treatment in [Har77, III.10]. This, together with a section on flat morphisms, provides the basis for the definitions of the Grothendieck topologies commonly used for cohomology theories (see Chapter 6). The chapter includes also sections on rational maps and Frobenius morphisms: the latter are used to understand the Weil conjectures in Chapter 7.

The word “descent” has two unrelated meanings in arithmetic geometry. One meaning is as in Fermat’s method of infinite descent and its generalizations, in which it is the height of rational points that descends in the course of a proof. The second meaning is that of descent of the ground field: the problem here is to decide whether a variety over a field extension $L \supseteq k$ arises as the base extension of a variety $X$ over $k$ (and to describe all possibilities for $X$). Chapter 4 studies this problem and its analogue for morphisms, and its generalizations to schemes. It also gives applications to the classification of twists of geometric objects (different $k$-forms of the same object over a field extension $L$), and to restriction of scalars, which transforms varieties over a field extension $L \supseteq k$ into varieties over $k$. 

vi
Chapter 5 is a survey on group schemes and algebraic groups over fields. After discussing their general properties, it defines special types of algebraic groups, and states the classification theorem that decomposes arbitrary smooth algebraic groups into those types. The final section of Chapter 5 introduces torsors, which are needed to define the descent obstruction in Chapter 8. For algebraic groups over global fields, we discuss weak and strong approximation (Section 5.10) and the local-global principle for their torsors (Section 5.12.8).

Chapter 6 is an introduction to étale cohomology and its variants such as fppf cohomology. These cohomology theories are applied to generalize from torsors of algebraic groups over a field to torsors of group schemes over an arbitrary base scheme, and we prove finiteness results for torsors over a global field that are unramified at all but finitely many places. Another application is to generalize the cohomological definition of the Brauer group of a field to Grothendieck’s definition of the cohomological Brauer group of a scheme; we end by discussing tools for computing these Brauer groups (the Hochschild–Serre spectral sequence, and residue homomorphisms) and give many examples since these will be needed to understand the Brauer–Manin obstruction in Section 8.2.

Although not needed for the main story of obstructions to rational points, we include in Chapter 7 the motivating application of étale cohomology, namely the Weil conjectures on varieties over finite fields. There we also discuss related issues, such as the étale cohomology classes of algebraic cycles and the Tate conjecture.

Chapter 8 defines the cohomological obstructions to the local-global principle and weak approximation for a variety $X$ over a global field; these are expressed as subsets of the set $X(\mathbb{A})$ of adelic points that constrain where $k$-points may lie. First is the Brauer–Manin obstruction, coming from elements of the Brauer group of $X$. Next is the descent obstruction coming from torsors of algebraic groups; this is motivated by an example of a genus 2 curve in which the algebraic group is simply a finite group. Next we define hybrids of these two obstructions, and compare their strengths for constraining $k$-points. Finally, we explain why all these obstructions are still not enough to decide whether a variety has a $k$-point.

Chapter 9 is a survey of the geometry and arithmetic of higher-dimensional varieties, with special attention paid to surfaces. It begins with the crude classification given by Kodaira dimension, and compares the properties of being rational, unirational, rationally connected, and so on. Next we give the classification of surfaces over an arbitrary ground field, and discuss the arithmetic of del Pezzo surfaces in some detail since these serve as excellent examples for the techniques presented earlier in the book. We end by discussing very briefly what is proved and conjectured for curves of genus $>1$ and more generally for varieties of general type; the reasons for not exploring this in greater detail are first, that it would require a few more hundred pages to develop the required theory of height functions and diophantine approximation, and second, that several books on these topics exist already (we cite some of them).
A few appendices serve various purposes. Appendix A discusses some set theory that is implicitly used when discussing sheafification, for instance. Appendix B defines certain interesting classes of fields that did not make it into Chapter 1. Appendix C contains reference tables with lists of adjectives that can be applied to morphisms, varieties, or algebraic groups; the tables indicate where to find definitions, and propositions about their preservation under base extension, descent, and so on.

0.6. Anything new in this book?

Almost all of the theorems in this book existed previously in the published literature in some form, but in many places we have tried to make proofs more readable and to organize topics so as to form a coherent exposition. There are a few new results: for example, the finiteness of Selmer sets (see Theorems 6.5.13 and 8.4.6) and Minchev’s theorem on the failure of strong approximation (Corollary 8.4.11) were previously known only over number fields, whereas we generalize them to all global fields; these generalizations require extra arguments in the function field case because of the failure of Hermite’s finiteness theorem on extensions of bounded degree unramified outside a fixed set of places. A few smaller innovations include an improved proof of Theorem 9.3.1(b)(ii) stating that proper birational morphisms between smooth surfaces factor into blow-ups at separable points, the use of the Lang–Nishimura theorem to avoid general position arguments in the proof of Lemma 9.4.18 on degree 6 del Pezzo surfaces, and the k-rationality of degree 5 del Pezzo surfaces over even the smallest of finite fields (Theorem 9.4.29).

The book whose content overlaps the most with ours is probably Sko01. That book, written by a leading expert, also discusses torsors and the Brauer–Manin and descent obstructions. Our book can serve as preparation for reading that one, since ours includes more background material (on algebraic groups, on étale and fppf cohomology, etc.), while Sko01 goes further in other directions, proving theorems on the Brauer–Manin obstruction for conic bundle surfaces and for homogeneous spaces of simply connected algebraic groups, for instance.
0.7. Standard notation

Following Bourbaki, define

\[ \mathbb{N} := \text{the set of natural numbers} = \{0, 1, 2, \ldots\} \]
\[ \mathbb{Z} := \text{the ring of integers} = \{\ldots, -2, -1, 0, 1, 2, \ldots\} \]
\[ \mathbb{Q} := \text{the field of rational numbers} = \left\{ \frac{m}{n} : m, n \in \mathbb{Z}, n \neq 0 \right\} \]
\[ \mathbb{R} := \text{the field of real numbers} \]
\[ \mathbb{C} := \text{the field of complex numbers} = \{a + bi : a, b \in \mathbb{R}\}, \text{where } i = \sqrt{-1} \]
\[ \mathbb{F}_q := \text{the finite field of } q \text{ elements} \]
\[ \mathbb{Z}_p := \text{the ring of } p\text{-adic integers} = \varprojlim \mathbb{Z}/p^n\mathbb{Z} \]
\[ \mathbb{Q}_p := \text{the field of } p\text{-adic numbers} = \text{the fraction field of } \mathbb{Z}_p. \]

The cardinality of a set \( S \) is denoted \#\( S \) or sometimes \( |S| \). If \((A_i)_{i \in I}\) is a collection of sets, and for all but finitely many \( i \in I \) a subset \( B_i \subseteq A_i \) is specified, then the restricted product \( \prod'_{i \in I} (A_i, B_i) \) is the set of \((a_i) \in \prod_{i \in I} A_i\) such that \( a_i \in B_i \) for all but finitely many \( i \) (with no condition being placed at the \( i \) for which \( B_i \) is undefined).

If \( a, b \in \mathbb{Z} \), then \( a \mid b \) means that \( a \) divides \( b \), that is, that there exists \( k \in \mathbb{Z} \) such that \( b = ka \). Similarly, \( a \nmid b \) means that \( a \) does not divide \( b \). Define \( \mathbb{Z}_{\geq 1} := \{n \in \mathbb{Z} : n \geq 1\} \) and so on.

Rings are associative and have a 1 by definition \cite{Poole}. Suppose that \( R \) is a ring. Let \( R^\times \) denote the unit group of \( R \). Let \( R[t_1, \ldots, t_n] \) denote the ring of polynomials in \( t_1, \ldots, t_n \) with coefficients in \( R \). Let \( R[[t_1, \ldots, t_n]] \) denote the ring of formal power series in \( t_1, \ldots, t_n \) with coefficients in \( R \). The ring \( R((t)) := R[[t]][t^{-1}] \) is called the ring of formal Laurent series in \( t \) with coefficients in \( R \); its elements can be written as formal sums \( \sum_{n \in \mathbb{Z}} a_n t^n \) where \( a_n \in R \) for all \( n \) and \( a_n = 0 \) for sufficiently negative \( n \). If \( R \) is an integral domain, then \( \text{Frac } R \) denotes its fraction field.

Suppose that \( k \) is a field. The characteristic of \( k \) is denoted \( \text{char } k \). The rational function field \( k(t_1, \ldots, t_n) \) is \( \text{Frac } k[t_1, \ldots, t_n] \). The ring \( k((t)) \) defined above is a field, isomorphic to \( \text{Frac } k[[t]] \). Given an extension of fields \( \mathbb{L}/k \), a transcendence basis for \( \mathbb{L}/k \) is a subset \( S \subseteq L \) such that \( S \) is algebraically independent over \( k \) and \( L \) is algebraic over \( k(S) \); such an \( S \) always exists, and \#\( S \) is determined by \( \mathbb{L}/k \) and is called the transcendence degree \( \text{tr deg}(\mathbb{L}/k) \).

Suppose that \( R \) is a ring and \( n \in \mathbb{Z}_{\geq 0} \). Then \( M_n(R) \) denotes the \( R \)-algebra of \( n \times n \) matrices with coefficients in \( R \), and we define the group \( \text{GL}_n(R) := M_n(R)^\times \). If \( R \) is commutative, a matrix \( A \in M_n(R) \) belongs to \( \text{GL}_n(R) \) if and only if its determinant \( \det(A) \) is in \( R^\times \).

If \( \mathcal{A} \) is a category, then \( \mathcal{A}^{\text{opp}} \) denotes the opposite category, with the same objects but with morphisms reversed. We can avoid dealing with an anti-equivalence of categories \( \mathcal{A} \to \mathcal{B} \)
by rewriting it as an equivalence of categories $A^{opp} \to B$. Let $\text{Sets}$ be the category whose objects are sets and whose morphisms are functions. Let $\text{Groups}$ denote the category of groups in which the morphisms are the homomorphisms. Let $\text{Ab}$ denote the category of abelian groups; this is a full subcategory of $\text{Groups}$: “full” means that for $A, B \in \text{Ab}$, the definition of $\text{Hom}(A, B)$ in $\text{Ab}$ agrees with the definition of $\text{Hom}(A, B)$ in $\text{Groups}$. We work in a fixed universe so that the objects in each category form a set (instead of a class): see Appendix A. From now on, we will usually not mention the universe.

0.8. Acknowledgements

I thank Dan Abramovich, Roman Bezrukavnikov, Kęstutis Česnavičius, CheeWhye Chin, Dustin Clausen, Jean-Louis Colliot-Thélène, Brian Conrad, Patrick Corn, David Corwin, Samit Dasgupta, Christopher Davis, Pavel Etingof, E. Victor Flynn, Thomas Graber, David Harari, Yonatan Harpaz, Robin Hartshorne, Ruthi Hortsch, Borys Kadets, Timo Keller, Steven Kleiman, Nikita Kozin, Chu-Wee Lim, William Messing, James Milne, Nghi Nguyen, Pace Nielsen, Arthur Ogus, René Pannekoek, Anatoly Preygel, Bhairav Singh, David Speyer, Padmavathi Srinivasan, Ronald van Luijk, Anthony Várilly-Alvarado, John Voight, Jared Weinstein, Olivier Wittenberg, Chenyang Xu, and several referees. In addition, various unpublished notes from the websites of Brian Conrad and James Milne have been very helpful to me. I also thank Yun Hao for converting my hand-drawn figures into TikZ.

While writing the book, the author was partially supported by National Science Foundation grants DMS-0301280, DMS-0841321, DMS-1069236, and DMS-1601946; a Packard Fellowship; a Guggenheim Fellowship; and grants from the Simons Foundation (#340694 and #402472 to Bjorn Poonen).

© Bjorn Poonen, April 29, 2017
CHAPTER 1

Fields

The first section of this chapter describes some types of fields. The other sections are concerned with questions one can ask about a field $k$ in order to quantify how far it is from being algebraically closed:

1. How many variables must a degree $d$ homogeneous form over $k$ have before it is guaranteed to have a nontrivial zero? (the $C_r$ property)
2. How complicated is the absolute Galois group of $k$? (cohomological dimension)
3. How complicated is the set of isomorphism classes of finite-dimensional central division algebras over $k$? (the Brauer group)

1.1. Some fields arising in classical number theory

1.1.1. Closures. Let $k$ be a field. Let $\overline{k}$ denote a fixed algebraic closure of $k$. Let $k_s$ denote the separable closure of $k$ in $\overline{k}$, so $k_s$ is the maximal separable extension of $k$ contained in $\overline{k}$. Let $k_{perf}$ denote the perfect closure of $k$, so $k_{perf}$ is the smallest perfect field containing $k$ and contained in $\overline{k}$. Equivalently, if $\text{char} \ k = p > 0$, then, in order to form a more perfect union, one can define $k_{perf} := \bigcup_{n \geq 1} k^{1/p^n} \subseteq \overline{k}$. The absolute Galois group of $k$ is the profinite group $G_k := \text{Gal}(k_s/k) \simeq \text{Aut}(\overline{k}/k)$.

1.1.2. Local fields.

(References: [Frö67], [Ser79], [RV99], Section 4.2])

A local field is a field $k$ satisfying one of the following equivalent conditions:

1. $k$ is a finite extension of $\mathbb{R}$, $\mathbb{Q}_p$, or $\mathbb{F}_q((u))$, for some prime $p$.
2. $k$ is isomorphic to one of the following:
   - $\mathbb{R}$,
   - $\mathbb{C}$,
   - a finite extension of $\mathbb{Q}_p$ for some prime $p$, or
   - $\mathbb{F}_q((u))$ for some prime power $q$.
3. $k$ is $\mathbb{R}$ or $\mathbb{C}$, or else $k$ is the fraction field of a complete discrete valuation ring with finite residue field.
4. $k$ is a nondiscrete locally compact topological field (more precisely, $k$ is locally compact and Hausdorff with respect to some nondiscrete topology for which the field operations are continuous).
(5) \(k\) is the completion of a global field (see Section 1.1.3) with respect to a nontrivial absolute value.

See Theorem 4-12 in [RV99] for a proof of the difficult part of the equivalence, namely that nondiscrete locally compact topological fields satisfy the other conditions.

If \(k\) is \(\mathbb{R}\) or \(\mathbb{C}\), then \(k\) is called archimedean; other local fields are called nonarchimedean.

1.1.3. Global fields.

(Reference: [Cas67])

A number field is a finite extension of \(\mathbb{Q}\). A global function field is a finite extension of \(\mathbb{F}_p(t)\) for some prime \(p\), or equivalently is the function field of a geometrically integral curve over a finite field \(\mathbb{F}_q\), where \(q\) is a power of some prime \(p\). (See Section 2.2 for the meaning of “geometrically integral curve.”) When we say that \(k\) is a global field we mean that \(k\) is either a number field or a global function field.

Equivalently, a global field is the fraction field of a finitely generated \(\mathbb{Z}\)-algebra that is an integral domain of Krull dimension 1.

By a place of \(k\), we always mean a nontrivial place of \(k\). Let \(\Omega_k\) be the set of places of \(k\).

Definition 1.1.1. If \(S\) is a finite nonempty subset of \(\Omega_k\) containing all the archimedean places, then the ring of \(S\)-integers in \(k\) is

\[\mathcal{O}_{k,S} := \{ a \in k : v(a) \geq 0 \text{ for all } v \notin S \} \]

If \(k\) is a number field, also define the ring of integers of \(k\) as \(\mathcal{O}_k := \mathcal{O}_{k,S}\) where \(S\) is the set of archimedean places.

If \(v\) is a place of \(k\), then \(k_v\) denotes the completion of \(k\) at \(v\). Let \(\mathcal{O}_v\) be the valuation ring of \(k_v\) if \(v\) is nonarchimedean, and let \(\mathcal{O}_v = k_v\) if \(v\) is archimedean. Equip \(k_v\) and its subset \(\mathcal{O}_v\) with the analytic (i.e., \(v\)-adic) topology coming from the place.

The adèle ring \(\mathbb{A} = \mathbb{A}_k\) of \(k\) is defined as the restricted product \(\prod'_{v \in \Omega_k} (k_v, \mathcal{O}_v)\); it is a \(k\)-algebra for the diagonal embedding of \(k\), and it is equipped with the unique topology such that

- \(\mathbb{A}\) is a topological group under addition,
- the subset \(\prod_{v \in \Omega_k} \mathcal{O}_v\) is open, and
- the subspace topology on \(\prod_{v \in \Omega_k} \mathcal{O}_v\) agrees with the product topology.

The image of \(k\) in \(\mathbb{A}\) is discrete, and \(\mathbb{A}/k\) is compact.

1.1.4. Other fields. For some other kinds of fields, see Appendix B.

1.2. \(C_r\) fields

(References: [Gre69], [Sha72], [Pfi95] Chapter 5)
Definition 1.2.1 (Lan52). Let $k$ be a field and let $r \in \mathbb{R}_{\geq 0}$. Then $k$ is $C_r$ if and only if every homogeneous form $f(x_1, \ldots, x_n)$ of degree $d > 0$ in $n$ variables with $n > d^r$ has a nontrivial zero in $k^n$. The adjective quasi-algebraically closed is a synonym for $C_1$.

1.2.1. Norm forms and normic forms.

Definition 1.2.2. Let $L$ be a finite extension of a field $k$. Let $e_1, \ldots, e_n$ be a basis for $L/k$. Write $L' = L(x_1, \ldots, x_n)$ and $k' = k(x_1, \ldots, x_n)$ where $x_1, \ldots, x_n$ are indeterminates. If $N_{L'/k'}$ denotes the norm from $L'$ to $k'$, then $N_{L'/k'}(x_1e_1 + \cdots + x_ne_n)$ is called a norm form for $L$ over $k$.

Example 1.2.3. Let $k = \mathbb{Q}$ and $L = \mathbb{Q}(\sqrt{7})$. The norm form for $L$ over $k$ associated to the basis $1, \sqrt{7}$ is $x_1^2 - 7x_2^2$.

Every norm form is a homogeneous polynomial of degree $n$ in $k[x_1, \ldots, x_n]$, for some $n \geq 1$. Although it depends on the choice of basis, changing the basis changes the norm form only by an invertible $k$-linear transformation of the variables. The value of the norm form at $(b_1, \ldots, b_n) \in k^n$ equals $N_{L/k}(b_1e_1 + \cdots + b_ne_n)$.

Definition 1.2.4. Let $k$ be a field. A homogeneous form $f \in k[x_1, \ldots, x_n]$ is called normic if $\deg f = n$ and $f$ has only the trivial zero in $k^n$.

Any norm form is normic. To construct other normic forms, we introduce some notation. If $f$ and $g$ are homogeneous forms, let $f(g \mid g \mid \cdots \mid g)$ be the homogeneous form obtained by substituting a copy of $g$ for each variable in $f$, except that a new set of variables is used after each occurrence of $\mid$. If $f$ is of degree $d$ in $n$ variables, and $g$ is of degree $e$ in $m$ variables, then $f(g \mid g \mid \cdots \mid g)$ is of degree $de$ in $nm$ variables. If $f$ and $g$ are normic, then so is $f(g \mid g \mid \cdots \mid g)$.

Lemma 1.2.5. If $k$ is a field, and $k$ is not algebraically closed, then $k$ has normic forms of arbitrarily high degree.

Proof. Since $k$ is not algebraically closed, it has a finite extension of degree $d > 1$. Let $f_1 = f$ be an associated norm form. For $\ell \geq 2$, let $f_\ell = f_{\ell-1}(f \mid f \mid \cdots \mid f)$. Then $f_\ell$ is normic of degree $d^\ell$. $\square$

1.2.2. Systems of forms.

Proposition 1.2.6 (Artin, Lang, Nagata). Let $k$ be a $C_r$ field, and let $f_1, \ldots, f_s$ be homogeneous forms of the same degree $d > 0$ in $n$ common variables. If $n > sd^r$, then $f_1, \ldots, f_s$ have a nontrivial common zero in $k^n$. 3
PROOF. Suppose that $k$ is algebraically closed. Since $n > sd^r \geq s$, the projective dimension theorem \cite{Har77} 1.7.2 implies that the intersection of the $s$ hypersurfaces $f_i = 0$ in $\mathbb{P}^{n-1}$ contains a point.

Therefore from now on assume that $k$ is not algebraically closed. Suppose also that the $f_i$ have no nontrivial common zero. We will build forms $\Phi_m$ of degree $D_m$ in $N_m$ variables having no nontrivial zero, by induction, and get a contradiction for large $m$. By Lemma 1.2.5 we can find a normic form $\Phi_0$ of arbitrarily high degree $e$ (later we will specify how large we need $e$ to be). So $D_0 = N_0 = e$. For $m \geq 1$, define

$$\Phi_m = \Phi_{m-1}(f_1, \ldots, f_s \mid f_1, \ldots, f_s \mid \cdots \mid f_1, \ldots, f_s \mid 0, 0, \ldots, 0)$$

where within each block $f_1, \ldots, f_s$ the same $n$ variables are used, but new variables are used after each $\mid$, and we use as many blocks as possible (namely, $\lfloor N_{m-1}/s \rfloor$ blocks) and pad with zeros to get the right number of arguments to $\Phi_{m-1}$. Thus $D_m = dD_{m-1}$ and $N_m = n \lfloor N_{m-1}/s \rfloor$. By induction on $m$, the form $\Phi_m$ has no nontrivial zero.

By induction, $D_m = d^m e$. If we could ignore the $\lfloor \rfloor$, then $N_m$ would be $(n/s)^m e$, and

$$\frac{N_m}{D_m} = \left( \frac{n}{sd^r} \right)^m e^{1-r} > 1$$

for sufficiently large $m$, since $n > sd^r$. But we cannot quite ignore $\lfloor \rfloor$, so choose $\beta \in \mathbb{R}$ with $d^r < \beta < n/s$, and choose the degree $e$ of the normic form $\Phi_0$ so that $n \lfloor x/s \rfloor \geq \beta x$ holds for all $x \geq e$. Then $N_m \geq \beta^m e$ by induction on $m$, and

$$\frac{N_m}{D_m} \geq \left( \frac{\beta}{d^r} \right)^m e^{1-r} > 1$$

for $m$ sufficiently large.

Since $k$ is $C_r$, the form $\Phi_m$ has a nontrivial zero, a contradiction. \hfill \square

1.2.3. Transition theorems.

THEOREM 1.2.7. Let $k$ be a $C_r$ field, and let $L$ be a field extension of $k$.

(i) If $L$ is algebraic over $k$, then $L$ is $C_r$.
(ii) If $L = k(t)$, where $t$ is an indeterminate, then $L$ is $C_{r+1}$.
(iii) If $\text{tr} \ \text{deg}(L/k) = s$, then $L$ is $C_{r+s}$.

PROOF.

(i) Let $f \in L[x_1, \ldots, x_n]$ be a form of degree $d > 0$, where $n > d^r$. Since $L$ is algebraic over $k$, the coefficients of $f$ generate a finite extension $L_0$ of $k$. If we find a nontrivial zero of $f$ over $L_0$, then the same is a nontrivial zero over $L$. Thus we reduce to the case where $L$ is a finite extension of $k$. 

4
Choose a basis $e_1, \ldots, e_s$ of $L$ over $k$. Introduce new variables $y_{ij}$ with $1 \leq i \leq n$ and $1 \leq j \leq s$, and substitute

$$x_i = \sum_{j=1}^{s} y_{ij} e_j$$

for all $i$ into $f$, so that

$$f(x_1, \ldots, x_n) = F_1 e_1 + \cdots + F_s e_s$$

where each $F_\ell \in k[\{y_{ij}\}]$ is a form of degree $d$ in $ns$ variables. Since $n > d^r$, we have $ns > sd^r$, so Proposition [1.2.6] implies that the $F_\ell$ have a nontrivial common zero $(y_{ij})$ over $k$. This means that $f$ has a nontrivial zero over $L$.

(ii) Let $f \in k(t)[x_1, \ldots, x_n]$ be a form of degree $d > 0$, where $n > d^{r+1}$. Multiplying $f$ by a polynomial in $k[t]$ to clear denominators, we may assume that $f$ has coefficients in $k[t]$. Let $m$ be the maximum of the degrees of these coefficients. Choose $s \in \mathbb{Z}_{>0}$ large (later we’ll say how large), introduce new variables $y_{ij}$ with $1 \leq i \leq n$ and $0 \leq j \leq s$, and substitute

$$x_i = \sum_{j=0}^{s} y_{ij} t^j$$

for all $i$ into $f$, so that

$$f(x_1, \ldots, x_n) = F_0 + F_1 t + \cdots + F_{ds+m} t^{ds+m},$$

where each $F_\ell \in k[\{y_{ij}\}]$ is a form of degree $d$ in $n(s+1)$ variables. Because $n > d^{r+1}$,

$$n(s + 1) > (ds + m + 1)d^r$$

holds for sufficiently large $s$, and then Proposition [1.2.6] implies that the $F_\ell$ have a nontrivial common zero $(y_{ij})$ over $k$. This means that $f$ has a nontrivial zero over $k[t]$, hence over $k(t)$.

(iii) This follows from (i) and (ii), by induction on $s$.

\[ \square \]

1.2.4. Examples of $C_r$ fields.

(1) A field is $C_0$ if and only if it is algebraically closed. For a generalization, see Exercise [1.3].

(2) The following special case of Theorem [1.2.7] is known as Tsen’s theorem: If $L$ is the function field of a curve over an algebraically closed field $k$ (that is, $L$ is a finitely generated extension of $k$ of transcendence degree 1), then $L$ is $C_1$.

(3) The Chevalley–Warning theorem states that finite fields are $C_1$. This was conjectured by E. Artin, and proved first by Chevalley [Che36], who proved more generally that over a finite field $\mathbb{F}_q$, a (not necessarily homogeneous) polynomial $f$ of total
degree $d$ in $n > d$ variables with zero constant term has a nontrivial zero. Warning’s proof \cite{War36} of this proceeded by showing that the total number of zeros, including the trivial zero, was a multiple of $p := \operatorname{char} \mathbb{F}_q$. Ax \cite{Ax64} showed moreover that the number of zeros was divisible by $q$, and in fact divisible by $q^b$ where $b = \lceil n/d \rceil - 1$ is the largest integer strictly less than $n/d$. For an improvement in a different direction, observe that Warning’s theorem says that a hypersurface $X$ in $\mathbb{P}^{n-1}$ over $\mathbb{F}_q$ defined by a homogeneous form of degree $d < n$ satisfies $\# X(\mathbb{F}_q) \equiv 1 \pmod{p}$; this can be extended to some varieties that are not hypersurfaces, such as smooth projective rationally chain connected varieties \cite[Corollary 1.3]{Esn03}; see \cite{Wit10} for a survey about this and further generalizations.

(4) Lang proved that if $k$ is complete with respect to a discrete valuation having algebraically closed residue field, then $k$ is $C_1$. More generally, if $k$ is a henselian discrete valuation field with algebraically closed residue field such that the completion $\hat{k}$ is separable over $k$, then $k$ is $C_1$. (See Section B.3 for the definition of henselian.) This applies in particular if $k$ is the maximal unramified extension of a complete discrete valuation field with perfect residue field. For example, the maximal unramified extension $\mathbb{Q}_p^{unr}$ of $\mathbb{Q}_p$ is $C_1$. See \cite{Lan52} for all these results.

(5) A local field of positive characteristic is $C_2$: see Theorem 8 of \cite{Lan52}. More generally, if $k$ is $C_r$, then $k((t))$ is $C_{r+1}$ \cite{Gre66}.

1.2.5. Counterexamples. The field $\mathbb{R}$ is not $C_r$ for any $r$, since for every $n \geq 1$ the equation $x_1^2 + \cdots + x_n^2 = 0$ has no nontrivial solution. The same argument applies to any formally real field.

E. Artin conjectured that nonarchimedean local fields were $C_2$, the expectation being that if a field $k$ is complete with respect to a discrete valuation with a $C_r$ residue field, then $k$ should be $C_{r+1}$. That nonarchimedean local fields satisfy the $C_2$ property \textit{restricted to degree $d$ forms} was proved for $d = 2$ \cite{Has24} and $d = 3$ \cite{Dem50,Lew52}. Also Ax and Kochen \cite{AK65} nearly proved that the field $\mathbb{Q}_p$ is $C_2$: using model theory they showed that for each $d$, for all primes $p$ outside a finite set depending on $d$, every homogeneous form of degree $d$ in $> d^2$ variables over $\mathbb{Q}_p$ has a nontrivial zero. But then Terjanian \cite{Ter66} disproved Artin’s conjecture by finding a homogeneous form of degree 4 in 18 variables over $\mathbb{Q}_2$ with no nontrivial zero. Later it was shown that if $[k : \mathbb{Q}_p] < \infty$, then $k$ is not $C_r$ for any $r$ \cite{AK81,Ale85}. It follows that if $k$ is a number field, then $k$ is not $C_r$ for any $r$ (Exercise 1.8).

1.2.6. Open questions.

Question 1.2.8. Is there a field $k$ and $r \in \mathbb{R}_{\geq 0}$ such that $k$ is $C_r$ but not $C_{\lfloor r \rfloor}$?
QUESTION 1.2.9 (E. Artin). Let \( \mathbb{Q}^{ab} \) be the maximal abelian extension of \( \mathbb{Q} \). (The Kronecker–Weber theorem states that \( \mathbb{Q}^{ab} \) is obtained by adjoining all roots of 1 to \( \mathbb{Q} \).) Is \( \mathbb{Q}^{ab} \) a \( C_1 \) field?

DEFINITION 1.2.10. A field \( k \) is called \( C'_r \) if whenever one has homogeneous forms \( f_1, \ldots, f_s \) in \( n \) common variables of degrees \( d_1, \ldots, d_s \), respectively, with \( n > d_1^r + \cdots + d_s^r \), the forms have a nontrivial common zero in \( k^n \).

QUESTION 1.2.11 ([Gre69, p. 21]). Is \( C_r \) equivalent to \( C'_r \)?

By definition, \( C'_r \) implies \( C_r \). The converse holds at least for fields \( k \) such that for every \( d \geq 1 \) there exists a homogeneous form of degree \( d \) in \( d^r \) variables over \( k \) with no nontrivial zero [Lan52, Theorem 4]. The \( C'_r \) property is studied in more detail in [Pfi95, Chapter 5].

QUESTION 1.2.12. What general classes of varieties are guaranteed to have a \( k \)-point whenever \( k \) is \( C_1 \)?

QUESTION 1.2.13 (Ax). Is every perfect PAC field \( C_1 \)? (See Section B.5 for the definition of PAC.)

By [Kol07a, Theorem 1], every PAC field of characteristic 0 is \( C_1 \), and even \( C'_1 \). See [FJ08, 21.3.6] for a few other positive partial results towards Question 1.2.13.

1.3. Galois theory

1.3.1. \( \mathfrak{G}_k \)-sets. Let \( k \) be a field. Let \( \mathfrak{G}_k \) be the profinite group \( \text{Gal}(k_\bar{s}/k) \). A \( \mathfrak{G}_k \)-set is a set \( S \) (with the discrete topology) equipped with a continuous action of \( \mathfrak{G}_k \). A morphism of \( \mathfrak{G}_k \)-sets is a map of sets respecting the \( \mathfrak{G}_k \)-actions. A \( \mathfrak{G}_k \)-set is called finite if it is finite as a set. For example, if \( H \) is an open subgroup of \( \mathfrak{G}_k \), then \( \mathfrak{G}_k/H \) equipped with the left multiplication action of \( \mathfrak{G}_k \) is a finite \( \mathfrak{G}_k \)-set.

A continuous action of \( \mathfrak{G}_k \) on a set \( S \) is called transitive if \( S \neq \emptyset \) and for every \( s_1, s_2 \in S \) there exists \( g \in \mathfrak{G}_k \) such that \( gs_1 = s_2 \). In this case, if we fix \( s \in S \) and define \( H = \text{Stab}_{\mathfrak{G}_k}(s) := \{ g \in \mathfrak{G}_k : gs = s \} \), then \( H \) is open and the map \( \mathfrak{G}_k/H \to S \) sending \( gH \in \mathfrak{G}_k/H \) to \( gs \) is an isomorphism of \( \mathfrak{G}_k \)-sets; in particular, \( S \) is finite. Every \( \mathfrak{G}_k \)-set decomposes uniquely as a disjoint union of transitive \( \mathfrak{G}_k \)-sets, the orbits.

1.3.2. Étale algebras. The problem with field extensions \( L \supseteq k \) is that if we change the base by tensoring with a field extension \( k' \) of \( k \), the resulting algebra \( L \otimes_k k' \) over \( k' \) need not be a field. The notion of étale algebra generalizes the notion of finite separable field extension in order to fix this problem.

DEFINITION 1.3.1. A \( k \)-algebra \( L \) is called étale if it satisfies any of the following equivalent conditions:
• $L$ is a direct product of finite separable extensions of $k$;
• the $k_s$-algebra $L \otimes_k k_s$ is a finite product of copies of $k_s$;
• the morphism of schemes $\text{Spec } L \to \text{Spec } k$ is finite and étale in the sense of Section 3.5.8 (see Proposition 3.5.35).

A morphism between two étale $k$-algebras is a homomorphism of $k$-algebras. If $L$ is an étale $k$-algebra, and $k'$ is any field extension of $k$, then $L \otimes_k k'$ is an étale $k'$-algebra.

The following is Grothendieck’s restatement and generalization of Galois theory.

**Theorem 1.3.2 ([SGA 1 V.7 and Proposition V.8.1]).** The functors
\[ \{\text{finite } \mathcal{G}_k\text{-sets}\}^{\text{opp}} \leftrightarrow \{\text{étale } k\text{-algebras}\} \]
\[ S \mapsto \text{Hom}_{\mathcal{G}_k\text{-sets}}(S, k_s) = \text{Hom}_{\text{sets}}(S, k_s)^{\mathcal{G}_k} \]
\[ \text{Hom}_{k\text{-algebras}}(L, k_s) \mapsto L \]
are inverse equivalences of categories.

**Example 1.3.3.** If $S$ is a transitive $\mathcal{G}_k$-set, say $S = \mathcal{G}_k/H$ for an open subgroup $H \leq \mathcal{G}_k$, then the corresponding étale algebra is the $H$-fixed subfield $\text{Hom}_{\mathcal{G}_k\text{-sets}}(\mathcal{G}_k/H, k_s) = (k_s)^H$ of $k_s$, i.e., the finite separable extension of $k$ associated to $H$ by classical Galois theory.

In general, a finite $\mathcal{G}_k$-set $S$ is a finite disjoint union $\coprod S_i$ of transitive $\mathcal{G}_k$-sets. If $S_i$ corresponds to the finite separable extension $L_i$, then $S$ corresponds to the étale algebra $\prod L_i$.

**Example 1.3.4.** If $S$ is a finite set with trivial $\mathcal{G}_k$-action, the corresponding étale algebra is a finite product of copies of $k$. Such étale algebras are called split.

**1.3.3. Galois étale algebras.** Just as étale algebras generalize finite separable field extensions, Galois étale algebras generalize finite Galois field extensions:

**Definition 1.3.5.** Let $L$ be an étale $k$-algebra with a left action of a finite group $G$. If $\Omega \supseteq k$ is a field extension, then $L \otimes_k \Omega$ is an étale $\Omega$-algebra with left $G$-action, and so is $\prod_{g \in G} \Omega = \text{Hom}_{\text{sets}}(G, \Omega)$ via the right translation $G$-action on $G$. Call $L$ a **Galois étale $k$-algebra with Galois group $G$** if for some field extension $\Omega \supseteq k$ we have $L \otimes_k \Omega \simeq \prod_{g \in G} \Omega$ as étale $\Omega$-algebras with left $G$-action.

**Warning 1.3.6.** The group $\text{Aut}(L/k)$ can be larger than $G$, and in fact $G$ is not determined by $L/k$. For example, if $L = k \times k \times k \times k$, then $L/k$ can be equipped with actions of $\mathbb{Z}/4\mathbb{Z}$ or $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ making it a Galois étale algebra, but $\text{Aut}(L/k) \simeq S_4$. This explains why in Definition 1.3.5 the group $G$ and its action on $L$ must be specified in advance.

**Remark 1.3.7.** If an $\Omega$ as in Definition 1.3.5 exists, then one such $\Omega$ is $k_s$. 

8
1.3.4. Galois descent for vector spaces. Let $L/k$ be a finite Galois extension of fields with Galois group $G$. An action of $G$ on an $L$-vector space $W$ is **semilinear** if $\sigma(\ell w) = (\sigma \ell)(\sigma w)$ for all $\sigma \in G$, $\ell \in L$, and $w \in W$.

**Example 1.3.8.** The coordinate-wise action of $G$ on $L^n$ is semilinear. More generally, if $V$ is any $k$-vector space, then $V \otimes_k L$ is an $L$-vector space with semilinear $G$-action.

**Lemma 1.3.9.** Let $V$ be a $k$-vector space. Then the $k$-linear map

$$V \longrightarrow (V \otimes_k L)^G$$

$$v \longmapsto v \otimes 1$$

is an isomorphism.

**Proof.** For $V = k$, this is the Galois theory fact $L^G = k$. Any $V$ is a direct sum of copies of the 1-dimensional space $k$, and the formation of the map respects direct sums. □

**Lemma 1.3.10.** Let $W$ be an $L$-vector space with semilinear $G$-action. Then the $L$-linear map

$$W^G \otimes_k L \longrightarrow W$$

$$w \otimes \ell \longmapsto \ell w$$

is an isomorphism.

**Proof.** We will prove that the same holds even if $L/k$ is only a Galois étale $k$-algebra with Galois group $G$ (and $W$ is an $L$-module with semilinear $G$-action). The advantage of considering this more general statement is that now we can extend the ground field by applying $\otimes_k \Omega$ to $k$, $L$, and $W$. The operation of taking $G$-invariants and the property of a linear map being an isomorphism are preserved by such a base change, so after renaming $\Omega$ as $k$, we reduce to the split case $L = \prod_{g \in G} k$. Let $e_g = (0, \ldots, 0, 1, 0, \ldots, 0) \in L$, with 1 in the $g$th coordinate. Then the $L$-module $W$ is $\prod_{g \in G} W_g$ for some $k$-vector spaces $W_g := e_g W$. An element $g \in G$ maps $e_g$ to $e_1$, and hence provides an isomorphism $W_g \simeq W_1$. Then $W^G$ is the diagonal image of $W_1 \hookrightarrow \prod_{g \in G} W_g$. Finally, the map $W^G \otimes_k L \rightarrow W$ restricts to an isomorphism $W^G \otimes_k ke_g \simeq W_g$ for each $g$, so it is an isomorphism. □

**Theorem 1.3.11.** Let $L/k$ be a finite Galois extension of fields with Galois group $G$. The functors

$$\{k\text{-vector spaces}\} \xrightarrow{\otimes_k L} \{L\text{-vector spaces with semilinear } G\text{-action}\}$$

are inverse equivalences of categories.
Proof. The two compositions are isomorphic to the identity functors, by Lemmas 1.3.9 and 1.3.10.

Corollary 1.3.12. Let $L/k$ be a finite Galois extension of fields with Galois group $G$.
Let $r \in \mathbb{Z}_{\geq 0}$. Then there is only one $r$-dimensional $L$-vector space with semilinear $G$-action, up to isomorphism.

Proof. The functor $\otimes_k L$ in Theorem 1.3.11 respects dimension: $\dim_k V = \dim_L (V \otimes_k L)$.
There is only one $r$-dimensional $k$-vector space, up to isomorphism.

Remark 1.3.13. Theorem 1.3.11 and its proof generalize to the theory of descent developed by Weil and Grothendieck. See Chapter 4.

### 1.3.5. Hilbert’s theorem 90 and generalizations.

Let us gather a few fundamental results in Galois cohomology. Let $L^+$ denote the additive group of a field $L$. If $k$ is a field, and $n \in \mathbb{Z}_{\geq 1}$ is not divisible by $\text{char } k$, let $\mu_n$ denote the group of $n$th roots of 1 in $k^\times$.

Definition 1.3.14. If $A$ is a commutative group scheme (see Section 5.1) over a field $k$, then $H^q(k, A)$ denotes the Galois cohomology group $H^q(G_k, A(k_s))$. (This definition is made so as to agree with the étale cohomology group $H^q_{\text{ét}}(\text{Spec } k, A)$ of the sheaf defined by $A$ on the étale site of Spec $k$: see Section 6.4.3.) If $A$ is noncommutative, the same definition is made for $q = 0, 1$.

Proposition 1.3.15. Let $L/k$ be a Galois extension of fields.
(i) $H^q(\text{Gal}(L/k), L^+) = 0$ for all $q \geq 1$. In particular, $H^q(k, \mathbb{G}_a) = 0$ for all $q \geq 1$.
(ii) (“Hilbert’s theorem 90”) $H^1(\text{Gal}(L/k), L^\times) = 0$. In particular, $H^1(k, \mathbb{G}_m) = 0$.
(iii) Let $r \in \mathbb{Z}_{\geq 0}$. Then $H^1(\text{Gal}(L/k), \text{GL}_r(L)) = 0$. In particular, $H^1(k, \text{GL}_r) = 0$.

Remark 1.3.16. Hilbert’s original theorem 90 was essentially the special case of (iii) in which $\text{Gal}(L/k)$ is a finite cyclic group: see Exercise 1.10. It was E. Noether who generalized it to arbitrary (finite) Galois extensions.

Proof. We may assume that $[L : k] < \infty$, since the general case then follows by taking a direct limit.

(i) By the normal basis theorem, $L^+$ is an induced $\text{Gal}(L/k)$-module, so it has trivial cohomology.
(ii) This is the $r = 1$ case of (iii), which we will now prove.
(iii) Let $G = \text{Gal}(L/k)$. Given a 1-cocahn (i.e., function) $\xi : G \to \text{GL}_r(L)$, let $W_\xi$ be $L^\times$ equipped with the function $G \times L^\times \to L^\times$ sending $(\sigma, w)$ to $\xi_\sigma(\sigma w)$. Exercise 1.9a shows that this describes a semilinear $G$-action (i.e., the group action axiom $(\sigma \tau)^* w = \sigma^* (\tau^* w)$ is satisfied) if and only if $\xi$ is a cocycle. Exercise 1.9b shows also that given two 1-cocycles
ξ and ξ’, we have \( W_ξ \simeq W_{ξ’} \) as \( L \)-vector spaces with semilinear \( G \)-action if and only if \( ξ \) and \( ξ’ \) are cohomologous. Thus we obtain a bijection

\[
\text{H}^1(G, \text{GL}_r(L)) \leftrightarrow \{ r\text{-dimensional } L\text{-vector spaces with semilinear } G\text{-action} \}_{\text{isomorphism}}.
\]

By Corollary 1.3.12, the latter set has one element, so \( \text{H}^1(G, \text{GL}_r(L)) = 0 \) too. □

Remark 1.3.17. There is an alternative proof of (iii) that proceeds by showing directly that every 1-cocycle \( ξ: G \to \text{GL}_r(L) \) is cohomologous to the trivial 1-cocycle, by writing down a “Poincaré series”: see [Ser79, Chapter X, Proposition 3]. This proof has the advantage of being short and needing little beyond Dedekind’s theorem on linear independence of automorphisms, but is harder to remember and does not readily generalize to give the theory in Chapter 4.

Remark 1.3.18. Suppose that \( L \) is an extension of \( k \). Choose an embedding \( ι: k_s \hookrightarrow L_s \); we then get an inclusion homomorphism \( A(k_s) \to A(L_s) \), and a restriction homomorphism \( \mathfrak{G}_L \to \mathfrak{G}_k \). Thus we get a homomorphism \( \text{H}^q(k, A) \to \text{H}^q(L, A) \), and it is independent of \( ι \), since the conjugation action of a group \( G \) on any cohomology group \( \text{H}^q(G, M) \) is trivial, as can be proved by dimension shifting.

1.4. Cohomological dimension
(Reference: [Ser02])

This section is almost never used in the rest of the book, so it may be skipped upon a first reading.

1.4.1. Definitions. Let \( G \) be a profinite group. When we say that \( A \) is a \( G \)-module, we mean that \( A \) is an abelian group with an action of the abstract group \( G \) such that the map \( G \times A \to A \) giving the action is continuous for the profinite topology on \( G \) and the discrete topology on \( A \).

A \( G \)-module \( A \) is called torsion if and only if every element of the abelian group \( A \) has finite order. If \( B \) is an abelian group, and \( n \) is an integer, define \( B[n] := \{ b \in B : nb = 0 \} \).

If \( p \) is a prime number, define \( B[p^\infty] := \bigcup_{n \geq 1} B[p^n] \).

Definition 1.4.1. Let \( G \) be a profinite group, and let \( p \) be a prime number.

(i) The \( p \)-cohomological dimension of \( G \), denoted \( \text{cd}_p(G) \), is the smallest \( n \in \mathbb{N} \) such that for all torsion \( G \)-modules \( A \) and all integers \( q > n \), \( \text{H}^q(G, A)[p^\infty] = 0 \). If no such \( n \) exists, then \( \text{cd}_p(G) = +\infty \).

(ii) The strict \( p \)-cohomological dimension of \( G \), denoted \( \text{scd}_p(G) \), is defined in the same way as \( \text{cd}_p(G) \), except that the word “torsion” is omitted.

(iii) The cohomological dimension of \( G \) is \( \text{cd}(G) := \sup_p \text{cd}_p(G) \).
(iv) The strict cohomological dimension of $G$ is $\text{scd}(G) := \sup_p \text{scd}_p(G)$.

**Proposition 1.4.2.*** For any profinite group $G$ and any prime number $p$, $\text{scd}_p(G)$ equals $\text{cd}_p(G)$ or $\text{cd}_p(G) + 1$.

**Proof.** Clearly $\text{scd}_p(G) \geq \text{cd}_p(G)$. To complete the proof, we assume that $\text{cd}_p(G) = n < \infty$ and attempt to prove that $\text{scd}_p(G) \leq n + 1$.

Let $A$ be a $G$-module. Take the long exact sequences associated to

$$0 \rightarrow A[p] \rightarrow A \xrightarrow{p} pA \rightarrow 0$$

and

$$0 \rightarrow pA \rightarrow A \rightarrow A/pA \rightarrow 0.$$ 

For $q > n + 1$, $H^q(G, A[p]) = 0$ and $H^{q-1}(G, A/pA) = 0$ (since $\text{cd}_p(G) = n$), so the long exact sequences give injections $H^q(G, A) \hookrightarrow H^q(G, pA)$ and $H^q(G, pA) \hookleftarrow H^q(G, A)$, respectively. The composition of these injections is multiplication by $p$ on $H^q(G, A)$, so $H^q(G, A)[p\infty] = 0$. Thus $\text{scd}_p(G) \leq n + 1$, by definition. \hfill $\square$

Recall that if $k$ is a field, then $\mathfrak{G}_k$ denotes the profinite group $\text{Gal}(k_s/k)$.

**Definition 1.4.3.** If $k$ is a field, then $\text{cd}_p(k) := \text{cd}_p(\mathfrak{G}_k)$. Define $\text{scd}_p(k), \text{cd}(k)$, and $\text{scd}(k)$ similarly.

**1.4.2. Transition theorems.** The condition $\text{cd}(k) \leq r$ on a field behaves under field extensions similarly to the $C_r$ condition. To prove such results, we need to develop analogous transition theorems for cohomological dimension of groups.

Let us first recall the definition of induced modules, and Shapiro’s lemma.

**Definition 1.4.4.** Suppose that $H$ is a closed subgroup of a profinite group $G$, and $A$ is an $H$-module. The induced module $\text{Ind}_H^G(A)$ is the group of continuous maps $\phi : G \rightarrow A$ such that $\phi(hx) = h\phi(x)$ for all $x \in G$ and $h \in H$. Each $g \in G$ acts on $\text{Ind}_H^G(A)$ by $(g\phi)(x) = \phi(xg)$; this makes $\text{Ind}_H^G(A)$ a $G$-module.

**Lemma 1.4.5 (Shapiro’s lemma).** Suppose that $H$ is a closed subgroup of a profinite group $G$, and $A$ is an $H$-module. Then $H^q(G, \text{Ind}_H^G(A)) \cong H^q(H, A)$.

Now we prove a transition theorem for cohomological dimension of groups.

**Proposition 1.4.6.** Let $H$ be a closed subgroup of a profinite group $G$, and let $p$ be prime. Then $\text{cd}_p(H) \leq \text{cd}_p(G)$ and $\text{scd}_p(H) \leq \text{scd}_p(G)$. Equality holds in both, if either

(i) the index $(G : H)$ is prime to $p$, or

(ii) the subgroup $H$ is open in $G$ and $\text{cd}_p(G) < \infty$. 

12
Remark 1.4.7. The condition “\((G : H)\) is prime to \(p\)” means that each open subgroup of \(G\) containing \(H\) has index prime to \(p\). Alternatively (but equivalently), \((G : H)\) can be interpreted as a supernatural number \([\text{Ser02}]\ I.1.3\).

Proof. Let \(A\) be a torsion \(H\)-module. Then \(A' := \text{Ind}_{H}^{G}(A)\) is a torsion \(G\)-module with \(H^{n}(G, A') \cong H^{n}(H, A)\) (Shapiro’s lemma). Thus \(\text{cd}_{p}(H) \leq \text{cd}_{p}(G)\) by definition.

Now suppose (i). The corestriction-restriction formula \(\text{Cor} \circ \text{Res} = n\) on cohomology for subgroups of finite index \(n\) implies that \(\text{Res}: H^{n}(G, A)[p\infty] \to H^{n}(H, A)[p\infty]\) is injective, at least if \((G : H)\) is finite (and prime to \(p\)). In fact, this holds also for \((G : H)\) infinite (and prime to \(p\)), by expressing the cohomology as direct limits over cohomology of finite groups. Hence \(\text{cd}_{p}(G) \leq \text{cd}_{p}(H)\).

Now suppose (ii) instead. Let \(n = \text{cd}_{p}(G)\). We may assume \(n \geq 1\). Choose a torsion \(G\)-module \(A\) such that \(H^{n}(G, A)[p\infty] \neq 0\). Let \(A' = \text{Ind}_{H}^{G}(A)\). There is a surjection of \(G\)-modules \(\pi: A' \to A\) mapping \(\phi\) to \(\sum_{x \in G/H} x \cdot \phi(x^{-1})\) (where \(x\) ranges over a set of coset representatives for \(H\) in \(G\)). If \(B = \ker \pi\), then we have an exact sequence
\[
H^{n}(G, A') \to H^{n}(G, A) \to H^{n+1}(G, B).
\]
These groups are torsion, so taking \(p\)-primary parts is exact. Since \(\text{cd}_{p}(G) = n\), we have \(H^{n+1}(G, B)[p\infty] = 0\), so \(H^{n}(G, A')[p\infty] \to H^{n}(G, A)[p\infty]\) is surjective. Thus \(H^{n}(G, A')[p\infty]\) is nonzero, and Shapiro’s lemma identifies this with \(H^{n}(H, A)[p\infty]\). Hence \(\text{cd}_{p}(H) \geq n = \text{cd}_{p}(G)\).

The same proofs work for \(\text{scd}_{p}\). \(\square\)

Given an algebraic extension \(L \supseteq k\), let \([L : k]_{s}\) denotes the separable degree; then “\([L : k]_{s}\) is prime to \(p\)” means that every finite separable extension of \(k\) inside \(L\) has degree prime to \(p\).

Corollary 1.4.8. Let \(L\) be an algebraic extension of \(k\), and let \(p\) be prime. Then \(\text{cd}_{p}(L) \leq \text{cd}_{p}(k)\). Equality holds in both, if either

(i) \([L : k]_{s}\) is prime to \(p\), or
(ii) \([L : k]_{s} < \infty\) and \(\text{cd}_{p}(k) < \infty\).

Corollary 1.4.8 can be strengthened for finite extensions.

Proposition 1.4.9. Suppose \([L : k] < \infty\). Then \(\text{cd}_{p}(L) = \text{cd}_{p}(k)\) unless the following are simultaneously satisfied:

(i) \(p = 2\),
(ii) \(k\) is formally real, and
(iii) \(\text{cd}_{2}(L) < \infty\).

Proof. See Proposition 10’ in II.§4.1 of \([\text{Ser02}]\). \(\square\)

Remark 1.4.10. We have \(\text{cd}_{2}(\mathbb{R}) = \infty\) but \(\text{cd}_{2}(\mathbb{C}) = 0\), so the “unless” clause in Proposition 1.4.9 cannot be eliminated.
Proposition 1.4.11. Let $L$ be an extension of $k$ with $\text{tr} \deg(L/k) = s$, and let $p$ be prime. Then $\text{cd}_p(L) \leq \text{cd}_p(k) + s$. Equality holds if $L$ is finitely generated over $k$, $\text{cd}_p(k) < \infty$, and $p \neq \text{char} \ k$.

Proof. See Proposition 11 in II.§4.2 of [Ser02]. □

Proposition 1.4.12. Let $L$ be complete with respect to a discrete valuation with residue field $k$, and let $p$ be prime. Then $\text{cd}_p(L) \leq \text{cd}_p(k) + 1$. Equality holds if $\text{cd}_p(k) < \infty$ and $p \neq \text{char} \ L$.

Proof. See Proposition 12 in II.§4.3 of [Ser02]. □

1.4.3. Examples.

(1) If $k$ is a separably closed field, then $\mathfrak{G}_k$ is trivial, so $\text{cd}_p(k) = \text{scd}_p(k) = 0$ for all $p$.

(2) If $k$ is a finite field, then $\mathfrak{G}_k = \hat{\mathbb{Z}}$, and $\text{cd}_p(k) = 1$ and $\text{scd}_p(k) = 2$ for all $p$.

(3) If $k$ is a nonarchimedean local field, then $\text{cd}_p(k) = \text{scd}_p(k) = 2$ for all $p \neq \text{char} \ k$. (For $\text{cd}_p$ this follows from Proposition 1.4.12. For $\text{scd}_p$ in the case of finite extensions of $\mathbb{Q}_\ell$, see Proposition 15 in II.§5.3 of [Ser02]. For a proof of the more general fact that an $n$-dimensional local field $k$ in the sense of Section B.1 has $\text{cd}_p(k) = \text{scd}_p(k) = n + 1$ for $p \neq \text{char} \ k$, see [Koy03].)

(4) Suppose that $k$ is a global field, and $p \neq \text{char} \ k$. If $k$ has a real place, suppose that $p \neq 2$. Then $\text{cd}_p(k) = \text{scd}_p(k) = 2$. (See Proposition 13 in II.§4.4 of [Ser02] and Theorems 8.3.17 and 10.2.3 in [NSW08].)

(5) Let $k_0$ be a finite field or a number field. Let $p$ be a prime not equal to $\text{char} \ k_0$. In the case where $k_0$ is a number field having a real place, assume in addition that $p \neq 2$. Then for any finitely generated field extension $k$ of $k_0$,

$$\text{cd}_p(k) = \begin{cases} 
\text{tr} \deg(k/k_0) + 1, & \text{if } k_0 \text{ is a finite field} \\
\text{tr} \deg(k/k_0) + 2, & \text{if } k_0 \text{ is a number field}.
\end{cases}$$

This follows from the previous examples by using Proposition 1.4.11.

1.5. Brauer groups of fields

(Reference: [GS06])

1.5.1. Azumaya algebras over a field.
**Definition 1.5.1.** An Azumaya algebra\(^1\) over a field \(k\) is a \(k\)-algebra \(A\) (associative and with 1, but possibly noncommutative) such that \(A \otimes_k k_s\) is isomorphic as a \(k_s\)-algebra to the matrix algebra \(M_n(k_s)\) for some \(n \geq 1\).

Equivalent definitions are given in Proposition 1.5.2. Some of these definitions require additional terminology, which we now provide. Let \(A\) be a (possibly noncommutative) \(k\)-algebra. Then \(A\) is said to be **finite-dimensional** if and only if the dimension of \(A\) as a \(k\)-vector space is finite. We say that \(A\) is **central** if and only if its center is the image of \(k\) in \(A\). Finally, \(A\) is **simple** if and only if \(A\) has exactly two 2-sided ideals, namely 0 and \(A\).

**Proposition 1.5.2** (Characterizations of Azumaya algebras). For a \(k\)-algebra \(A\), the following are equivalent:

(i) There exists a finite separable extension \(L \supseteq k\) such that the \(L\)-algebra \(A \otimes_k L\) is isomorphic to the matrix algebra \(M_n(L)\) for some \(n \geq 1\).

(ii) \(A \otimes_k k_s\) is isomorphic to the matrix algebra \(M_n(k_s)\) for some \(n \geq 1\); i.e., \(A\) is an Azumaya algebra over \(k\).

(iii) There exists a field extension \(L \supseteq k\) such that the \(L\)-algebra \(A \otimes_k L\) is isomorphic to the matrix algebra \(M_n(L)\) for some \(n \geq 1\).

(iv) The algebra \(A\) is a finite-dimensional central simple algebra over \(k\).

(v) There is a \(k\)-algebra isomorphism \(A \simeq M_r(D)\) for some integer \(r \geq 1\) and some finite-dimensional central division algebra \(D\) over \(k\).

In (v), \(r\) and \(D\) are uniquely determined by \(A\).

**Sketch of proof.** The implications (i) \(\iff\) (ii) \(\Rightarrow\) (iii) \(\Rightarrow\) (iv) and the implication (v) \(\Rightarrow\) (iv) are left as Exercise 1.14. The implication (iv) \(\Rightarrow\) (v) and the uniqueness of \(r\) and \(D\) are a consequence of Wedderburn’s theorem [GS06, Theorem 2.1.3]: the idea is to choose a simple \(A\)-module \(M\), to recover \(D\) as \(\operatorname{End}_A M\), and to show that the homomorphism \(A \rightarrow \operatorname{End}_D M\) is an isomorphism. The implication (v) \(\Rightarrow\) (ii), or equivalently the statement that a finite-dimensional division algebra over a separably closed field is commutative, is due to Noether and Köthe: for a proof, see [Bou12, §13.2, Proposition 3]. □

Let \(\mathbf{Az}_k\) be the category of Azumaya algebras over \(k\), with \(k\)-algebra homomorphisms as the morphisms. Each \(A\) of dimension \(d\) can be described by \(d^3\) elements of \(k\) expressing the product of each pair from a basis in terms of the basis. It follows that the isomorphism classes in \(\mathbf{Az}_k\) form a set (in the universe \(U\) we are working in, as in Appendix A), in contrast

\(^1\)Azumaya algebras over a field are more commonly called **central simple algebras**, while the term “Azumaya algebra” is reserved for the generalization in which the field is replaced by a ring or scheme. Our reason for calling them Azumaya algebras even over a field is (1) to use a single term consistently for all bases and (2) to highlight that the property of being a twist of a matrix algebra is often more useful or relevant than the properties of being central and simple.
with, say, the category of isomorphism classes of arbitrary \( k \)-algebras, which is too large to be a set (in \( \mathcal{U} \)).

The **opposite algebra** \( A^{\text{opp}} \) of \( A \) is the \( k \)-algebra with the same underlying \( k \)-vector space structure, but with multiplication \( \cdot \) defined by \( a \cdot b = ba \), the reverse of the original multiplication.

**Proposition 1.5.3.**

(i) If \( A \in \mathbb{A}z_k \), then \( A^{\text{opp}} \in \mathbb{A}z_k \).

(ii) If \( A, B \in \mathbb{A}z_k \), then \( A \otimes_k B \in \mathbb{A}z_k \).

(iii) If \( A \in \mathbb{A}z_k \), and \( L \) is a field extension of \( k \), then \( A \otimes_k L \in \mathbb{A}z_L \).

**Proof.** We leave this as Exercise [1.15]. □

**Definition 1.5.4.** A **quaternion algebra** over \( k \) is a 4-dimensional Azumaya algebra over \( k \).

**1.5.2. Splitting fields.**

**Definition 1.5.5.** An Azumaya algebra \( A \) is called **split** if it is isomorphic to \( M_n(k) \). A field \( L \) such that the \( L \)-algebra \( A \otimes_k L \) is isomorphic to \( M_n(L) \) for some \( n \geq 1 \) is called a **splitting field** for \( A \), and then one says that \( L \) splits \( A \).

**Proposition 1.5.6.** Let \( A \in \mathbb{A}z_k \). Let \( L \) be a field with \( k \subseteq L \subseteq A \). Then \( [L : k]^2 \leq [A : k] \). If equality holds, then \( L \) splits \( A \).

**Proof.** Let \( n = [L : k] \). View \( A \) as a right \( L \)-vector space; let \( r \) be its dimension. Left multiplication by any \( a \in A \) defines an \( L \)-endomorphism \( A \to A \). Thus we obtain a \( k \)-algebra homomorphism \( A \otimes_k L \to \text{End}_L A \cong M_r(L) \). Since \( A \otimes_k L \) is simple, this homomorphism is injective. Thus

\[
rn = [A : k] = [A \otimes_k L : L] \leq [M_r(L) : L] = r^2.
\]

Multiply the inequality \( rn \leq r^2 \) by \( n/r \) to obtain \( n^2 \leq rn = [A : K] \). If equality holds, then \( A \otimes_k L \to \text{End}_L A \cong M_r(L) \) must have been an isomorphism. □

**Proposition 1.5.7.** Let \( D \) be a central division algebra of degree \( r^2 \) over a field \( k \). Then \( D \) contains a degree \( r \) separable field extension \( L \supseteq k \).

**Proof.** See [GS06, Proposition 4.5.4]. □

**1.5.3. Reduced norm and reduced trace.** If \( A \in \mathbb{A}z_k \), the composition \( \nu \iota \) of an isomorphism \( \iota \): \( A \otimes_k k_s \xrightarrow{\sim} M_r(k_s) \) with the determinant map \( M_r(k_s) \to k_s \) is independent of the choice of \( \iota \), since any two \( \iota \)'s differ by an \( k_s \)-algebra automorphism of \( M_r(k_s) \), and any such automorphism is given by conjugation by an element of \( \text{GL}_r(k_s) \). (More generally, any automorphism of an Azumaya algebra over a field is inner, i.e., conjugation by a unit. Even more generally, the **Skolem–Noether theorem** [GS06, Theorem 2.7.2] states that for any two
k-algebra homomorphisms \( f, g \) from a simple \( k \)-algebra \( A \) to an Azumaya \( k \)-algebra \( B \), there exists \( b \in B^\times \) such that \( f(x) = bg(x)b^{-1} \) for all \( x \in A \).

If \( \sigma \in \mathfrak{G}_k \), then \( \sigma \) acts on \( A \otimes_k k_s \) (through the second factor) and on \( M_r(k_s) \) (entry-by-entry), so we get a \( k_s \)-algebra isomorphism \( \iota \), characterized by the fact that it makes the diagram

\[
\begin{array}{ccc}
A \otimes_k k_s & \xrightarrow{\iota} & M_r(k_s) \\
\sigma \downarrow & & \downarrow \sigma \\
A \otimes_k k_s & \xrightarrow{\sigma \iota} & M_r(k_s)
\end{array}
\]

commute. The independence of \( \iota \) on \( \iota \) implies that \( \iota := \iota_\phi \) is \( \mathfrak{G}_k \)-equivariant, meaning that \( \sigma \iota(x) = \iota(\sigma x) \) for all \( \sigma \in \mathfrak{G}_k \) and \( x \in A \otimes_k k_s \). By Galois theory, \( \iota \) restricts to a multiplicative map \( \iota := \iota_\phi : A \to k \), called the reduced norm. It restricts further to a group homomorphism \( A^\times \to k^\times \).

Similarly one can define the reduced trace \( \text{tr}_{A/k} : A \to k \), by using the trace instead of the determinant. It is a \( k \)-linear map.

**Example 1.5.8.** Let \( k = \mathbb{R} \), and let \( A = \mathbb{H} \) be Hamilton's ring of quaternions, which is a 4-dimensional \( \mathbb{R} \)-algebra generated by \( i \) and \( j \) satisfying \( i^2 = -1 \), \( j^2 = -1 \), and \( ji = -ij \). There is a \( \mathbb{C} \)-algebra isomorphism \( \mathbb{H} \otimes \mathbb{C} \iso M_2(\mathbb{C}) \) sending \( \alpha \otimes 1 \) to left-multiplication-by-\( \alpha \) on the right \( \mathbb{R}(i) \)-vector space \( \mathbb{H} = \mathbb{R}(i) \oplus j\mathbb{R}(i) \) with basis \( 1, j \). Explicitly, we have

\[
\begin{align*}
1 \otimes 1 & \mapsto \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \\
i \otimes 1 & \mapsto \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix} \\
 j \otimes 1 & \mapsto \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \\
i j \otimes 1 & \mapsto \begin{pmatrix} 0 & -i \\ -i & 0 \end{pmatrix}.
\end{align*}
\]

If \( \alpha = a + bi + cj + dij \), where \( a, b, c, d \in \mathbb{R} \), then

\[
\begin{align*}
\text{nr}_{\mathbb{H}/\mathbb{R}}(\alpha) &= \det \begin{pmatrix} a+bi & -c-di \\ c-di & a-bi \end{pmatrix} = a^2 + b^2 + c^2 + d^2 \\
\text{tr}_{\mathbb{H}/\mathbb{R}}(\alpha) &= \text{tr} \begin{pmatrix} a+bi & -c-di \\ c-di & a-bi \end{pmatrix} = 2a.
\end{align*}
\]
1.5.4. Definition of the Brauer group. Call elements \(A, B \in \text{Az}_k\) similar (or Brauer equivalent), and write \(A \sim B\), if either of the following equivalent conditions holds:

1. There exist \(m, n \geq 1\) and a division algebra \(D \in \text{Az}_k\) such that \(A \simeq M_m(D)\) and \(B \simeq M_n(D)\) as \(k\)-algebras.
2. There exist \(m, n \geq 1\) such that \(M_n(A) \simeq M_m(B)\) as \(k\)-algebras.

Define \(\text{Br}k\) as the set \(\text{Az}_k / \sim\) of similarity classes. It turns out that the operations \((A, B) \mapsto A \otimes_k B\) and \(A \mapsto A^{\text{opp}}\) on \(\text{Az}_k\) induce the multiplication and inverse maps for a group structure on \(\text{Br}k\). The abelian group \(\text{Br}k\) is called the Brauer group of \(k\). (Equivalently, but slightly less elegantly, one can define \(\text{Br}k\) as the set of isomorphism classes of finite-dimensional central division algebras over \(k\), and define the product of \(D\) and \(D'\) to be the division algebra \(D''\) such that \(D \otimes_k D' \simeq M_n(D'')\) for some \(n \geq 1\).)

If \(L\) is a field extension of \(k\), then \(A \mapsto A \otimes_k L\) induces a group homomorphism \(\text{Br}k \to \text{Br}L\). In fact, \(\text{Br}\) is a covariant functor from fields to abelian groups.

1.5.5. Cohomological interpretation of the Brauer group.

Proposition 1.5.9. For each \(r \geq 1\), there is a natural injection

\[
\frac{\{\text{Azumaya}\ k\text{-algebras of dimension } r^2\}}{k\text{-isomorphism}} \hookrightarrow H^1(\mathfrak{G}_k, \text{PGL}_r(k_s)).
\]

Proof. Let \(A \in \text{Az}_k\) be such that \([A : k] = r^2\). Choose a \(k_s\)-algebra isomorphism \(\phi: M_r(k_s) \cong A \otimes_k k_s\). As in Section 1.5.3, \(\mathfrak{G}_k\) acts on such isomorphisms. Define

\[
\xi_\sigma := \phi^{-1}(\sigma \phi) \in \text{Aut}_{k_s}\text{-algebras}(M_r(k_s)) \simeq \text{PGL}_r(k_s);
\]

the last isomorphism is due to the fact that every automorphism of a matrix algebra is inner. If \(\sigma, \tau \in \mathfrak{G}_k\), then

\[
\xi_{\sigma \tau} = \phi^{-1}(\sigma \tau \phi) = \phi^{-1}(\sigma \phi) (\xi_{\sigma \tau}) = \phi^{-1}(\sigma \phi) \cdot (\xi_{\sigma}) \cdot (\xi_{\tau}) = \xi_{\sigma} \cdot \xi_{\tau}.
\]

In other words, \(\xi\) is a 1-cocycle. Changing \(\phi\) (i.e., composing \(\phi\) with an automorphism of \(M_r(k_s)\)) changes \(\xi\) to a cohomologous cocycle, so we get an element of \(H^1(\mathfrak{G}_k, \text{PGL}_r(k_s))\) depending only on \(A\).

Finally, we must prove that the map just defined is injective. Suppose that \(A, B \in \text{Az}_k\) satisfy \([A : k] = [B : k] = r^2\), and that choices of \(\phi: M_r(k_s) \cong A \otimes_k k_s\) and \(\psi: M_r(k_s) \cong B \otimes_k k_s\) give rise to cohomologous cocycles. Then, after changing \(\psi\), the cocycles become equal: \(\phi^{-1}(\sigma \phi) = \psi^{-1}(\sigma \psi)\) for all \(\sigma \in \mathfrak{G}_k\). Rewriting this as \(\psi \phi^{-1} = (\psi \phi^{-1})^\sigma\) shows that the \(k_s\)-algebra isomorphism \(\psi \phi^{-1}: A \otimes_k k_s \cong B \otimes_k k_s\) restricts to a \(k\)-algebra isomorphism \(A \cong B\). \(\square\)
Remark 1.5.10. In fact, the injection of Proposition 1.5.9 is a bijection. This is an elementary special case of descent theory, Theorem 4.5.2 in particular: an Azumaya algebra of dimension $r^2$ is the same thing as a twist of the matrix algebra $M_r(k)$.

Taking cohomology of the short exact sequence of $G_k$-modules

$$1 \to k_s^\times \to GL_r(k_s) \to PGL_r(k_s) \to 1$$

and applying Proposition 1.3.15(iii) gives a map of pointed sets

$$(1.5.11) \quad H^1(G_k, PGL_r(k_s)) \to H^2(G_k, k_s^\times),$$

The latter is denoted $H^2(k, G_m)$. Composing Proposition 1.5.9 with (1.5.11) lets us associate to each $A \in \text{Az}_k$ an element $[A] \in H^2(k, G_m)$.

Theorem 1.5.12. The map taking each $A \in \text{Az}_k$ to the associated element of $H^2(k, G_m)$ induces an isomorphism of abelian groups $\text{Br} k \to H^2(k, G_m)$.

Proof. See Chapter X, §5, of [Ser79].

Proposition 1.5.13. Let $k$ be a field.

(i) $H^1(k, \mu_n) \simeq k^\times/k^{xn}$ if $(\text{char } k) \nmid n$.
(ii) $H^2(k, \mu_n) \simeq (\text{Br } k)[n]$ if $(\text{char } k) \nmid n$.
(iii) For any Galois extension $L/k$ of fields, $H^2(\text{Gal}(L/k), L^\times) \simeq \ker (\text{Br } k \to \text{Br } L)$.

Proof.

(i) Take the long exact sequence of cohomology associated to

$$0 \to \mu_n \to k_s^\times \to k_s^\times \to 0$$

and apply Hilbert’s theorem 90.

(ii) Same proof as (i), but using Theorem 1.5.12.

(iii) Since $H^1(L, G_m) = 0$ by (ii), we get an inflation-restriction sequence for $H^2$

$$0 \to H^2(\text{Gal}(L/k), L^\times) \xrightarrow{\text{inf}} H^2(k, G_m) \xrightarrow{\text{res}} H^2(L, G_m).$$

(To construct this sequence and prove it is exact, one can either use cocycles explicitly, or deduce it from the Hochschild–Serre spectral sequence: see Corollary 6.7.4) Now apply Theorem 1.5.12 to the two groups on the right.

Remark 1.5.14. Parts (i) and (iii) can be generalized to the case where $\text{char } k \mid n$, but in place of Galois cohomology one must use the fppf cohomology to be introduced in Section 6.4.1.
1.5.6. Period and index.

**Definition 1.5.15.** The index of a finite-dimensional central division algebra $D$ over $k$ is $\sqrt{|D:k|}$, which is a positive integer by Proposition [1.5.2](#). More generally, the index of $M_r(D)$ is defined to be the index of $D$. This makes index a well-defined function $\text{Br} \, k \to \mathbb{Z}_{>0}$.

**Definition 1.5.16.** The period of an element $A \in \mathbb{A}Z \, k$ (or of its class $[A]$) is the order of $[A]$ in $\text{Br} \, k$.

**Proposition 1.5.17.** If $A$ is an Azumaya algebra of dimension $r^2$ over $k$, then $r[A] = 0$ in $\text{Br} \, k$. In other words, period divides index.

**Proof.** Write $A \simeq M_n(D)$ for a central division algebra $D$ over $k$. Then $|D:k|$ divides $[A:k]$, and $A$ and $D$ have the same period and the same index, so we may reduce to the case that $A$ is a central division algebra $D$. By Proposition [1.5.7](#), $D$ contains a degree $r$ separable field extension $L \supseteq k$. By Proposition [1.5.6](#), $L$ is a splitting field for $D$. Then $[D] \in \ker(\text{Br} \, k \to \text{Br} \, L)$. By Exercise [1.19](#), we have $r[D] = 0$.

For a different proof, see the proof of Theorem [6.6.17](#). \qed

**Remark 1.5.18.** If $k$ is a local or global field, every element of $\text{Br} \, k$ has period equals index (Theorems [1.5.34](#) and [1.5.36](#)), so the injection $H^1(\mathcal{O}_k, \text{PGL}_r(k)) \to (\text{Br} \, k)[r]$ is a bijection for each $r \geq 1$.

**Warning 1.5.19.** For general $k$, the image of $H^1(\mathcal{O}_k, \text{PGL}_r(k)) \to \text{Br} \, k$ need not even be a subgroup! For example, if $r = 2$, the image consists of the classes of quaternion algebras, but a tensor product of quaternion algebras can be a division algebra, in which case it is not similar to another quaternion algebra. Explicitly, if $k_0$ is a field of characteristic not 2, and $k = k_0(t_1, t_2, t_3, t_4)$, then the $k$-algebra $(t_1, t_2) \otimes (t_3, t_4)$ (in the notation of Section [1.5.7.4](#)) turns out to be a division algebra \cite{GS06} Example 1.5.7]. Its period is 2, but its index is 4.

1.5.7. Cyclic algebras.

1.5.7.1. **Cyclic algebras from cyclic fields.** Let $L/k$ be a degree $n$ cyclic extension of fields. Given $a \in k^\times$ and a generator $\sigma$ of $\text{Gal}(L/k)$, we construct a $k$-algebra as follows. Let $L[x]_\sigma$ denote the “twisted polynomial ring” having the same additive group as $L[x]$, but whose multiplication is defined so that $x\ell = (\sigma \ell) x$. Let $A$ be the quotient of $L[x]_\sigma$ by the ideal generated by the central element $x^n - a$. Then one can show that $A \in \mathbb{A}Z \, k$: see Exercise [1.20](#).

1.5.7.2. **Cyclic algebras from étale algebras.** One can generalize the construction by allowing $L$ to be only an étale $k$-algebra instead of a field extension.

Start with an element $a \in k^\times$ and a continuous homomorphism $\chi : \mathcal{O}_k \to \mathbb{Z}/n\mathbb{Z}$. Let $S = \mathbb{Z}/n\mathbb{Z}$, and let each $g \in \mathcal{O}_k$ act on $S$ by $s \mapsto s + \chi(g)$. By Theorem [1.3.2](#), $S$ corresponds to an étale $k$-algebra $L$, and the automorphism $s \mapsto s + 1$ of the $\mathcal{O}_k$-set $S$ corresponds to a
The $k$-algebra automorphism $\sigma$ of $L$. As in Section 1.5.1 form $A := L[x]_\sigma/(x^n - a)$. Again it turns out that $A \in \text{Az}_k$: see Exercise 1.20.

**Definition 1.5.20.** The $k$-algebra $A$ just constructed, or its class in $\text{Br } k$, is denoted $(a, \chi)$. Such an algebra is called a cyclic algebra.

One advantage of allowing $L$ to be an étale algebra instead of insisting on a field is that now if $A$ is a cyclic algebra over $k$, and $k' \supset k$ is a field extension, then $A \otimes_k k'$ is a cyclic algebra over $k'$.

**1.5.7.3. First cohomological interpretation.** The construction of $(a, \chi)$ can also be understood cohomologically. For simplicity, suppose that $\chi : \mathfrak{G}_k \to \mathbb{Z}/n\mathbb{Z}$ is surjective, or equivalently that $L$ is a field. Let $G = \text{Gal}(L/k)$, so $\chi$ induces $\chi : G \to \mathbb{Z}/n\mathbb{Z}$. By definition of Tate cohomology, $\hat{H}^0(G, L^\times) = k^\times/N_{L/k}(L^\times)$, and we may consider the image of $a$ in this group. The generator $\sigma = \chi^{-1}(1)$ of $G$ determines a generator $u$ of the cyclic group $\hat{H}^2(G, \mathbb{Z})$, and “cup product with $u$” gives an isomorphism $\hat{H}^0(G, L^\times) \cong \hat{H}^2(G, L^\times)$, §8, Theorem 5]. The latter is isomorphic to $\ker(Br k \to Br L)$ by Proposition 1.3.15 [iii], and one can show that the composition

$$(1.5.21) \quad k^\times \to \hat{H}^0(G, L^\times) \cong \hat{H}^2(G, L^\times) \hookrightarrow \text{Br } k,$$

maps any $a \in k^\times$ to the class of the cyclic algebra $(a, \chi)$, maybe with a sign error, depending on the definition of $u$. This has several consequences:

**Proposition 1.5.22.** Let $L$ and $\chi$ be as above. Suppose that $A \in \text{Az}_k$ and that $[A : k] = [L : k]^2$. Then $A$ is split by $L$ if and only if $A \cong (a, \chi)$ for some $a \in k^\times$.

**Proof.** By (1.5.21), $A$ is split by $L$ if and only if it is similar to $(a, \chi)$ for some $a \in k^\times$. But $A$ and $(a, \chi)$ have the same dimension, so similar is equivalent to isomorphic.

**Proposition 1.5.23.** Let $L$ and $\chi$ be as above. For $a \in k^\times$, the $k$-algebra $(a, \chi)$ is split if and only if $a \in N_{L/k}(L^\times)$.

**Proof.** The kernel of the composite homomorphism in (1.5.21) equals the kernel of the first homomorphism, which is $N_{L/k}(L^\times)$.

**1.5.7.4. Second cohomological interpretation.** We can give another cohomological interpretation of $(a, \chi)$, at least when $(\text{char } k) \nmid n$. The element $a$ can be mapped to an element of $k^\times/k^\times n \cong H^1(k, \mu_n)$. On the other hand, $\chi \in \text{Hom}(\mathfrak{G}_k, \mathbb{Z}/n\mathbb{Z}) \cong H^1(k, \mathbb{Z}/n\mathbb{Z})$. Under the cup product

$H^1(k, \mu_n) \times H^1(k, \mathbb{Z}/n\mathbb{Z}) \to H^2(k, \mu_n) \cong (Br k)[n]

a$ and $\chi$ pair to give an element of $(Br k)[n]$, which turns out to be the class of the cyclic algebra $(a, \chi)$, at least up to a sign.
Suppose now that \((\text{char } k) \nmid n\) and that \(k\) contains a primitive \(n^{\text{th}}\) root of unity, \(\zeta\). Then \(\zeta\) determines an isomorphism \(\mathbb{Z}/n\mathbb{Z} \rightarrow \mu_n\) of \(G_k\)-modules, so we get an isomorphism \(H^1(k, \mathbb{Z}/n\mathbb{Z}) \simeq H^1(k, \mu_n) \simeq k^\times/k^{\times n}\). Now given \(a, b \in k^\times\), we can take the cup product of their images under

\[
H^1(k, \mathbb{Z}/n\mathbb{Z}) \times H^1(k, \mathbb{Z}/n\mathbb{Z}) \rightarrow H^2(k, \mu_n) \simeq (\text{Br } k)[n]
\]

to get an element of \(\text{Br } k\). Alternatively, from \(a\) and the étale \(k\)-algebra \(L = k[t]/(t^n - b)\) equipped with the automorphism \(\sigma\) mapping \(t\) to \(\zeta t\), one can construct a cyclic algebra \((a, b)_\zeta \in \mathbb{A}z_k\) representing the element of \(\text{Br } k\) defined in the previous sentence. When \(n = 2\), one writes simply \((a, b)\) for \((a, b)_{-1}\).

Remark 1.5.24. Exercise 1.23 shows that every quaternion algebra is cyclic. In particular, if \(\text{char } k \neq 2\), then every quaternion algebra \(D\) over \(k\) is of the form \((a, b)\) for some \(a, b \in k^\times\): this algebra has a \(k\)-basis \(1, i, j, ij\) where \(i^2 = a, j^2 = b,\) and \(ji = -ij\). (The elements \(a\) and \(b\) are not uniquely determined by \(D\)).

1.5.8. Connections with the \(C_r\) property and cohomological dimension.

Proposition 1.5.25. Let \(k\) be a field. The following eight conditions are equivalent:

(i) \(\text{cd } k \leq 1,\) and if \(\text{char } k = p > 0,\) then \((\text{Br } K)[p^\infty] = 0\) for every algebraic extension \(K\) of \(k\).

(ii) \(\text{Br } K = 0\) for every algebraic extension \(K\) of \(k\).

(iii) If \(K\) is an algebraic extension of \(k\), and \(L/K\) is a finite Galois extension, then \(H^q(\text{Gal}(L/K), L^\times) = 0\) for all \(q \geq 1\).

(iv) If \(K\) is an algebraic extension of \(k\), and \(L/K\) is a finite Galois extension, then \(N_{L/K}: L^\times \rightarrow K^\times\) is surjective.

(i'), (ii'), (iii'), (iv'): Same as [(i), (ii), (iii), (iv)], but restricted to extensions \(K\) that are finite and separable over \(k\).

Proof. See Proposition 5 in II.§3.1 of [Ser02].

Definition 1.5.26. A field \(k\) is said to be of dimension \(\leq 1\) if it satisfies the equivalent conditions of Proposition 1.5.25. We then write \(\text{dim } k \leq 1\).

Warning 1.5.27. This has nothing to do with the Krull dimension, which is 0 for any field \(k\).

Proposition 1.5.28. If \(k\) is \(C_1\), then \(\text{Br } k = 0\).

Proof. Let \(D\) be a finite-dimensional central division algebra over \(k\), so \([D : k] = r^2\) for some \(r \geq 1\). An associated reduced norm form is of degree \(r\) in \(r^2\) variables, and has
no nontrivial zero. This contradicts the $C_1$ property unless $r = 1$. This holds for all $D$, so $\text{Br} \ k = 0$. \hfill \Box

**Corollary 1.5.29.** If $k$ is $C_1$, then $k$ is of dimension $\leq 1$.

**Proof.** We check condition (ii) in the definition of “dimension $\leq 1$.” Let $k$ be $C_1$. Any algebraic extension $K/k$ is $C_1$ by Theorem 1.2.7(i), and hence satisfies $\text{Br} \ K = 0$ by Proposition 1.5.28. \hfill \Box

**Warning 1.5.30.** The converse to Corollary 1.5.29 is false. See p. 80 of [Ser02] for a counterexample, due to Ax [Ax65]. In fact, Ax finds a field of dimension $\leq 1$ that is not $C_r$ for any $r$.

**Remark 1.5.31.** Serre wrote in [Ser02, p. 88] that it is probable that for all $r \geq 0$, all $C_r$ fields satisfy $\text{cd} \ k \leq r$. This is true for $r \leq 2$ (the $r = 2$ case is a theorem of Merkurjev and Suslin). Moreover, [OVV07] shows that $C_r$ fields of characteristic 0 satisfy $\text{cd}_2 \ k \leq r$.

**1.5.9. Examples.**

**Theorem 1.5.32 (Wedderburn).** If $k$ is a finite field, then $\text{Br} \ k = 0$.

**Proof.** The Chevalley–Warning theorem says that $k$ is $C_1$. Apply Proposition 1.5.28. \hfill \Box

**Theorem 1.5.33 (original form of Tsen’s theorem).** If $k$ is a field of transcendence degree 1 over an algebraically closed field, then $\text{Br} \ k = 0$.

**Proof.** Again $k$ is $C_1$, so apply Proposition 1.5.28. \hfill \Box

**Theorem 1.5.34 (Brauer group of a local field).** Suppose that $k$ is a local field.

(i) There is an injection $\text{inv}: \text{Br} \ k \to \mathbb{Q}/\mathbb{Z}$, whose image is

$$
\begin{cases}
\frac{1}{2}\mathbb{Z}/\mathbb{Z} & \text{if } k = \mathbb{R}, \\
0 & \text{if } k = \mathbb{C}, \\
\mathbb{Q}/\mathbb{Z} & \text{if } k \text{ is nonarchimedean}.
\end{cases}
$$

(ii) If $L$ is a finite extension of $k$, then the diagram

$$
\begin{array}{ccc}
\text{Br} \ k & \xrightarrow{\text{inv}} & \mathbb{Q}/\mathbb{Z} \\
\downarrow & & \downarrow_{[L:k]} \\
\text{Br} \ L & \xrightarrow{\text{inv}} & \mathbb{Q}/\mathbb{Z}
\end{array}
$$

commutes.

(iii) Every Azumaya algebra over $k$ is cyclic.

(iv) Every element of $\text{Br} \ k$ has period equal to index.
Proof. The cases where $k$ is $\mathbb{R}$ or $\mathbb{C}$ are easy, so assume that $k$ is nonarchimedean.

(i) If $F$ is the residue field of $k$, one shows that $Br k \simeq H^1(F, \mathbb{Q}/\mathbb{Z}) \simeq \mathbb{Q}/\mathbb{Z}$: see the bottom of page 130 in [Ser67].

(ii) See [Ser67, Theorem 3].

(iii) Let $m/n \in \mathbb{Q}$ be a rational number in lowest terms, with $n \geq 1$. Let $L$ be the degree $n$ unramified extension of $k$. Let $\sigma \in \text{Gal}(L/k)$ be the Frobenius automorphism. Choose $a \in k^\times$ of valuation $m$. By [Ser67, p. 138], the cyclic algebra $A := L[x]/(x^n - a)$ is a division algebra with $\text{inv} A = m/n \in \mathbb{Q}/\mathbb{Z}$. These $m/n$ cover all possible invariants, so every Azumaya algebra is a matrix algebra over one of these and is cyclic by Exercise 1.24.

(iv) Each $A$ in (iii) has period equal to index. □

If $L/k$ is a finite extension of global fields, we write $w \mid v$ to mean that the place $w$ of $L$ lies over the place $v$ of $k$; in this case, the inclusion $k_v \hookrightarrow L_w$ gives rise to a homomorphism $Br k_v \rightarrow Br L_w$.

Theorem 1.5.36 (Brauer group of a global field). Suppose that $k$ is a global field. For each place $v$ of $k$, let $k_v$ be the completion of $k$ at $v$, and let $\text{inv}_v : Br k_v \hookrightarrow \mathbb{Q}/\mathbb{Z}$ be the injection associated to the local field $k_v$.

(i) Then the sequence

$$0 \rightarrow Br k \rightarrow \bigoplus_v Br k_v \stackrel{\sum \text{inv}_v}{\rightarrow} \mathbb{Q}/\mathbb{Z} \rightarrow 0$$

is exact.

(ii) If $L$ is a finite extension of $k$, then the diagram

$$0 \rightarrow Br k \rightarrow \bigoplus_v Br k_v \stackrel{\sum \text{inv}_v}{\rightarrow} \mathbb{Q}/\mathbb{Z} \rightarrow 0$$

$$\downarrow \quad \downarrow \quad \downarrow [L:k]$$

$$0 \rightarrow Br L \rightarrow \bigoplus_v \bigoplus_w Br L_{wv} \stackrel{\sum \text{inv}_w}{\rightarrow} \mathbb{Q}/\mathbb{Z} \rightarrow 0$$

commutes.

(iii) Every Azumaya algebra over $k$ is cyclic.

(iv) Every element of $Br k$ has period equal to index.

Proof.

(i) This follows from results in [Tat67]: see diagram (9) in Section 11.2, together with Proposition 7.3(b) and Section 11.2(bis).

(ii) Cf. diagram (7) in Section 11.2 of [Tat67]. The commutativity of the left square follows from functoriality of $Br$. The commutativity of the right square follows from the identity $\sum_{w|v}[L_w : k_v] = [L : k]$. 24
(iii) By Exercise 1.24 it suffices to consider a central division algebra \( A \) over \( k \). Let \( n \) be the order of \( [A] \in \text{Br} k \). Let \( S \) be the finite set of places \( v \) such that \( \text{inv}_v A \neq 0 \). The Grunwald–Wang theorem produces a degree \( n \) cyclic extension \( L/k \) such that each local degree \( [L_w : k_v] \) above a place \( v \in S \) is \( n \) if \( v \) is nonarchimedean, and \( 2 \) if \( v \) is real: see [AT67, Chapter 10, Theorem 5]. By Theorem 1.5.34(ii), all local invariants of \( A \otimes_k L \) are \( 0 \). By the injectivity of the first homomorphism in (i), the extension \( L \) splits \( A \). Now

\[
(1.5.37) \quad n = \text{(period of } A) \leq \text{(index of } A) \leq [L : k] = n,
\]

so equality holds everywhere. In particular, \( [A : k] = [L : k]^2 \), so \( A \) is cyclic by Proposition 1.5.22.

(iv) This follows from the equality in (1.5.37).

Theorems 1.5.34 and 1.5.36 are by-products of the cohomological proofs of local and global class field theory; it seems that they cannot be proved without effectively doing a large part of the work towards class field theory.

**Theorem 1.5.38** (Faddeev). Suppose that \( k \) is any field, and \( K = k(t) \). There is an exact sequence

\[
0 \rightarrow \text{Br} k \rightarrow \text{Br} K \xrightarrow{\text{res}} \bigoplus_f H^1(k[t]/(f), \mathbb{Q}/\mathbb{Z}) \rightarrow 0,
\]

where \( f \) ranges over all monic irreducible polynomials in \( k[t] \), with the caveat that one must exclude the \( p \)-primary parts if \( k \) is imperfect of characteristic \( p \).

**Proof.** See [Ser02, II.Appendix.§5] and [GS06, 6.4.5] for a proof and a generalization.

**Remark 1.5.39.** It is perhaps more natural to let the direct sum range over all closed points of \( \mathbb{P}^1_k \), in which case it contains one more summand, so one must add a new term \( H^1(k, \mathbb{Q}/\mathbb{Z}) \) to the end, to get a four-term exact sequence.

Theorem 1.5.38 is related to Theorems 6.8.3 and 6.9.7.

**Exercises**

1.1. (a) Prove that an algebraic extension of a separably closed field is separably closed.

(b) Prove that an algebraic extension of a perfect field is perfect.

(c) Let \( k \) be a field. Prove that \( \overline{k} = (k_s)^{\text{perf}} = (k^{\text{perf}})_s = k^{\text{perf}} \cdot k_s \). (The last expression denotes the subfield of \( \overline{k} \) generated by \( k^{\text{perf}} \) and \( k_s \).)  

1.2. Let \( k \) be a global or local field. Prove that \( k \) is perfect if and only if char \( k = 0 \).

1.3. For which \( r \in \mathbb{R}_{\geq 0} \) is \( C_r \) equivalent to being algebraically closed?

1.4. (a) For each finite field \( \mathbb{F}_q \) and nonnegative integer \( n \), evaluate \( \sum_{a \in \mathbb{F}_q} a^n \).
(b) Prove the Chevalley–Warning theorem, that every finite field $\mathbb{F}_q$ is $C_1$. (Hint: given a homogeneous polynomial $f \in \mathbb{F}_q[x_1, \ldots, x_n]$ of degree $d < n$, evaluate
\[ \sum_{(a_1, \ldots, a_n) \in (\mathbb{F}_q)^n} (1 - f(a_1, \ldots, a_n)^q) \in \mathbb{F}_q \]
in two different ways.)

(c) Using a similar method, prove directly that $\mathbb{F}_q$ is $C'_1$, without using the paragraph following Question 1.2.11.

1.5. Let $L/k$ be a finite extension of fields, and let $r \in \mathbb{R}_{\geq 0}$. If $L$ is $C_r$, must $k$ be $C_r$?

1.6. Let $k$ be a $C_1$ field, and let $L$ be a finite extension. Prove that the norm homomorphism $N_{L/k}: L^\times \to k^\times$ is surjective.

1.7. Let $k$ be a field.
   (a) Prove that \{ $r \in \mathbb{R}_{\geq 0} : k$ is $C_r$ \} has a minimum, if it is nonempty.
   (b) Let $r(k)$ denote the real number in part (1.7a), if it exists. Let $k(t)$ be the rational function field over $k$. Prove that $r(k(t)) = r(k) + 1$, in the sense that if one side is defined, then so is the other, and then they are equal.

1.8. Let $k_v$ be a nonarchimedean completion of a number field $k$, and let $r \in \mathbb{R}_{\geq 0}$. Assuming (as is true) that $k_v$ is not $C_r$, prove that $k$ is not $C_r$.

1.9. Let $L/k$ be a finite Galois extension with Galois group $G$. Let $r \in \mathbb{Z}_{\geq 0}$. Given a 1-cochain (i.e., function) $\xi: G \to GL_r(L)$, let $W_\xi$ be $L^r$ equipped with the function $G \times L^r \to L^r$ sending $(\sigma, w)$ to $\xi_\sigma(\sigma w)$.
   (a) Prove that this describes a semilinear $G$-action (i.e., the group action axiom $(\sigma \tau) * w = \sigma * (\tau * w)$ is satisfied) if and only if $\xi$ is a 1-cocycle.
   (b) Prove that given two 1-cocycles $\xi$ and $\xi'$, we have $W_\xi \simeq W_{\xi'}$ as $L$-vector spaces with semilinear $G$-action if and only if $\xi$ and $\xi'$ are cohomologous.

1.10. Let $L/k$ be a finite Galois extension of fields. Suppose that Gal($L/k$) is cyclic, generated by $\sigma$. The original Hilbert theorem 90 proved by Hilbert stated that if $a \in L^\times$ satisfies $N_{L/k}(a) = 1$, then there exists $b \in L^\times$ such that $a = \frac{\sigma b}{b}$. Explain why Proposition 1.3.15(ii) is a generalization of this.

1.11. Use the original Hilbert theorem 90 to prove that if $x, y \in \mathbb{Q}$ satisfy $x^2 + y^2 = 1$, then there exist $u, v \in \mathbb{Q}$ not both 0 such that
\[ (x, y) = \left( \frac{u^2 - v^2}{u^2 + v^2}, \frac{2uv}{u^2 + v^2} \right). \]
(This can be proved also in more elementary ways.)

1.12. Let $A$ be a torsion abelian group. Prove that $A \simeq \bigoplus_p A[p^\infty]$, where the direct sum is over all prime numbers $p$. 

26
1.13. Let $G$ be a profinite group, let $p$ be a prime, and let $n \in \mathbb{N}$. Prove that $\text{cd}_p(G) \leq n$ if and only if $H^{n+1}(G, A) = 0$ for every simple $G$-module $A$ killed by $p$. (A $G$-module $A$ is simple if $A \neq 0$ and the only $G$-submodules of $A$ are $0$ and $A$.)

1.14. (Equivalence of definitions of Azumaya algebra) Prove the implications (i) $\iff$ (ii) $\Rightarrow$ (iii) $\Rightarrow$ (iv) and the implication (v) $\Rightarrow$ (iv) of Proposition 1.5.2.

1.15. (Properties of Azumaya algebras) Prove Proposition 1.5.3.

1.16. If $A$ is a finite-dimensional algebra over a field $k$, the usual norm $N_{A/k} : A \to k$ maps $a$ to the determinant of the $k$-linear endomorphism of $A$ given by $x \mapsto ax$. For $A \in \text{Az}_k$, what is the relationship between $N_{A/k}$ and the reduced norm $\text{nr}_{A/k}$?

1.17. Let $\{K_\alpha\}$ be a directed system of fields, and let $K = \lim\limits_{\longrightarrow} K_\alpha$ be the direct limit. Prove that $\text{Br} K = \lim\limits_{\longrightarrow} \text{Br} K_\alpha$.

1.18. Prove that if $L$ is an extension of $k$, the diagram

$$
\begin{array}{ccc}
\text{Br} k & \longrightarrow & H^2(k, \mathbb{G}_m) \\
\downarrow & & \downarrow \\
\text{Br} L & \longrightarrow & H^2(L, \mathbb{G}_m)
\end{array}
$$

commutes.

1.19. Let $L/k$ be a field extension of degree $n$. Prove that the kernel of $\text{Br} k \to \text{Br} L$ is killed by $n$. (Hint: If $L/k$ is separable, use the identity $\text{Cor} \circ \text{Res} = [L : k]$ of [AW67, Section 6, Proposition 8].)

1.20. Let $(a, \chi)$ be a cyclic algebra over a field $k$. Prove that $(a, \chi) \in \text{Az}_k$.

1.21. Let $k$ be a field. Suppose that $\text{char} k \nmid n$ and that $k$ contains a primitive $n$th root of unity $\zeta$. Show that

$$
\frac{k^\times}{k^\times n} \times \frac{k^\times}{k^\times n} \longrightarrow (\text{Br} k)[n]
$$

$$
(a, b) \mapsto (a, b)_\zeta
$$

is an antisymmetric pairing; that is, $(b, a)_\zeta = -(a, b)_\zeta$ in $\text{Br} k$.

1.22. Let $D$ be a quaternion algebra over a field $k$. Let $\text{tr}$ and $\text{nr}$ denote the reduced trace and reduced norm for $D/k$. Prove that for $\alpha \in D$ one can define $\bar{\alpha} \in D$ such that the following hold:

(a) The map

$$
D \to D^{\text{opp}}
$$

$$
\alpha \mapsto \bar{\alpha}
$$

is a $k$-algebra isomorphism.

(b) $\bar{\bar{\alpha}} = \alpha$.

(c) $\text{tr}(\alpha) = \text{tr}(\bar{\alpha}) = \alpha + \bar{\alpha}$.

27
(d) \(\text{nr}(\alpha) = \text{nr}(\bar{\alpha}) = \alpha\bar{\alpha}\).

(e) If \(L\) is an étale \(k\)-subalgebra of \(D\) and \([L : k] = 2\), then the involution \(\alpha \mapsto \bar{\alpha}\) restricts to the nontrivial automorphism of \(L\) over \(k\).

1.23. Prove that every quaternion algebra over a field is a cyclic algebra.

1.24. Show that if \(A\) is a cyclic algebra over a field \(k\), then so is \(M_r(A)\) for any \(r \geq 1\).

1.25. Describe all Azumaya algebras over \(\mathbb{R}\), and show that they are all cyclic algebras.

1.26. Let \(k\) be a separably closed field that is not algebraically closed. Let \(p = \text{char} \ k\).

   (a) Prove that \(\text{Br} \ k(t) \neq 0\). Better yet, find an element of \(\text{Br} \ k(t)\) whose image in \(\text{Br} \ k((t))\) is nonzero.

   (b) Prove that every element of \(\text{Br} \ k(t)\) is killed by some power of \(p\).

1.27. (a) Let \(k\) be a global field, and let \(a \in \text{Br} \ k\). Prove that there is a root of unity \(\zeta \in \overline{k}\) such that the image of \(a\) in \(\text{Br} \ k(\zeta)\) is 0.

   (b) Let \(k\) be a global field, and let \(k^{ab}\) denote its maximal abelian extension. Prove that \(k^{ab}\) is of dimension \(\leq 1\). (So in particular, \(\text{Br} \ k^{ab} = 0\).)

1.28. Let \(k\) be a perfect field.

   (a) Prove that if \(\text{char} \ k = p > 0\), then \((\text{Br} \ k)[p] = 0\).

   (b) Prove that \(\dim k \leq 1\) if and only if \(\text{cd} \ k \leq 1\).

1.29. Let \(k\) be a field.

   (a) Show that if \(t\) is an indeterminate, the field \(k(t)\) has a nontrivial cyclic extension of degree not divisible by \(\text{char} \ k\).

   (b) Let \(k\) be a field, and let \(K\) be the purely transcendental extension \(k(t_1, \ldots, t_m)\) for some \(m \geq 2\). Use Theorem \ref{thm:1.5.38} to show that \(\text{Br} \ K\) is huge in the following sense: the cardinality of \(\text{Br} \ K\) equals the cardinality of \(K\).
CHAPTER 2

Varieties over arbitrary fields

We refer to [Har77] for definitions of standard terms regarding schemes: noetherian, connected, irreducible, reduced, integral, regular, finite type, separated, proper, projective, dimension, rational map, dominant.

**Definition 2.0.40.** If $S$ is a scheme, an $S$-scheme $(X, f)$ is a scheme $X$ equipped with a morphism of schemes $f: X \to S$. The morphism $f$ is called the **structure morphism**.

To simplify notation, we usually write $X$ instead of $(X, f)$. Sometimes it helps to think of $X \to S$ as a family of schemes, one above each point of $S$.

**Definition 2.0.41.** An $S$-morphism between $S$-schemes $(X, f)$ and $(Y, g)$ is a morphism of schemes $\phi: X \to Y$ such that

\[
\begin{array}{ccc}
X & \xrightarrow{\phi} & Y \\
\downarrow{f} & & \downarrow{g} \\
S & \xrightarrow{} & S
\end{array}
\]

commutes.

For a scheme $S$, let $\textbf{Schemes}_S$ denote the category whose objects are $S$-schemes and whose arrows are $S$-morphisms. If $X$ and $Y$ are $S$-schemes, let $\text{Hom}_S(X, Y)$ denote the set of $S$-morphisms from $X$ to $Y$.

When $R$ is a commutative ring, $R$ may be used as an abbreviation for $\text{Spec } R$; the meaning is usually clear from context. For instance, if $X$ is a scheme (over $\text{Spec } \mathbb{Z}$), then $X \times \mathbb{Q}$ means $X \times_{\text{Spec } \mathbb{Z}} \text{Spec } \mathbb{Q}$.

**2.1. Varieties**

Our definition of variety will be rather inclusive. If we want to consider a more restricted class of varieties, we can apply adjectives (such as “irreducible”) as needed.

**Definition 2.1.1.** A **variety** over a field $k$ is a separated scheme $X$ of finite type over $\text{Spec } k$.

---

\[\text{Note: This definition should read as follows: A scheme } X \text{ is integral if it is nonempty and for every nonempty open set } U \subseteq X, \text{ the ring } \mathcal{O}_X(U) \text{ is an integral domain.}\]
Warning 2.1.2. In [Har77 II.4], varieties must also be integral; we are not including this condition in the definition of variety.

Varieties over a field \( k \) may also be called \( k \)-varieties.

**Definition 2.1.3.** A curve is a variety of pure dimension 1. (Pure means that all the irreducible components have the same dimension.) A surface is a variety of pure dimension 2. A 3-fold is a variety of pure dimension 3, and so on.

### 2.2. Base extension

**Definition 2.2.1.** If \( X \) is an \( S \)-scheme, and \( S' \to S \) is a morphism, then the **base extension** \( X_{S'} \) is the \( S' \)-scheme \( X \times_S S' \). The base extension of a morphism of \( S \)-schemes \( X \to Y \) is the \( S' \)-morphism \( X_{S'} \to Y_{S'} \) induced by the universal property of the fiber product \( X \times_S S' \).

Recall some important applications of base extension:

- If \( X \) is a \( k \)-variety or \( k \)-scheme, and \( L \) is a field extension of \( k \), then \( X_L \) is the scheme defined by the same equations but considered over \( L \) instead of \( k \).
- Let \( X \) be a \( k \)-scheme and let \( \sigma \in \text{Aut} k \). Then the base extension of \( X \) by the morphism \( \sigma^* : \text{Spec} k \to \text{Spec} k \) induced by \( \sigma \) is a new \( k \)-scheme \( \sigma X \). Since \( \sigma^* \) is an isomorphism of schemes, \( \sigma X \) and \( X \) are isomorphic as abstract schemes, but generally they are not isomorphic as \( k \)-schemes. For instance, if \( X \) is an affine variety, then \( \sigma X \) can be obtained by applying \( \sigma \) to each coefficient in the equations defining \( X \).

\[
\begin{array}{c}
\sigma X \longrightarrow X \\
\downarrow \\
\text{Spec} k \longrightarrow \text{Spec} k \\
\end{array}
\]

- Let \( X \) be an \( S \)-scheme with structure morphism \( f : X \to S \). If \( U \) is an open subscheme of \( S \), then \( X_U \) is also written \( f^{-1}U \) since its underlying topological space is \( f^{-1}U \). The same applies to closed subschemes of \( S \).
- Let \( s \in S \). Let \( k(s) \) be the residue field of the local ring \( \mathcal{O}_{S,s} \). The scheme \( S' := \text{Spec} k(s) \) has a natural morphism to \( S \). The resulting scheme \( X_{S'} \) may also be written \( X_s \) or \( f^{-1}(s) \) since its underlying topological space is \( f^{-1}(s) \). It is called the **fiber** of \( X \to S \) above \( s \) [Har77, p. 89]. If \( p \) is a prime ideal of a ring \( A \), and \( X \) is an \( A \)-scheme, then the fiber \( X_p \) is also called the **reduction of** \( X \) **modulo** \( p \).

**Example 2.2.2 (Varieties that become isomorphic only after base field extension).** Let \( X \) be the affine plane curve over \( \mathbb{Q} \) defined by the equation \( x^2 + y^2 = 1 \); that is, \( X := \text{Spec} \mathbb{Q}[x,y]/(x^2 + y^2 - 1) \). Let \( Y \) be the plane curve over \( \mathbb{Q} \) defined by \( x^2 + y^2 = -1 \). If
$L = \mathbb{Q}(i)$, then $X_L \simeq Y_L$ as $L$-varieties. But $X \not\cong Y$, because $\mathbb{Q}[x, y]/(x^2 + y^2 - 1)$ admits a $\mathbb{Q}$-algebra homomorphism to $\mathbb{Q}$ while $\mathbb{Q}[x, y]/(x^2 + y^2 + 1)$ does not.

Most properties of morphisms are preserved by base extension. Often they are defined expressly so as to make this so.

**Theorem 2.2.3.** Let “blah” denote a property for which a positive answer is listed in the “base extension” column of Table 1. If $X \to S$ is blah, then $X_{S'} \to S'$ is blah for any morphism $S' \to S$.

![Diagram](image)

The following properties of a variety can be lost by base extension of the ground field: integral, connected, irreducible, reduced, and regular. This motivates some more definitions.

**Definition 2.2.4.** Let $X$ be a scheme over a field $k$. Then $X$ is said to be **geometrically integral** if and only if $X_k$ is integral. Define **geometrically connected**, **geometrically irreducible**, **geometrically reduced**, and **geometrically regular** similarly.

**Remark 2.2.5.** When one speaks of the geometry of $X$, as opposed to the arithmetic of $X$, one is usually referring to properties of $X_k$.

**Example 2.2.6.** Let $X$ be the affine plane curve $x^2 - 2y^2 = 0$ over $\mathbb{Q}$. Then $X$ is irreducible. (In fact, $X$ is integral, since $x^2 - 2y^2$ is an irreducible element of the unique factorization domain $\mathbb{Q}[x, y]$.) But $X$ is not geometrically irreducible, since $X_{\overline{\mathbb{Q}}}$ is the union of the closed subvarieties defined by $x + \sqrt{2}y = 0$ and $x - \sqrt{2}y = 0$.

**Example 2.2.7.** Let $X$ be the curve $y^2 = 2$ over $\mathbb{Q}$ in the $(x, y)$-plane. Then $X$ is connected, but not geometrically connected.

**Example 2.2.8.** Let $k$ be the imperfect field $\mathbb{F}_p(t)$, where $t$ is an indeterminate. Let $X$ be the affine plane curve $y^p = tx^p$ over $k$. Then $X$ is reduced, but not geometrically reduced.

**Example 2.2.9.** Let $L$ be a finite extension of a field $k$. View $X = \text{Spec} L$ as a $k$-variety. Then $X$ is integral. But if the separable degree of $L$ over $k$ is greater than 1 (that is, $L$ is not purely inseparable over $k$), then $X$ is neither geometrically connected nor geometrically irreducible. And if the inseparable degree of $L$ over $k$ is greater than 1 (that is, $L$ is not separable over $k$), then $X$ is not geometrically reduced, and hence not geometrically regular.

**Example 2.2.10.** Regular local rings are reduced, so regular implies reduced, and geometrically regular implies geometrically reduced. So if $L$ is a finite inseparable extension of a field $k$, then $\text{Spec} L$ is a regular $k$-variety that is not geometrically regular.
For another example of a $k$-variety that is regular but not geometrically regular, see Example 3.5.23. That example is also geometrically integral.

### 2.2.1. Function fields.

**Definition 2.2.11.** If $X$ is an integral finite-type $k$-scheme, its **function field** $k(X)$ is the residue field at the generic point of $X$. Alternatively, $k(X) := \text{Frac } \mathcal{A}$ for any affine open subset $U = \text{Spec } \mathcal{A}$ of $X$.

**Remark 2.2.12.** Suppose that $X$ is irreducible but not necessarily reduced. Then the first part of Definition 2.2.11 still makes sense. The alternative definition must be modified slightly, however: $A$ might not be a domain, so one should take $\text{Frac}(A/\text{nil}(A))$, where $\text{nil}(A)$ is the nilradical of the ring $A$.

We can construct varieties with given function field:

**Proposition 2.2.13.** Let $K$ be a finitely generated field extension of $k$. Then there exists a normal projective integral $k$-variety $X$ with $k(X) \cong K$.

**Proof.** Let $S$ be a finite set of generators of $K$ as a field extension of $k$. Let $A_0$ be the $k$-subalgebra of $K$ generated by $S$. Thus $A_0$ is a domain with $\text{Frac } A_0 = K$. Then $X_0 := \text{Spec } A_0$ is an affine integral $k$-variety with $k(X_0) = K$. If we choose a closed immersion $X_0 \hookrightarrow \mathbb{A}^n$ and choose a standard open immersion $\mathbb{A}^n \hookrightarrow \mathbb{P}^n$, then the Zariski closure of $X_0$ in $\mathbb{P}^n$ is a projective integral $k$-variety $X_1$ with $k(X_1) = K$. Let $X$ be the normalization of $X_1$. By [Har77, Exercise II.3.8], $X$ is finite over $X_1$, so $X$ is projective. The other properties are immediate. \hfill \Box

**Remark 2.2.14.** A weak form of the “resolution of singularities” conjecture states that Proposition 2.2.13 holds with “normal” replaced by the stronger condition “regular”. Resolution of singularities was proved by Hironaka [Hir64] in the case that $k$ has characteristic 0; see [Kol07b] for an exposition of a proof. In arbitrary characteristic it is known in dimension $\leq 2$ (i.e., $\text{tr deg}(K/k) \leq 2$): see [Art86b] for an exposition of a proof by Lipman [Lip78]. Finally, if one can tolerate replacing $K$ by a finite extension, then one can solve the problem in general [dJ96]; this suffices for many applications.

### 2.2.2. Separable and primary field extensions.

Section 2.2.3 will show that for an integral $k$-variety $X$, the properties of being geometrically irreducible, geometrically reduced, and geometrically integral are equivalent to field-theoretic properties of the extension $k(X)/k$.

First we define the field-theoretic properties. The following definition of separable agrees with the usual notion for algebraic field extensions.

**Definition 2.2.15.** A field extension $L$ of $k$ is **separable** if the ring $L \otimes_k k'$ is reduced for all field extensions $k'$ of $k$. 

Proposition 2.2.16. Let $L$ be a finitely generated field extension of a field $k$.

(i) The field $L$ is separable over $k$ if and only if $L$ is a finite separable extension of a purely transcendental extension $k(t_1,\ldots,t_n)$.

(ii) Let $n = \deg(L/k)$. Elements $t_1,\ldots,t_n$ of $L$ generate a purely transcendental extension of $k$ over which $L$ is a finite separable extension if and only if $dt_1,\ldots,dt_n$ form a basis for the $L$-vector space $\Omega_{L/k}$ of Kähler differentials.

Proof.

(i) See [Mat80] (27.F).

(ii) See the proof of [Mat80] (27.B). □

Warning 2.2.17. If $L$ is separable over $k$, then every subextension is separable over $k$, so in particular every finite subextension is separable over $k$. But there exist also inseparable field extensions $L$ over $k$ such that all finite subextensions are separable over $k$. See Exercise 2.2.

Definition 2.2.18. A field extension $L$ of $k$ is primary if the largest separable algebraic extension of $k$ contained in $L$ is $k$ itself.

Purely inseparable algebraic field extensions are primary. Purely transcendental field extensions are primary and separable. For equivalent definitions of “primary” and “separable”, see [FJ08] §2.6.

2.2.3. Geometric properties determined by the function field.

Proposition 2.2.19. Let $X$ be a finite-type $k$-scheme. Then the following are equivalent:

(i) $X$ is geometrically irreducible.

(ii) There is a separably closed field $L$ containing $k$ such that the $L$-scheme $X_L$ is irreducible.

(iii) For all fields $L$ containing $k$, the $L$-scheme $X_L$ is irreducible.

(iv) $X$ is irreducible, and the field extension $k(X)$ of $k$ is primary.

Sketch of proof. See [EGA IV$_2$ 4.5.9]. One shows first that for a field $L$ containing $k$, the $L$-scheme $X \times_k L$ is irreducible if and only if Spec$(k(X) \otimes_k L)$ is irreducible. The rest is field theory. □

Proposition 2.2.20. Let $X$ be a finite-type $k$-scheme. Then the following are equivalent:

(i) $X$ is geometrically reduced.

(ii) There is a perfect field $L$ containing $k$ such that the $L$-scheme $X_L$ is reduced.

(iii) For all fields $L$ containing $k$, the $L$-scheme $X_L$ is reduced.

(iv) $X$ is reduced, and for each irreducible component $Z$ of $X$, the field extension $k(Z)$ of $k$ is separable.

Proof. See [EGA IV$_2$ 4.6.1]. □
Combining Propositions 2.2.19 and 2.2.20 leads to equivalent conditions for $X$ to be geometrically integral.

**Remark 2.2.21.** The property of $X$ being geometrically regular depends on more than the function field, even when $X$ is assumed to be a projective integral variety over an algebraically closed field $k$. For instance, the cuspidal cubic curve $y^2z = x^3$ in $\mathbb{P}_k^2$ is not regular at $(0 : 0 : 1)$, but it has the same function field as $\mathbb{P}_k^1$, which is regular.

**2.2.4. The constant field of a function field.** Let $K$ be a finitely generated field extension of $k$, so $K = k(X)$ for some integral finite-type $k$-scheme $X$. The **constant field** of $K$ or of $X$ is the maximal algebraic extension $k'$ of $k$ contained in $K$. It is a finite extension of $k$: in fact, if $t_1, \ldots, t_n$ is a transcendence basis of $K/k$, then

$$[k' : k] = [k'(t_1, \ldots, t_n) : k(t_1, \ldots, t_n)] \leq [K : k(t_1, \ldots, t_n)] < \infty.$$

**Proposition 2.2.22.** Let $X$ be an integral finite-type $k$-scheme. Let $k' \supseteq k$ be its constant field.

(i) If $X$ is geometrically integral, then $k' = k$.

(ii) If $X$ is proper, then $\mathcal{O}_X(X)$ is a subfield of $k'$.

(iii) If $X$ is normal, then $k' \subseteq \mathcal{O}_X(X)$.

**Proof.**

(i) Proposition 2.2.19 implies that $k'/k$ is primary. Proposition 2.2.20 implies that $k'/k$ is separable. A primary separable finite extension of a field is trivial.

(ii) Let $L$ be the $k$-algebra $\mathcal{O}_X(X)$. Since $X$ is proper, $\dim_k L < \infty$. Since $X$ is integral, $L$ is an integral domain. Thus $L$ is a finite field extension of $k$ contained in $k(X)$, so $L \subseteq k'$.

(iii) We have $k \subseteq k' \subseteq k(X)$, with $k'$ integral over $k$. For each $x \in X$, the ring $\mathcal{O}_{X,x}$ is integrally closed in its fraction field $k(X)$ and contains $k$, so it contains $k'$. Thus $k' \subseteq \bigcap_{x \in X} \mathcal{O}_{X,x} = \mathcal{O}_X(X)$. $\square$

**Remark 2.2.23.** To see why the hypothesis in each part of Proposition 2.2.22 is needed, consider the following counterexamples:

(i) $\mathbb{P}_k^1$ as $k$-scheme, for any nontrivial finite extension $F/k$,

(ii) $\mathbb{A}_k^1$, and

(iii) $x^2 - 2y^2 = 0$ over $\mathbb{Q}$.

**2.3. Scheme-valued points**
2.3.1. Motivation: rational points on affine varieties over fields. Let $X$ be the subvariety of $\mathbb{A}^n_k$ defined by a system of polynomial equations
\[
\begin{align*}
f_1(x_1, & \ldots, x_n) = 0 \\
f_2(x_1, & \ldots, x_n) = 0 \\
& \vdots \\
f_m(x_1, & \ldots, x_n) = 0.
\end{align*}
\]
In other words, $X$ is the affine $k$-variety $\text{Spec } A$ where $A = k[x_1, \ldots, x_n]/(f_1, \ldots, f_m)$. Then a $k$-rational point (or simply $k$-point) on $X$ is an $n$-tuple $(a_1, \ldots, a_n) \in k^n$ such that $f_1(a_1, \ldots, a_n) = f_m(a_1, \ldots, a_n) = 0$. The set of $k$-points on $X$ is in bijection with the set $\text{Hom}_{k\text{-algebras}}(A, k)$, which is in bijection with $\text{Hom}_{k\text{-schemes}}(\text{Spec } k, X)$. This motivates the general definition in the next section.

2.3.2. The set of scheme-valued points.

**Definition 2.3.1.** Let $X$ be an $S$-scheme. If $T$ is a $S$-scheme, then the set of $T$-points on $X$ is $X(T) := \text{Hom}_S(T, X)$.

**Warning 2.3.2.** The definition of $X(T)$ depends on the structure morphism $X \to S$, even though the notation does not show it explicitly. This is in keeping with our notational convention of using $X$ as abbreviation for the $S$-scheme $(X, f)$ where $f : X \to S$ is the structure morphism.

In the case where $S = \text{Spec } k$ and $T = \text{Spec } L$ for a field extension $L$ of $k$, an element of $X(L)$ is called an $L$-rational point or simply an $L$-point.

2.3.3. Functor of points, Yoneda’s lemma, and representable functors.

(Reference: [Vis05, §2.1])

If $T' \to T$ is an $S$-morphism, then sending each $S$-morphism $T \to X$ to the composition $T' \to T \to X$ defines a map of sets $X(T) \to X(T')$. In fact, we obtain a functor:

**Definition 2.3.3.** The functor of points of an $S$-scheme $X$ is the functor
\[
h_X : \text{Schemes}_S^\text{opp} \to \text{Sets}
\]
\[
T \mapsto X(T) := \text{Hom}_S(T, X).
\]
A morphism of $S$-schemes $f \colon X \to Y$ induces a map of sets $X(T) \to Y(T)$ for each $S$-scheme $T$, and whenever $T' \to T$ is an $S$-morphism we obtain a commutative square

$$
\begin{array}{ccc}
X(T) & \longrightarrow & Y(T) \\
\downarrow & & \downarrow \\
X(T') & \longrightarrow & Y(T').
\end{array}
$$

In other words, $f$ induces a morphism of functors (i.e., natural transformation) $h_f \colon h_X \to h_Y$.

The following is purely formal, true in any category, not just $\textbf{Schemes}_S$; but it is also very useful:

**Lemma 2.3.4 (Yoneda's lemma).** Let $X$ and $Y$ be $S$-schemes. The function

$$
\text{Hom}_S(X,Y) \longrightarrow \text{Hom}(h_X,h_Y)
$$

$f \mapsto h_f$

is a bijection.

**Sketch of proof.** The inverse map takes a morphism of functors $F \colon h_X \to h_Y$ to the image of the identity $1_X \in \text{Hom}_S(X,X) = X(X)$ under the map $F(X) \colon X(X) \to Y(X)$. □

For a stronger version of Yoneda’s lemma, see [Vis05, p. 14].

**Remark 2.3.5.** Yoneda’s lemma implies that $X$ is determined by its functor of points $h_X$. In fact, $X$ is already determined by the restriction of $h_X$ to affine schemes, because $h_X(T) = X(T)$ can be recovered as $\varprojlim X(T_i)$ where $(T_i)$ is the directed system of all affine open subschemes of $T$ ordered by inclusion.

Because no information is lost in passing from $X$ to $h_X$, it is sometimes convenient to identify $X$ with its functor of points $h_X$! Then more general functors $\textbf{Schemes}_{S}^{\text{op}} \to \textbf{Sets}$ can be thought of as generalizations of schemes; some of these functors are of the form $h_X$, and some are not.

**Definition 2.3.6.** A functor $F \colon \textbf{Schemes}_{S}^{\text{op}} \to \textbf{Sets}$ is **representable** if it is isomorphic to $h_M$ for some $S$-scheme $M$. In this case, one says also that $M$ **represents** $F$, or that $M$ is a **fine moduli space** for $F$.

Sometimes when one wants to construct a scheme, at first one can construct only what should be its functor of points $F$. Then one must ask whether $F$ is actually represented by a scheme. If so, then all the tools of algebraic geometry can be applied to that scheme in order to understand $F$ better. If not, one can hope that $F$ might still be represented by some algebraic object more general than a scheme, but close enough to a scheme that some tools of geometry can still be applied. For example, $F$ might be represented by an **algebraic space**.
or an algebraic stack: for an introduction, see [LMB00] or [Ols16]. Alternatively, if $F$ is not represented by a scheme, so $F$ is not isomorphic to any $h_M$, then it might be at least approximated by a functor $h_M$ in the following sense:

**Definition 2.3.7.** Let $F : \text{Schemes}_S^{\text{op}} \to \text{Sets}$ be a functor. An $S$-scheme $M$ equipped with a morphism of functors $F \to h_M$ is a coarse moduli space for $F$ if

(i) For every other $S$-scheme $M'$ with a morphism $F \to h_{M'}$, there is a unique morphism $h_M \to h_{M'}$ (or equivalently, a unique $S$-morphism $M \to M'$) such that $F \to h_{M'}$ factors as $F \to h_M \to h_{M'}$.

(ii) For every algebraically closed field $k$ and morphism $\text{Spec} \, k \to S$, the map $F(\text{Spec} \, k) \to M(k)$ given by $\iota$ is a bijection.

Intuitively, one can understand this definition as follows. The set $F(\text{Spec} \, k)$ is a certain collection of objects. If $T$ is an $k$-scheme, an element of $F(T)$ may be thought of as a family of such objects parameterized by $T$. Thus giving $F$ specifies both the objects and also what constitutes a family of objects. If $M$ is a coarse moduli space, then each object in $F(\text{Spec} \, k)$ has a class in $M(k)$, and condition (ii) says that the objects are in bijection with their classes. The morphism $F \to h_M$ gives in particular, that for each $T$, there is a map $F(T) \to \text{Hom}_S(T, M)$; it may be thought of as taking a family $\pi : \mathcal{X} \to T$ to the morphism $T \to M$ sending each point $t \in T(k)$ to the point of $M$ corresponding to class of the fiber $\pi^{-1}(t)$. Finally, condition (i) requires that $M$ is such that $h_M$ is as close as possible to $F$; it prevents, for example, replacing the morphism $F \to h_M$ by a composition $F \to h_M \to h_{\tilde{M}}$ such that $M(k) \to \tilde{M}(k)$ is a bijection. In fact, since condition (i) is a universal property, it guarantees that $M$ is unique if it exists.

**Example 2.3.8 (Moduli space of curves).** Fix $g \in \mathbb{Z}_{\geq 0}$. For an algebraically closed field $k$, let $\mathcal{M}_g(k)$ be the set of isomorphism classes of smooth projective geometrically integral curves of genus $g$ over $k$ (see Section 3.5 for the definition of smooth). More generally, for any scheme $T$, let $\mathcal{M}_g(T)$ be the set of isomorphism classes of smooth proper $T$-schemes whose fibers are geometrically integral curves of genus $g$. Then the functor $F := \mathcal{M}_g$ is not represented by a scheme, but it has a coarse moduli space $M_g$ that is a quasi-projective scheme over $\mathbb{Z}$; alternatively, $\mathcal{M}_g$ is represented by an algebraic stack [DM69]. Also, the subfunctor $\mathcal{M}_g^0$ parametrizing genus $g$ curves whose automorphism group is trivial is represented by a quasi-projective scheme $M_g^0$, and it is nonempty for $g \geq 3$.

**Example 2.3.9 (Moduli space of curves with marked points).** More generally, for any $g, n \in \mathbb{Z}_{\geq 0}$, there is a quasi-projective coarse moduli space $M_{g,n}$ whose points over an algebraically closed field parametrize genus $g$ curves with $n$ distinct marked points. The subfunctor parametrizing $(C, p_1, \ldots, p_n)$ such that the group of automorphisms of $C$ fixing
is trivial is represented by a quasi-projective scheme $M_{g,n}^0$. For fixed $g$, we have
$M_{g,n} = M_{g,n}^0$ for sufficiently large $n$; that is $M_{g,n}$ is a fine moduli space for $n$ large enough relative to $g$. The symmetric group $S_n$ acts on $M_{g,n}$.

**Example 2.3.10** (Moduli space of genus 0 curves with marked points). The group $\text{Aut} \mathbb{P}^1 \simeq \text{PGL}_2$ acts simply transitively on triples of distinct points of $\mathbb{P}^1$. Therefore, for $n \geq 3$, the space $M_{0,n}$ parametrizing $(\text{Aut} \mathbb{P}^1)$-orbits of $n$-tuples of points on $\mathbb{P}^1$ is a fine moduli space. Let us work over a field $k$. Then $M_{0,3}$ is a point $\text{Spec } k$. Next, $M_{0,4} \simeq \mathbb{P}^1 - \{0, 1, \infty\}$, since any 4-tuple of distinct geometric points can be moved by an automorphism of $\mathbb{P}^1$ to a unique 4-tuple of the form $(0, 1, \infty, x)$ with $x \notin \{0, 1, \infty\}$. And $M_{0,5}$ is $(\mathbb{P}^1 - \{0, 1, \infty\})^2 - \Delta$, where $\Delta$ is the diagonal; see Section 9.4.7 for an application. For each $n \geq 3$, the space $M_{0,n}$ is an open subscheme of $A^n$.

**Example 2.3.11** (Twists of $M_{g,n}$). Over non-algebraically closed fields, we may consider twists of $M_{g,n}$ in the sense of Section 4.5. Start by thinking of $M_{g,n}$ as parametrizing isomorphism classes of genus $g$ curves $C$ equipped with a closed immersion $\text{Spec } k \rightarrow C$. If $L$ is a degree $n$ étale $k$-algebra, then there is a coarse moduli space $M_{g,n}(L)$ over $k$ parametrizing genus $g$ curves $C$ equipped with a closed immersion $\text{Spec } L \rightarrow C$. The varieties $M_{g,n}(L)$ and $M_{g,n}$ become isomorphic after base change to $k_s$.

**Example 2.3.12** (Compactifications of the moduli space of curves). There is a functor $\overline{M}_g$ that parametrizes isomorphism classes of stable genus $g$ curves: see [HM98, Theorem 2.15] for an introduction and for the definition of stable. Knudsen and Mumford proved that $\overline{M}_g$ has a coarse moduli space $\overline{M}_g$ that is a projective variety containing $M_g$ as an open subvariety: the first proof, published long after its discovery, was that in [Knu83, Theorem 6.1], but a simpler proof was given in [Mum77, Corollary 5.2]. Similarly one can construct projective varieties $\overline{M}_{g,n}$ and $\overline{M}_{g,n}(L)$.

**2.3.4. Functorial properties.** If $X$ is an $S$-scheme, and $U \subseteq X$ is an open subscheme, then $U(T) \subseteq X(T)$ for any $S$-scheme $T$: see Exercise 2.4.

**Remark 2.3.13.** Let $k$ be a field, and let $X$ be a $k$-scheme. If $\{X_i\}$ is an open covering of $X$, then $\bigcup X_i(k) = X(k)$.

**Warning 2.3.14.** Remark 2.3.13 holds more generally for a local ring $k$, but not for an arbitrary ring. It can fail for a polynomial ring, for instance: a morphism $A^1 \rightarrow X$ need not have image contained in any one $X_i$.

Despite Warning 2.3.2, we do get independence of $S$ if we base change $X$ appropriately:
PROPOSITION 2.3.15. If $X$ is an $S$-scheme, and $S' \rightarrow S$ is a morphism of schemes, and $T$ is an $S'$-scheme, then $X_{S'}(T) = X(T)$, where on the right we view $T$ as $S$-scheme via the composition $T \rightarrow S' \rightarrow S$.

PROOF. The universal property of the fiber product gives $\text{Hom}_{S'}(T, X_{S'}) = \text{Hom}_{S}(T, X)$.

2.3.5. Example: scheme-valued points on projective space. Let $X$ be an $S$-scheme. By Proposition 2.3.15, $\mathbb{P}^n_S(X) = \mathbb{P}^n_2(X) := \text{Hom}_Z(X, \mathbb{P}^n_Z)$, and the set on the right is described by [Har77] II.7.1. The outcome is that there is a bijection

$$\mathbb{P}^n_S(X) \leftrightarrow \left\{ (\mathcal{L}, s_0, \ldots, s_n) : \begin{array}{c} \mathcal{L} \text{ is a line bundle on } X \\ \text{and } s_0, \ldots, s_n \in \Gamma(X, \mathcal{L}) \text{ generate } \mathcal{L} \end{array} \right\} / \sim.$$

By definition, global sections $s_0, \ldots, s_n$ generate $\mathcal{L}$ if and only if for every $P \in X$, they do not simultaneously vanish when evaluated at $P$ (that is, for every $P \in X$, their images in the 1-dimensional $k(P)$-vector space stalk $\mathcal{L}_P/\mathfrak{m}_P\mathcal{L}_P$ do not all vanish). On the right, tuples are considered up to isomorphism: $(\mathcal{L}, s_0, \ldots, s_n)$ and $(\mathcal{L}', s_0', \ldots, s_n')$ are called isomorphic if and only if there is an isomorphism of line bundles $\mathcal{L} \rightarrow \mathcal{L}'$ mapping $s_i$ to $s_i'$ for each $i$.

REMARK 2.3.16. Intuitively one can think of $(\mathcal{L}, s_0, \ldots, s_n)$ as describing the morphism

$$X \rightarrow \mathbb{P}^n_S,$$

$$P \mapsto (s_0(P), \ldots, s_n(P)).$$

Strictly speaking, this does not make sense, since the $s_i(P)$ are not well-defined elements of the field $k(P)$ ($s_i$ not being a function on $X$). But at each $P$, we can fix $j$ such that $s_j$ is nonvanishing at $P$ (that is, $s_j \notin \mathfrak{m}_P\mathcal{L}_P$), and then for every $i$ the ratio $s_i/s_j$ may be viewed as a function defined in a neighborhood of $P$ in $X$.

EXAMPLE 2.3.17. Let us compute $\mathbb{P}^n(A)$ when $A$ is a principal ideal domain. By [Har77] II.6.2, II.6.16], $\text{Pic} A = 0$. That is, the only line bundle on $X := \text{Spec} A$, up to isomorphism, is $\mathcal{O}_X$. Global sections of $\mathcal{O}_X$ are simply elements of $A$, and a sequence of global sections $a_0, \ldots, a_n \in A$ generate $\mathcal{O}_X$ if and only if $a_0, \ldots, a_n$ generate the unit ideal. An isomorphism of line bundles $\mathcal{O}_X \rightarrow \mathcal{O}_X$ is the same as an $A$-module isomorphism $A \rightarrow A$, which is the same as multiplication by some unit $\lambda \in A^\times$. Hence

$$\mathbb{P}^n(A) = \left\{ (a_0, \ldots, a_n) \in A^{n+1} : a_0, \ldots, a_n \text{ generate } (1) \right\} / \sim,$$

where the equivalence relation $\sim$ is as follows: $(a_0, \ldots, a_n) \sim (a_0', \ldots, a_n')$ if and only if there exists $\lambda \in A^\times$ such that $a_i' = \lambda a_i$ for all $i$. The equivalence class of $(a_0, \ldots, a_n)$ is denoted $(a_0 : \cdots : a_n)$.

In the special case where $A$ is a field, this gives the expected description of $\mathbb{P}^n(k)$. 39
Remark 2.3.18. If $A$ is a principal ideal domain, and $K = \text{Frac } A$, it follows from Example 2.3.17 that the natural map $\mathbb{P}^n(A) \to \mathbb{P}^n(K)$ is a bijection. Namely, given $(a_0 : \ldots : a_n) \in \mathbb{P}^n(K)$, the fractional ideal generated by $a_0, \ldots, a_n$ is principal, and if we choose a generator $\lambda$, then scaling all the $a_i$ by $\lambda^{-1}$ results in an equivalent point that comes from $\mathbb{P}^n(A)$. For a generalization of this remark, see Theorem 3.2.13.

2.3.6. Scheme-valued points on separated schemes.

(Reference: [EGA IV], §11.10]

Definition 2.3.19. A morphism of schemes $f: X \to Y$ is called dominant if the set $f(X)$ is dense in the topological space $Y$; i.e., the only closed subset of $Y$ containing $f(X)$ is $Y$ itself. Call $f$ scheme-theoretically dominant (cf. [EGA IV], 11.10.2) if either of the following equivalent conditions holds:

- Whenever $U$ is an open subscheme of $Y$, and $f|_{f^{-1}U}: f^{-1}U \to U$ factors as $f^{-1}U \to U' \hookrightarrow U$ for some closed subscheme $U'$ of $U$, we have $U' = U$.
- The sheaf homomorphism $\mathcal{O}_Y \to f_* \mathcal{O}_X$ is injective.

Warning 2.3.20. It is not enough to require that the only closed subscheme of $Y$ through which $f$ factors is $Y$ itself; one really needs to impose the condition above every open subscheme $U \subseteq Y$. See Exercise 2.10.

Scheme-theoretically dominant implies dominant. If $Y$ is reduced, then the notions are equivalent, since then every open subscheme $U$ is reduced too, and the only closed subscheme of $U$ having the same topological space as $U$ is $U$ itself.

Proposition 2.3.21. Let $X$ be a separated $S$-scheme. If $T' \to T$ is a scheme-theoretically dominant $S$-morphism, then $X(T) \to X(T')$ is injective.

Proof. Let $f, g \in X(T)$ and let $e$ be the morphism $T' \to T$, so we have

$$T' \xrightarrow{e} T \xrightarrow{(f,g)} X \times_S X.$$ 

Since $X$ is separated over $S$, the diagonal $\Delta \subseteq X \times_S X$ is a closed subscheme. Let $Z = (f, g)^{-1}\Delta$, which is “the closed subscheme of $T$ on which $f$ and $g$ agree”. Let $f', g'$ be the images of $f, g$ in $X(T')$, and let $Z' = (f', g')^{-1}\Delta$. Then $Z' = e^{-1}(Z)$. If $f' = g'$, then $Z' = T'$, but $e$ is scheme-theoretically dominant, so then $Z = T$, which means that $f = g$. This proves injectivity.

Corollary 2.3.22. If $R \subseteq R'$ is an inclusion of rings, and $X$ is a separated $R$-scheme, then $X(R) \to X(R')$ is injective.

Proposition 2.3.21 implies also that, under suitable hypotheses, morphisms agreeing on a dense open subscheme agree everywhere:
Corollary 2.3.23. Let $X$ be a reduced $S$-scheme, and let $Y$ be a separated $S$-scheme. Let $U$ be a dense open subscheme of $X$. If $f$ and $g$ are morphisms $X \to Y$ such that $f|_U = g|_U$, then $f = g$.

Proof. Proposition 2.3.21 says that $Y(X) \to Y(U)$ is injective. \qed

2.3.7. Varieties that are not geometrically integral.

Proposition 2.3.24. Let $k$ be a field. A connected $k$-scheme with a $k$-point is geometrically connected.

Proof. More generally, if $X$ and $Y$ are connected $k$-schemes and $X$ has a $k$-point, then $X \times_k Y$ is connected: see [EGA IV$_2$] Corollaire 4.5.14 or [SGA 3$_1$] Exposé VI$_A$, Lemma 2.1.2]. \qed

Warning 2.3.25. In contrast with Proposition 2.3.24, an irreducible $k$-variety with a $k$-point need not be geometrically irreducible: the $\mathbb{Q}$-variety $x^2 - 2y^2 = 0$ in Example 2.2.6 has the rational point $(0, 0)$.

But if we have not just one $k$-point, but a Zariski dense set of $k$-points, we can say more:

Proposition 2.3.26. Let $X$ be a finite-type scheme over a field $k$ such that $X(k)$ is Zariski dense in $X$.

(i) If $X$ is irreducible, then $X$ is geometrically irreducible.

(ii) If $X$ is reduced, then $X$ is geometrically reduced.

(iii) If $X$ is integral, then $X$ is geometrically integral.

Proof.

(i) Replacing $X$ by its associated reduced subscheme $X_{\text{red}}$ affects neither the hypotheses nor the conclusion. Suppose that $X$ is not geometrically irreducible. By Proposition 2.2.19(i)$\iff$(iv), $k(X)/k$ is not primary, so there exists $\alpha \in k(X) \setminus k$ separable and algebraic over $k$. By definition of $k(X)$, we have $\alpha \in \mathcal{O}(U)$ for some nonempty affine open subscheme $U \subseteq X$. Since $X(k)$ is Zariski dense in $X$, there exists a $k$-point in $U$. This point induces a $k$-algebra homomorphism $\mathcal{O}(U) \to k$, which restricts to a $k$-algebra homomorphism $k(\alpha) \to k$, contradicting the fact that field homomorphisms are injective.

(ii) It suffices to prove the statement for each subscheme in an open cover of $X$. So assume that $X = \text{Spec } A$. Each $x \in X(k)$ corresponds to a $k$-algebra homomorphism $A \to k$. Putting these together gives a homomorphism $A \to \prod_{x \in X(k)} k$, which is injective since $X(k)$ is Zariski dense and $A$ is reduced. Tensoring with $\overline{k}$ yields an injection

$$A \otimes_k \overline{k} \hookrightarrow \left( \prod_{x \in X(k)} k \right) \otimes_k \overline{k} \subseteq \prod_{x \in X(k)} \overline{k}.$$
which shows that $A \otimes_k \overline{k}$ is reduced. Thus $X$ is geometrically reduced.

(iii) Combine (i) and (ii).

Remark 2.3.27. Proposition 2.3.26 is often applied in its contrapositive form: if $X$ is an integral $k$-variety that is not geometrically integral, then $X(k)$ is not Zariski dense. In this case, the study of $X(k)$ reduces to the study of $Y(k)$ for a lower-dimensional variety $Y$. For this reason, when studying rational points, we can reduce to the case of geometrically integral varieties.

2.4. Closed points

Definition 2.4.1. A closed point of a scheme $X$ is a point $x \in X$ such that $\{x\}$ is Zariski closed in $X$.

If $X$ is a variety over an algebraically closed field $k$, the map

$$X(k) \rightarrow \{\text{closed points of } X\}$$

$$(f: \text{Spec } k \rightarrow X) \mapsto f(\text{Spec } k)$$

is a bijection. The non-closed points of $X$ are the generic points of the positive-dimensional integral subvarieties of $X$.

To develop intuition for our generalizations to arbitrary fields $k$, namely Propositions 2.4.3 and 2.4.6, we begin with an example:

Example 2.4.2. Let $X = \mathbb{A}^1_k = \text{Spec } \mathbb{R}[t]$. The following are in bijection:

(i) The set of closed points of $X$.

(ii) The set of maximal ideals of $\mathbb{R}[t]$.

(iii) The set of monic irreducible polynomials of $\mathbb{R}[t]$.

(iv) The set of $\text{Gal}(\mathbb{C}/\mathbb{R})$-orbits in $X(\mathbb{C}) = \mathbb{C}$.

If $x \in X$ is a closed point corresponding to a monic irreducible polynomial $f \in \mathbb{R}[t]$, then $k(x) = \mathbb{R}[t]/(f)$, so $[k(x): \mathbb{R}] = \deg f$, which may be 1 or 2. Those $x$ with $[k(x): k] = 1$ correspond to size 1 orbits in (iv), which correspond to elements of $X(\mathbb{R})$.

Proposition 2.4.3. Let $X$ be a $k$-variety, and let $x \in X$. The following are equivalent:

(i) The point $x$ is closed.

(ii) The dimension of the closure of $\{x\}$ is 0.

(iii) The residue field $k(x)$ is a finite extension of $k$.

Proof. The closure $\overline{\{x\}}$ with its reduced structure is irreducible and reduced, hence an integral $k$-variety.

(i)⇒(ii): The dimension of a one-point space is 0.
(ii)⇒(i): Suppose that \( y \in \{ x \} \); we must prove that \( y = x \). We have irreducible closed subsets \( \{ y \} \subseteq \{ x \} \), but we are assuming \( \dim \{ x \} = 0 \), so \( \{ y \} = \{ x \} \). In a scheme, an irreducible closed subset has a unique generic point, so \( y = x \).

(ii)⇔(iii): The function field of \( \{ x \} \) is \( k(x) \), so \( \dim \{ x \} = \text{tr} \deg(k(x)/k) \). In particular, \( \dim \{ x \} = 0 \) if and only if \( k(x) \) is algebraic over \( k \), which is the same as saying that \( k(x) \) is a finite extension of \( k \) since we know in advance that \( k(x) \) is a finitely generated field extension of \( k \). \( \square \)

**Definition 2.4.4.** The degree of a closed point \( x \) on a \( k \)-variety \( X \) is \([k(x) : k]\).

**Remark 2.4.5.** Schemes of finite type over \( \mathbb{Z} \) share many properties with schemes of finite type over a field. In particular, there is an analogue of Proposition 2.4.3 that states that if \( X \) is a scheme of finite type over \( \mathbb{Z} \) and \( x \in X \), the following are equivalent:

(i) The point \( x \) is closed.

(ii) The (Krull) dimension of the closure of \( \{ x \} \) is 0.

(iii) The residue field \( k(x) \) is finite.

The proof of (i)⇔(ii) is as before, and (i)⇔(iii), which may be called the arithmetic weak Nullstellensatz, is [EGA IV 3, 10.4.11.1(i)].

**Proposition 2.4.6.** Let \( X \) be a \( k \)-variety. Then the map

\[
\{ \mathfrak{G}_k\text{-orbits in } X(\overline{k}) \} \longrightarrow \{ \text{closed points of } X \}
\]

\[
\text{orbit of } (f: \text{Spec} \overline{k} \rightarrow X) \longmapsto f(\text{Spec} \overline{k})
\]

is a bijection.

**Proof.** For any field extension \( L \) of \( k \), [Har77 II.4.4] gives a bijection

\[
X(L) \stackrel{\sim}{\rightarrow} \{ (x, \iota) \mid x \in X, \text{ and } \iota: k(x) \hookrightarrow L \text{ is a } k\text{-embedding } \}.
\]

in which the \( x \) coming from \( P \in X(L) \) is the unique point in the image of \( \text{Spec} L \rightarrow X \). Take \( L = \overline{k} \). Suppose that \( P \in X(\overline{k}) \) corresponds to \( (x, \iota) \). Since \( k(x) \) is finitely generated over \( k \), it is a finite extension of \( k \), so \( x \) is a closed point. Thus we get a bijection

\[
X(\overline{k}) \stackrel{\sim}{\rightarrow} \{ (x, \iota) \mid x \in X \text{ is closed, and } \iota: k(x) \hookrightarrow \overline{k} \text{ is a } k\text{-embedding } \}.
\]

This bijection is \( \mathfrak{G}_k \)-equivariant, where \( \sigma \) acts on \( X(\overline{k}) \) coordinate-wise (or equivalently, by forming the composition \( \text{Spec} \overline{k} \overset{\sigma}{\rightarrow} \text{Spec} \overline{k} \overset{P}{\rightarrow} X \), and acts on the right set by \( (x, \iota) \mapsto (x, \iota \circ \sigma) \). For each closed point \( x \in X \), the set of \( k \)-embeddings \( \iota: k(x) \hookrightarrow \overline{k} \) is a nonempty and transitive \( \mathfrak{G}_k \)-set, so the set of \( \mathfrak{G}_k \)-orbits on the right hand side equals the set of closed points \( x \). \( \square \)

In particular, if \( X \) is a \( k \)-variety, then \( k \)-points of \( X \) are in bijection with closed points with residue field \( k \).
Warning 2.4.7. On schemes that are not varieties, closed points can behave strangely. For instance, there exists a nonempty scheme with no closed points at all! See [Liu02 Exercise 3.27].

2.5. Curves

(Reference: [Liu02 Chapter 7])

2.5.1. Genus.

(Reference: [Liu02 Chapter 7, Definition 3.19])

Let $X$ be a regular, projective, geometrically integral curve over a field $k$. Its genus $g = g(X)$ admits several equivalent definitions:

- The arithmetic genus of $X$ is $p_a(X) := \dim_k H^1(X, \mathcal{O}_X)$.
- Let $\omega_X^\circ$ be the dualizing sheaf [Har77 III.§7], a line bundle on $X$; if $X$ is smooth (see Section 2.5), then $\omega_X^\circ$ is simply the canonical sheaf $\omega_X = \Omega^1_{X/k}$ [Har77 II.§8]. The geometric genus of $X$ is $p_g(X) := \dim_k H^0(X, \omega_X^\circ)$.
- The genus is the integer $g$ that makes the Riemann–Roch theorem (Theorem 2.5.3) hold.
- If $k = \mathbb{C}$, then the compact Riemann surface $X(\mathbb{C})$ can be viewed as a compact orientable 2-dimensional $\mathbb{R}$-manifold, which is a $g$-holed torus for a unique $g \geq 0$.

The proof of the Serre duality theorem [Har77 III.7.7] works over an arbitrary field $k$, and shows that the $k$-vector spaces $H^1(X, \mathcal{O}_X)$ and $H^0(X, \omega_X^\circ)$ are dual, so $p_a(X) = p_g(X)$.

If $Y$ is a curve birational to a regular, projective, geometrically integral curve $X$, define $g(Y) := g(X)$.

2.5.2. Genus change under field extension.

(Reference: [Tat52])

**Theorem 2.5.1.** Let $X$ be a regular, projective, geometrically integral $k$-curve. Let $L \supseteq k$ be a field extension. Then

(a) We have $g(X_L) \leq g(X)$, with equality if and only if $X_L$ is regular.
(b) The difference $g(X) - g(X_L)$ is divisible by $(p - 1)/2$.
(c) If $L$ is separable over $k$, then $g(X_L) = g(X)$.

**Sketch of proof.**

(a) Let $\tilde{X}_L$ be the desingularization of $X_L$. We can define $p_a(X_L)$ as before even if $X_L$ is not regular; in fact, $p_a(X_L) = p_a(X)$ since cohomology commutes with flat base extension [Har77 III.9.3]. But $g(X_L)$ is defined as $p_a(\tilde{X}_L)$, which is less than or equal to $p_a(X_L)$, with equality if and only if $X_L$ is already regular.
(b) See Tat52.

(c) If $L$ is separable over $k$, then $X_L$ is regular (this follows from Proposition 3.5.50(iii)), so this is a special case of (a). □

Example 2.5.2. Let $p$ be an odd prime. Let $k$ be the imperfect field $\mathbb{F}_p(t)$. Let $X$ be the affine curve $y^2 = x^p - t$ over $k$. One can show that $g(X) = (p - 1)/2$. On the other hand, $X_k$ is isomorphic to the curve $y^2 = x^p$, which is birational to $\mathbb{P}^1_k$, so $g(X_k) = 0$.

2.5.3. The Riemann–Roch theorem.  

(Reference: Liu02 §7.3)

Let $X$ be a regular, projective, geometrically integral $k$-curve of genus $g$. The group $\text{Div} X$ of Weil divisors on $X$ is the free abelian group on the set of closed points $P$ of $X$. Each $D \in \text{Div} X$ gives rise to a line bundle $\mathcal{O}(D)$. By [Har77, II.6.16], this induces an isomorphism from the group of Weil divisors modulo linear equivalence to the Picard group $\text{Pic} X$ of isomorphism classes of line bundles. If $D = \sum n_P P \in \text{Div} X$, define $\deg D := \sum n_P \deg P$, where $\deg P$ is as in Definition 2.4.4 and define $\ell(D) := \dim_k H^0(X, \mathcal{O}(D))$.

A canonical divisor is a divisor $K$ such that $\omega_X = \mathcal{O}(K)$.

Theorem 2.5.3 (Riemann–Roch). Let $X$ and $K$ be as above. Then

$$\ell(D) - \ell(K - D) = \deg D + 1 - g.$$  

Proof. Once one has the Serre duality theorem, this is very similar to the proof of [Har77, Theorem IV.1.3], so we leave it as Exercise 2.15. See also Liu02 Chapter 7, Theorem 3.26. □

2.6. Rational points over special fields

2.6.1. Rational points over finite fields. Let $k$ be a finite field, and let $X$ be a $k$-variety. Then $X(k)$ is finite. (This is obvious if $X$ is affine, and the general case follows by applying Remark 2.3.13 to an affine open covering.) More will be said in Chapter 7.

2.6.2. Rational points over topological fields.  

(Reference: Ser55)

Let $k$ be a topological field (for example, a local field), and let $X$ be a $k$-variety. We can use the topology of $k$ to define a topology on $X(k)$, called the analytic topology, as follows. Give $\mathbb{A}^n(k) = k \times \cdots \times k$ the product topology. If $X$ is a closed subvariety of $\mathbb{A}^n$, give $X(k) \subseteq \mathbb{A}^n(k)$ the subspace topology. Finally, if $X$ is obtained by glueing affine open subsets $X_1, \ldots, X_m$, then use the same glueing data to glue the topological spaces $X_1(k), \ldots, X_m(k)$. Two different affine open coverings give the same topology on $X(k)$, as one can check
by comparison with a common refinement. Any morphism of \(k\)-varieties \(X \to Y\) induces a continuous map \(X(k) \to Y(k)\) of topological spaces.

**Proposition 2.6.1.** Let \(k\) be a local field. Let \(X\) be a \(k\)-variety.

(i) If \(X\) is proper over \(k\), then \(X(k)\) is compact.

(ii) More generally, if \(X \to Y\) is a proper morphism of \(k\)-varieties, then \(X(k) \to Y(k)\) is a proper map of topological spaces. (The latter means that the inverse image of any compact subset of \(Y(k)\) is compact.)

The converses hold when \(k = \mathbb{C}\).

**Proof.** See Serre’s “GAGA” paper [Ser55].

\(\square\)

**Remark 2.6.3.** In the case \(k = \mathbb{C}\), one can go further by equipping the topological space \(X(\mathbb{C})\) with a sheaf of “germs of holomorphic functions” to get a locally ringed space \(X^{an}\). (If \(\dim X > 0\), then \(X^{an}\) is not a scheme.) Such locally ringed spaces are special cases of complex analytic spaces: see [Har77, Appendix B] for a survey with more details, and [SGA 1, XII] for a definition of \(X^{an}\) as the complex analytic space representing a certain functor. There are also various nonarchimedean analogues [Con08].

**Remark 2.6.4 (Hilbert’s tenth problem over a local field).** There is an algorithm that, given a local field \(k\) of characteristic 0 and a \(k\)-variety \(X\), decides whether \(X(k)\) is nonempty. (Strictly speaking, to make sense of this, one should assume that \(X\) is given over an explicitly presented finitely generated subfield of \(k\), so that \(X\) admits a finite description suitable for input into a Turing machine.) The analogue for \(\mathbb{F}_q((t))\) is an open question.

**2.6.3. Adelic points.**

(Reference: [Con12a])

Let \(k\) be a global field, and let \(\Omega_k, O_{k,S}, k_v, O_v\), and \(A\) be as in Section 1.1.3. Let \(X\) be a \(k\)-variety. Since \(A\) is a \(k\)-algebra, the set \(X(A)\) of adelic points is already defined, as the set of \(k\)-morphisms \(\text{Spec} A \to X\).

There is a more down-to-earth description of \(X(A)\), however, as we now sketch. There exists a finite set \(S\) of places and a separated finite-type \(O_{k,S}\)-scheme \(X\) such that \(X_k \simeq X\). Then \(X(A)\) is in bijection with \(\prod_{v \in \Omega_k} (X(k_v), \mathcal{X}(O_v))\): see Exercise 3.4.

This bijection lets us equip \(X(A)\) with a topology. First, equip each \(X(k_v)\) with the analytic topology. Next, for nonarchimedean \(v \notin S\), equip the open and closed subset \(\mathcal{X}(O_v) \subseteq \mathcal{X}(k_v) = X(k_v)\) with the subspace topology. Finally, define the adelic topology on \(X(A) \simeq \prod_{v \in \Omega_k} (X(k_v), \mathcal{X}(O_v))\) as the restricted product topology, in which the basic open
sets are those of the form \( \prod_{v \in T} U_v \times \prod_{v \not\in T} \mathcal{X}(\mathcal{O}_v) \) for a finite set \( T \supseteq S \) and open subsets \( U_v \subseteq X(k_v) \) for each \( v \in T \).

**Remark 2.6.5.** If \( X \) is a closed subscheme of \( \mathbb{A}^n \), the adelic topology on \( X(\mathbb{A}) \) agrees with the subspace topology obtained by viewing \( X(\mathbb{A}) \) as a subset of the topological space \( \mathbb{A}^n \).

### 2.6.4. Rational points over global fields.

Let \( k \) be a global field. Let \( X \) be a \( k \)-variety. One would like to know the answers to many questions, such as the following.

#### 2.6.4.1. Existence of rational points.

**Question 2.6.6.** Does \( X \) have a \( k \)-point?

The problem of answering this question given an arbitrary \( X \) is equivalent to **Hilbert’s tenth problem over \( k \)**, which is the problem of finding a general algorithm that takes a multivariable polynomial \( f(x_1, \ldots, x_n) \in k[x_1, \ldots, x_n] \) as input and outputs YES or NO according to whether there exists \( \bar{a} \in k^n \) such that \( f(\bar{a}) = 0 \).

- For each global function field \( k \), no such algorithm exists [Phe91, Shl92, Vid94, Eis03].
- On the other hand, for each number field \( k \), it is unknown whether such an algorithm exists. It is not even proved yet that one can decide, given \( a \in \mathbb{Q} \), whether \( x^3 + y^3 = a \) has a solution in rational numbers.

See [Poo08] for more about extensions of Hilbert’s tenth problem.

#### 2.6.4.2. Finiteness of rational points.

**Question 2.6.7.** Is \( X(k) \) finite or infinite? When \( X(k) \) is finite, can one list its elements?

For curves \( X \) over number fields, the following theorem of Faltings gives a partial answer. Because of Remark 2.3.26 and the fact that \( X \) and its normalization differ in only finitely many points, we may assume that \( X \) is nice in the sense of Definition 3.5.67.

**Theorem 2.6.8 (Fal83).** Let \( X \) be a nice curve of genus \( > 1 \) over a number field \( k \). Then \( X(k) \) is finite.

For more details and generalizations, see Section 9.5. Question 2.6.7 can be difficult to answer even for specific, simple-looking equations:

**Example 2.6.9.** Let \( X \) be the projective surface in \( \mathbb{P}^3_{\mathbb{Q}} \) defined by the homogeneous equation \( x^4 + 2y^4 = z^4 + 4w^4 \). There are two obvious rational points, given in homogeneous coordinates as \((1 : 0 : \pm1 : 0)\). The next smallest solutions are

\[(\pm1484801 : \pm1203120 : \pm1169407 : \pm1157520),\]
According to [EJ06]. Are there infinitely many others? (This surface is an example of a K3 surface: see Section 9.3.2.2. It is not known whether there is a K3 surface $X$ over a number field $k$ such that $X(k)$ is nonempty and finite.)

2.6.4.3. Growth of rational points. Let us now return to the case of an arbitrary variety $X$ over a global field $k$. If $X(k)$ is infinite, one can try to “measure its size” in some way. For example, given $P \in \mathbb{P}^n(\mathbb{Q})$, one can write $P = (a_0 : \cdots : a_n)$ with $a_i \in \mathbb{Z}$ and $\gcd(a_0, \ldots, a_n) = 1$, and define the **height** of $P$ as $H(P) := \max |a_i|$. Then, for $X \subseteq \mathbb{P}^n$, one defines

$$N_X(B) := \# \{ x \in X(\mathbb{Q}) : H(x) \leq B \}.$$

**Question 2.6.10**. For $X \subseteq \mathbb{P}^n$, can one predict the rate of growth of $N_X(B)$ as $B \to \infty$?

For a survey on this question, see [Pey02].

2.6.4.4. Zariski density of rational points.

**Question 2.6.11**. Is $X(k)$ Zariski dense in $X$?

**Question 2.6.12**. Is there a finite extension $L$ of $k$ such that $X(L)$ is Zariski dense (in $X_L$)? If so, one says that “rational points are potentially dense on $X$”.

Campana [Cam04, Conjecture 9.20] has conjectured that for a variety $X$ over a number field, potential density is equivalent to a certain geometric condition.

2.6.4.5. Local approximation of rational points.

**Question 2.6.13**. Given a place $v$ of $k$, is $X(k)$ dense in $X(k_v)$ with respect to the $v$-adic (analytic) topology?

Related to this is the following conjecture of Mazur:

**Conjecture 2.6.14** ([Maz92]). If $X$ is a $\mathbb{Q}$-variety, then the closure of $X(\mathbb{Q})$ in $X(\mathbb{R})$ with respect to the analytic topology has at most finitely many connected components.

One strategy for determining whether a variety over global field $k$ has a $k$-point is to check first whether it has a $k_v$-point for each completion $k_v$ of $k$. This motivates the following question:

**Question 2.6.15**. Does the implication

$$X(k_v) \neq \emptyset \text{ for all places } v \text{ of } k \implies X(k) \neq \emptyset$$

hold? If so, one says that $X$ satisfies the local-global principle (or Hasse principle).

If $X$ satisfies the local-global principle, one can ask for something stronger:

**Question 2.6.16**. Is the image of $X(k) \to \prod_v X(k_v)$ dense with respect to the product of the $v$-adic topologies? If so, one says that $X$ satisfies weak approximation.
Exercise 2.17 explains how weak approximation is about simultaneous approximation of \( k_v \)-points for finitely many \( v \) by a \( k \)-point. Some varieties satisfy the local-global principle and/or weak approximation, and others do not. See [Har04] for a survey on weak approximation.

One can ask for even more:

\textbf{Question 2.6.17.} Is the image of \( X(k) \to X(A) \) dense with respect to the adelic topology?

This is stronger than weak approximation since the adelic topology on \( X(A) \) generally has more open sets than the topology induced on \( X(A) \) as a subset of \( \prod X(k_v) \) equipped with the product topology. In fact, adelic density is too strong to have a chance of holding for many varieties: for instance, if \( X \) is affine, then \( X(k) \) is discrete in \( X(A) \) since \( k \) is discrete in \( A \). Therefore we now weaken the condition slightly.

Let \( S \) be a finite set of places of \( k \). Define the \textit{prime-to-\( S \) adèle ring} \( A^S := \prod'_{v \in S} (k_v, O_v) \), so \( A = (\prod_{v \in S} k_v) \times A^S \). For any \( k \)-variety, define an adelic topology on \( X(A^S) \) as in Section 2.6.3 by viewing \( X(A^S) \) as a restricted product. The weakened question is then:

\textbf{Question 2.6.18.} Is the image of \( X(k) \to X(A^S) \) dense with respect to the adelic topology? If so, one says that \( X \) satisfies \textit{strong approximation with respect to} \( S \).

See Section [5.10] for approximation theorems in the case that \( X \) is an algebraic group, and see Section [8.4.6] for a way to prove that strong approximation fails for certain varieties.

\textbf{Exercises}

2.1. Find a field \( k \) and a regular integral \( k \)-variety \( X \) that is neither affine, projective, geometrically connected, geometrically reduced, nor geometrically regular.

2.2. Let \( k = \mathbb{F}_p(s,t) \) where \( s \) and \( t \) are indeterminates. Let \( X \) be the \( k \)-variety \( sx^p + ty^p = 1 \) in \( \mathbb{A}_k^2 \). Let \( L \) be the function field of \( X \).
   
   (a) Show that the only finite extension of \( k \) contained in \( L \) is \( k \) itself.
   
   (b) Show that \( L \) is not separable over \( k \).

2.3. For any scheme \( X \) over a field, if \( X_{\text{red}} \) is the associated reduced scheme, then the natural map \( X_{\text{red}}(k) \to X(k) \) is a bijection. For which schemes \( S \) is it true that for every \( S \)-scheme \( X \), the map \( X_{\text{red}}(S) \to X(S) \) is a bijection?

2.4. Let \( X \) be an \( S \)-scheme, and let \( U \) be an open subscheme. Prove that for any \( S \)-scheme \( T \), the set \( U(T) \) is the subset of \( X(T) \) consisting of \( S \)-morphisms \( f: T \to X \) such that \( f(T) \) is contained in \( U \) as a set.

2.5. Let \( F \) be the functor \( \textbf{Schemes}^{\text{opp}} \to \textbf{Sets} \) that maps each scheme \( X \) to \( \mathcal{O}_X(X)^\times \), and that maps a morphism \( f: X \to Y \) to the natural map \( \mathcal{O}_Y(Y)^\times \to \mathcal{O}_X(X)^\times \) induced from the ring homomorphism \( \mathcal{O}_Y(Y) \to \mathcal{O}_X(X) \). Prove that \( F \) is representable.
2.6. Let $S$ be a scheme with a morphism $\text{Spec} \, k \to S$ for some algebraically closed field $k$. Let $F : \text{Schemes}_S^{\text{op}} \to \text{Sets}$ be a functor. Prove that any fine moduli space for $F$ is also a coarse moduli space for $F$.

2.7. Fix $p, q, r \in \mathbb{Z}_{>0}$. A primitive integer solution to the generalized Fermat equation $x^p + y^q = z^r$ is one in which $x, y, z \in \mathbb{Z}$ and $\gcd(x, y, z) = 1$. Let $S = \text{Spec} \, \mathbb{Z}[x, y, z]/(x^p + y^q - z^r)$ and let $T$ be the closed subscheme $\text{Spec} \, \mathbb{Z}[x, y, z]/(x, y, z)$. Let $S' = S - T$, which is an open subscheme of $S$. Prove that $S'(\mathbb{Z})$ is in bijection with the set of primitive integer solutions to $x^p + y^q = z^r$.

2.8. Find a scheme $X$ over $\mathbb{Z}$ such that

$$X(A) \simeq \{(a, b) \in A^2 : a, b \text{ generate the unit ideal in } A\}$$

functorially in the ring $A$.

2.9. Give an example of an $S$-scheme $X$ with open subschemes $U$ and $V$ such that $U \cup V = X$ but $U(S) \cup V(S) \neq X(S)$.

2.10. Let $k$ be a field. Let $Y = \text{Spec} \, k[t]$. For $n \geq 1$, let $X_n$ be the closed subscheme $\text{Spec} \, k[t]/(t^n)$. Let $X = \coprod_{n \geq 1} X_n$. Let $f : X \to Y$ be the morphism that on each $X_n$ is the inclusion.

(a) Is $f$ dominant?
(b) Is $f$ scheme-theoretically dominant?
(c) Does $f$ factor through a closed subscheme of $Y$, other than $Y$ itself?

2.11. (Failure of descent) Let $k = \mathbb{Q}(\sqrt{2})$. Prove that there does not exist a variety $X$ over $\mathbb{Q}$ such that $X_k$ is isomorphic to the affine plane curve $x^2 + y^2 = \sqrt{2}$ over $k$.

2.12. Let $X$ be the nice curve $x^2 + y^2 + z^2 = 0$ in $\mathbb{P}^2_k$. Prove that the homomorphism $\text{Pic} \, X \to (\text{Pic} \, X_{\mathbb{C}})^{\text{Gal}(\mathbb{C}/\mathbb{R})}$ is not an isomorphism.

2.13. Let $X$ be a scheme of finite type over $\mathbb{F}_q$. Let $N_d$ be the number of degree $d$ closed points on $X$. Prove that $\sum_{d|n} dN_d = \#X(\mathbb{F}_{q^n})$ for each $n \geq 1$.

2.14. Use Möbius inversion to give a formula for the number of degree $n$ monic irreducible polynomials in $\mathbb{F}_q[t]$.

2.15. Assuming that the Serre duality theorem [Har77, III.7.7] holds over an arbitrary field $k$ (it does), prove the Riemann–Roch theorem (Theorem 2.5.3) for regular, projective, geometrically integral curves over $k$.

2.16. Give two examples of non-proper $\mathbb{R}$-varieties $X$ such that $X(\mathbb{R})$ is compact in the analytic topology, one with $X(\mathbb{R})$ empty and one with $X(\mathbb{R})$ nonempty.

2.17. Let $k$ be a global field. Let $X$ be a $k$-variety with a $k_v$-point for every $v$. Prove that $X$ satisfies weak approximation if and only if for every finite set $S$ of places and any nonempty open sets $U_v \subseteq X(k_v)$ for $v \in S$, there exists $x \in X(k)$ such that $x \in U_v$ for all $v \in S$. 
CHAPTER 3

Properties of morphisms

3.1. Finiteness conditions

3.1.1. Quasi-compact and quasi-separated morphisms.

Definition 3.1.1. [Har77, Exercise II.2.13] A scheme $X$ is quasi-compact if one of the following equivalent conditions is satisfied:

(i) The topological space of $X$ is quasi-compact: i.e., every open cover of $X$ has a finite subcover. (One says “quasi-compact” instead of just “compact” for clarity since some authors include “Hausdorff” as part of the latter.)

(ii) The scheme $X$ is a finite union of affine open subsets.

Definition 3.1.2. [EGA I, 6.6.1], [EGA IV, §1.1] A morphism of schemes $f : X \to S$ is quasi-compact if one of the following equivalent conditions is satisfied:

(i) There is an affine open covering $\{S_i\}$ of $S$ such that for each $i$, the scheme $f^{-1}S_i$ is quasi-compact.

(ii) For every affine open subset $U \subseteq S$, the scheme $f^{-1}U$ is quasi-compact.

Definition 3.1.3. [EGA IV, §1.2] A morphism of schemes $f : X \to S$ is quasi-separated if one of the following equivalent conditions is satisfied:

(i) There is an affine open covering $\{S_i\}$ of $S$ such that whenever $X_1, X_2$ are affine open subsets of $f^{-1}S_i$, the intersection $X_1 \cap X_2$ is a union of finitely many affine open subsets.

(ii) For every affine open $U \subseteq S$, and every affine open subsets $X_1, X_2 \subseteq f^{-1}U$, the intersection $X_1 \cap X_2$ is a union of finitely many affine open subsets.

(iii) The diagonal morphism $X \to X \times_S X$ is quasi-compact.

If $X$ is noetherian, then every open subscheme of $X$ is quasi-compact, so every morphism $X \to S$ is both quasi-compact and quasi-separated. Most theorems about noetherian schemes use only that the schemes are quasi-compact and quasi-separated.

Example 3.1.4. Let $A$ be a polynomial ring $k[x_1, x_2, \ldots]$ in countably many indeterminates over some field $k$. Let $P \in \text{Spec} A$ be the closed point corresponding to the maximal ideal $(x_1, x_2, \ldots)$. Let $U$ be the open subscheme of $\text{Spec} A$ obtained by removing $P$. Then the open subsets $D(x_i)$ of $\text{Spec} A$ form an open cover of $U$ with no finite subcover, so $U$ is not quasi-compact.
Example 3.1.5. With notation as in Exercise 3.1.4 let $X$ be “infinite-dimensional affine space with a doubled origin”, i.e., the scheme obtained by glueing two copies $X_1, X_2$ of $\text{Spec } A$ along the copy of $U$ in each. The identity morphisms $X_i \to \text{Spec } A$ glue to give a morphism $X \to \text{Spec } A$ that is not quasi-separated, since $X_1$ and $X_2$ are affine open subsets whose intersection is not quasi-compact.

3.1.2. Finitely presented algebras.

Definition 3.1.6. \([\text{EGA IV}, 1.4.1]\) Let $A$ be a commutative ring, and let $B$ be an $A$-algebra. Then $B$ is said to be a \textit{finitely presented} $A$-algebra (or \textit{of finite presentation over }$A$) if $B$ is isomorphic as $A$-algebra to $A[t_1, \ldots, t_n]/I$ for some $n \in \mathbb{N}$ and some finitely generated ideal $I$ of the polynomial ring $A[t_1, \ldots, t_n]$.

Remark 3.1.7. The only difference between “finitely generated” and “finitely presented” is the requirement in the latter that $I$ be finitely generated as an ideal.

Proposition 3.1.8. Let $A$ be a commutative ring. If an $A$-algebra $B$ is finitely presented, then it is finitely generated. The converse holds for noetherian $A$.

Proof. Remark 3.1.7 explains why “finitely presented” implies “finitely generated”. If $A$ is noetherian, the Hilbert basis theorem says that $A[t_1, \ldots, t_n]$ is noetherian, so any ideal $I$ in it is automatically finitely generated.

Over non-noetherian rings, the more restrictive notion “finitely presented” has better properties than “finitely generated” (which is synonymous with “of finite type”). Non-noetherian rings do come up in arithmetic geometry: for instance, the adèle ring of a global field is not noetherian.

Example 3.1.9. Let $k$ be a field, and let $A = k[x_1, x_2, \ldots]$. Then the $A$-ideal $I := (x_1, x_2, \ldots)$ is not finitely generated. One can show that the finitely generated $A$-algebra $A/I$ is not finitely presented: see Exercise 3.1.

3.1.3. Morphisms locally of finite presentation.

Definition 3.1.10. \([\text{EGA IV}, 1.4.2]\) Let $f: X \to S$ be a morphism of schemes, let $x \in X$, and let $s = f(x)$. Then one says that $f$ is \textit{locally of finite presentation} at $x$ if there exist affine open neighborhoods $V = \text{Spec } A$ of $s$ and $U = \text{Spec } B$ of $x$ such that $B$ is of finite presentation over $A$. One says that $f$ is \textit{locally of finite presentation} (or that the $S$-scheme $X$ is \textit{locally of finite presentation}) if $f$ is locally of finite presentation at every $x \in X$.

Remark 3.1.11. An $S$-scheme is locally of finite presentation if and only if “its functor of points commutes with taking direct limits of rings”. More precisely, an $S$-scheme $X$ is
locally of finite presentation if and only if for every filtered inverse system of affine $S$-schemes $(\text{Spec } A_i)$, the natural map $\lim \rightarrow X(A_i) \rightarrow X(\lim \rightarrow A_i)$ is a bijection [EGA IV$_3$ 8.14.2.1]. (See Definition 4.3.2 for the meaning of “affine $S$-scheme”.) This is a version of “spreading out”, to be discussed further in Section 3.2.

### 3.1.4. Morphisms of finite presentation.

**Definition 3.1.12.** [EGA IV$_1$ 1.6.1] A morphism $f: X \rightarrow S$ is of **finite presentation** if it is locally of finite presentation, quasi-compact, and quasi-separated.

The three conditions in the definition of “finite presentation” are there so that for each affine open subset $U = \text{Spec } A$ of $S$, the scheme $f^{-1}U$ admits a finite description, as we now explain. First, the fact that $f$ is locally of finite presentation implies that $f^{-1}U$ is covered by affine open subsets $V_i$, each of the form $\text{Spec } B$, where $B$ is isomorphic to an $A$-algebra of the form $A[t_1, \ldots, t_n]/(f_1, \ldots, f_m)$ for some polynomials $f_1, \ldots, f_m$. Second, the fact that $f$ is quasi-compact implies that only finitely many $V_i$ are needed. Third, the fact that $f$ is quasi-separated implies that the intersections $V_i \cap V_j$ are covered by finitely many affine subsets (each of finite presentation over $A$), so the data needed to glue the $V_i$ to form $f^{-1}U$ are describable by a finite collection of polynomial maps with coefficients in $A$.

**Remark 3.1.13.** Suppose that $S$ is locally noetherian. Then by Proposition 3.1.8, a morphism $f: X \rightarrow S$ is locally of finite presentation if and only if it is locally of finite type, and it is of finite presentation if and only if it is of finite type.

### 3.2. Spreading out

If $X$ is an affine $\mathbb{Q}$-variety, then for some $N \geq 1$ there exists an affine finite-type scheme $X'$ over $\mathbb{Z}[1/N]$ whose generic fiber $X_\mathbb{Q}$ is isomorphic to $X$: simply let $N$ be the product of the denominators appearing in the finitely many coefficients appearing in the finitely many polynomials defining $X$.

We can generalize this by replacing $\mathbb{Z}$ and $\mathbb{Q}$ by any integral scheme $S$ and its generic point, respectively. In general, the principle of “spreading out” is that for schemes of finite presentation, whatever happens over the generic point also happens over some open neighborhood of the generic point.

**Theorem 3.2.1 (Spreading out).** Let $S$ be an integral scheme, and let $K$ be its function field. Let “blah” denote a property for which a positive answer is listed in the “Spreading out” column of Table [I].

(i) (Spreading out schemes) Suppose that $X$ is a scheme of finite presentation over $K$. Then there exist a dense open subscheme $U \subseteq S$ and a scheme $X'$ of finite presentation over $U$ such that $X'_K \simeq X$. (See Figure [J].)
(ii) (Spreading out properties of schemes) Suppose that $\mathcal{X} \to S$ is of finite presentation. If $\mathcal{X}_K \to \text{Spec } K$ is blah, then there exists a dense open subscheme $U \subseteq S$ such that $\mathcal{X}_U \to U$ is blah.

(iii) (Spreading out morphisms) Suppose that $\mathcal{X}$ and $\mathcal{X}'$ are schemes of finite presentation over $S$, and $f: \mathcal{X}_K \to \mathcal{X}'_K$ is a $K$-morphism. Then there exists a dense open subscheme $U \subseteq S$ such that $f$ extends to a $U$-morphism $\mathcal{X}_U \to \mathcal{X}'_U$.

(iv) (Spreading out properties of morphisms) Let $f: \mathcal{X} \to \mathcal{X}'$ be an $S$-morphism between schemes of finite presentation over $S$. If $f: \mathcal{X}_K \to \mathcal{X}'_K$ is blah, then there exists a dense open subscheme $U \subseteq S$ such that $f|_U: \mathcal{X}_U \to \mathcal{X}'_U$ is blah.

**Sketch of proof.** In all parts, we may replace $S$ by an affine open neighborhood of the generic point to assume that $S = \text{Spec } R$.

First we prove (ii). Let $X$ be a $K$-scheme of finite presentation. As in Section 3.1.4, $X$ has a finite description involving only finitely many polynomials over $K$. Write each coefficient as a fraction of elements of $R$, and let $R'$ be the localization of $R$ obtained by adjoining the inverses of all the denominators that appear. Then the description of $X$ over $K$ as the scheme obtained by glueing certain affine pieces also makes sense as the description of a scheme $\mathcal{X}$ over $U := \text{Spec } R'$, which is what we needed.

The proof of (iii) is similar to that of (ii).
Part (iv), on the other hand, requires a separate proof for each possibility for blah. See Table 1 for references.

Part (i) is the special case of (iv) with \( X' = S \).

Remark 3.2.2 (Spreading out to an open neighborhood of a point). Theorem 3.2.1 can be generalized as follows. Let \( S \) be any scheme, and let \( s \in S \). Then a scheme \( X \) of finite presentation over \( \text{Spec} \, \mathcal{O}_{S,s} \) can be spread out to a scheme \( X' \) of finite presentation over some open neighborhood of \( s \) in \( S \). The other parts of Theorem 3.2.1 generalize similarly.

Remark 3.2.3. The ring \( \mathcal{O}_{S,s} \) is the injective limit of the coordinate rings of the affine open neighborhoods of \( s \) in \( S \), so \( \text{Spec} \, \mathcal{O}_{S,s} \) is a projective limit of schemes. This suggests an even more general version of Theorem 3.2.1 for projective limits of schemes. This is the setting considered in [EGA IV, §8.10].

In the following sections, we give some standard applications of spreading out.

3.2.1. Reducing statements to the noetherian case.

Proposition 3.2.4. Suppose that \( X \) is of finite presentation over a commutative ring \( A \). Then there exists a noetherian ring \( A_0 \) contained in \( A \) and a scheme \( X_0 \) of finite presentation over \( A_0 \) whose base extension \( (X_0)_A \) is isomorphic to \( X \).

Proof. Any \( A \) is the direct limit (union) of its finitely generated subrings \( A_0 \). By Remark 3.2.3, \( X \simeq (X_0)_A \) for some scheme \( X_0 \) of finite presentation over a finitely generated ring \( A_0 \). (Concretely, one can take \( A_0 \) to be the \( \mathbb{Z} \)-subalgebra of \( A \) generated by the finitely many coefficients in a description of \( X \).) Now \( \mathbb{Z} \) is noetherian, so \( A_0 \) is noetherian too.

3.2.2. Specialization arguments. If \( X \) and \( Y \) are \( \mathbb{Q} \)-varieties whose base extensions \( X_{\mathbb{Q}(t)} \) and \( Y_{\mathbb{Q}(t)} \) are isomorphic, where \( t \) is an indeterminate, then one can specialize \( t \) to some rational number \( q \), chosen carefully to avoid the poles of the finitely many rational functions appearing in the description of the isomorphism, to obtain an isomorphism \( X \to Y \). This idea extends to the following.

Proposition 3.2.5 (Specializing an isomorphism). Let \( k \subseteq L \) be an arbitrary extension of fields. Let \( X \) and \( Y \) be \( k \)-varieties such that \( X_L \simeq Y_L \). Then \( X_F \simeq Y_F \) for some finite extension \( F \supseteq k \).

Proof. Let \( f : X_L \to Y_L \) be an isomorphism. The field \( L \) is the direct limit of its finitely generated \( k \)-subalgebras \( A \). By Remark 3.2.3, \( f \) is the base extension of an isomorphism \( f_A : X_A \to Y_A \). Let \( \mathfrak{m} \) be a maximal ideal of \( A \), and let \( F := A/\mathfrak{m} \). By the weak Nullstellensatz, \( F \) is a finite extension of \( k \). Reducing \( f_A \) modulo \( \mathfrak{m} \) (i.e., taking the base change by \( \text{Spec} \, A/\mathfrak{m} \to \text{Spec} \, A \)) yields an isomorphism \( X_F \to Y_F \).
The same technique reduces many questions about varieties over an arbitrary field to the case in which the field is a number field or a finite field, depending on the characteristic. In fact, by using the arithmetic weak Nullstellensatz (Remark 2.4.5 that the quotient of a finitely generated \( \mathbb{Z} \)-algebra by a maximal ideal is a finite field), even the characteristic 0 case can often be reduced to the finite field case.

Alternatively, after using spreading out to pass from a general field of characteristic 0 to the case of a finitely generated field \( K \supseteq \mathbb{Q} \), one can often use a theorem that any such \( K \) embeds in \( \mathbb{Q}_p \) for infinitely many primes \( p \) [Cas86, Chapter 5, Theorem 1.1], in order to reduce to a question over \( \mathbb{Q}_p \) for a suitable \( p \).

3.2.3. Models over discrete valuation rings. Let \( R \) be a discrete valuation ring, with fraction field \( K \), residue field \( k \), and uniformizer \( \pi \). (For instance, we could have \( R = \mathbb{Z}_p \), \( K = \mathbb{Q}_p \), \( k = \mathbb{F}_p \), \( \pi = p \).) Let \( X \) be a proper \( K \)-variety. We want to make sense of the reduction of \( X \) modulo \( \pi \), which should be a \( k \)-variety.

For a projective \( K \)-variety \( X \), the lowbrow approach is to scale each defining equation of \( X \) by a power of \( \pi \) so that its coefficients lie in \( R \) but not all in the maximal ideal (this procedure is sometimes called “chasing denominators”), and then reduce all the coefficients modulo \( \pi \). The isomorphism class of the \( k \)-variety defined by the resulting equations depends not only on the isomorphism class of \( X \), but also on the choice of defining equations.

We want to reinterpret this construction in terms of \( R \)-schemes. The scheme \( \text{Spec} \, R \) consists of two points: the generic point \( \eta = \text{Spec} \, K \) corresponding to the prime \( (0) \) of \( R \), and the special point or closed point \( s = \text{Spec} \, k \) corresponding to the maximal ideal \( (\pi) \) of \( R \).

Definition 3.2.6. Let \( X_R \) be an \( R \)-scheme. The generic fiber of \( X_R \) is the \( K \)-scheme \( X_K = X_R \times_{\text{Spec} \, R} \text{Spec} \, K \), and the special fiber of \( X_R \) is the \( k \)-scheme \( X_k = X_R \times_{\text{Spec} \, R} \text{Spec} \, k \).

Remark 3.2.7. Schemes of finite type over discrete valuation rings or rings of \( S \)-integers of number fields are often called arithmetic schemes (if they satisfy other technical conditions depending on the author). In the special case where the relative dimension is 1, they are called arithmetic surfaces, because the base is a ring of dimension 1.

Definition 3.2.8. An \( R \)-model of a \( K \)-scheme \( X \) is an \( R \)-scheme \( X_R \) equipped with an isomorphism \( X_R \times_R K \cong X \) of \( K \)-schemes.

Example 3.2.9. Let \( X \) be the \( \mathbb{Q}_7 \)-curve \( \text{Proj} \, \mathbb{Q}_7[x, y, z]/(xy - 7z^2) \). Then \( \text{Proj} \, \mathbb{Z}_7[x, y, z]/(xy - 7z^2) \) and \( \text{Proj} \, \mathbb{Z}_7[x, y, z]/(xy - z^2) \) (equipped with suitable isomorphisms) are \( \mathbb{Z}_7 \)-models of \( X \). They are not isomorphic, however, as one can see from their special fibers. See Figure 2.

According to Definition 3.2.8, \( X \) itself is yet another \( \mathbb{Z}_7 \)-model of \( X \).

Now, a “reduction modulo \( \pi \) of a \( K \)-variety \( X \)” can be understood as the special fiber of an \( R \)-model of \( X \). Example 3.2.9 shows, however, that to get a reasonable result, one should impose additional restrictions on the model. We will do so in Section 3.5.14.
3.2.4. Models over Dedekind domains and schemes. Definition 3.2.8 makes sense for any integral domain $R$. A common situation, generalizing the discrete valuation ring case, is where $R$ is a Dedekind domain, that is, an integrally closed noetherian domain of dimension $\leq 1$. The main examples of such $R$ are

1. the integer ring $\mathbb{Z}$, or more generally the ring of integers $\mathcal{O}_K$ of a number field,
2. the coordinate ring of an affine regular integral curve over a field, and
3. localizations of the above.

A scheme over a Dedekind domain has one generic fiber, and many closed fibers, one for each nonzero prime of $R$.

Remark 3.2.10. One can generalize even further, to integral Dedekind schemes. A Dedekind scheme is a noetherian normal scheme of dimension $\leq 1$. Examples include

(i) $\text{Spec } R$ for any Dedekind domain $R$,
(ii) regular curves over a field, and
(iii) \( X \setminus \{ x \} \), where \( X \) is a normal noetherian local scheme of dimension 2 and \( x \) is its closed point. (A scheme \( X \) is \textit{local} if it has exactly one closed point \( x \), and \( x \) is in the closure of \( \{ y \} \) for all \( y \in X \).) For example, \( X \) could be \( \text{Spec } k[s,t]_m \) where \( k \) is a field and \( m \) is the ideal \((s,t)\).

By Lemma 3.2.11(i)⇒(iii) below, any Dedekind scheme \( X \) is a disjoint union of integral Dedekind schemes, and their number is finite since \( X \) is noetherian. Also, any Dedekind scheme is covered by finitely many open sets of the form \( \text{Spec } R \) for Dedekind domains \( R \).

**Lemma 3.2.11.** For a locally noetherian scheme \( X \), the following are equivalent:

(i) For every \( x \in X \), the local ring \( \mathcal{O}_{X,x} \) is an integral domain.

(ii) The scheme \( X \) is \textit{locally integral}: every point has an open neighborhood that is an integral scheme.

(iii) The scheme \( X \) is a disjoint union of integral schemes.

**Proof.** The implications (iii)⇒(ii) and (ii)⇒(i) are trivial. It remains to prove (i)⇒(iii).

Suppose that each local ring \( \mathcal{O}_{X,x} \) is an integral domain; then each \( \mathcal{O}_{x,x} \) is reduced, so \( X \) is reduced. Since irreducible and reduced together imply integral, it remains to show that the irreducible components of \( X \) are disjoint. The irreducible components passing through a given point \( x \) are in bijection with the the minimal primes of \( \mathcal{O}_{X,x} \), of which there is just one (the zero ideal). Thus each \( x \) lies in exactly one irreducible component; i.e., the irreducible components are disjoint. \( \square \)

**3.2.5. Valuative criterion for properness.** Return to the setting of Section 3.2.3 where \( R \) is a discrete valuation ring. Suppose that we have extended a \( K \)-scheme to an \( R \)-model. We now wish to speak of reducing \( K \)-points on the generic fiber to \( k \)-points of the special fiber. There is no homomorphism \( K \to k \), so to make sense of this, we must first extend the \( K \)-point to an \( R \)-point of the model. For a proper scheme over a discrete valuation ring, this extension is always possible (and unique), by the \( S = \text{Spec } R \) case of one direction of the following:

**Theorem 3.2.12** (Valuative criterion for properness [Har77] II.4.7 and Exercise II.4.11]). Let \( f : X \to S \) be a morphism of finite type with \( S \) noetherian. Then \( f \) is proper if and only if whenever \( \text{Spec } R \) is an \( S \)-scheme with \( R \) a discrete valuation ring and \( K \) its fraction field, the natural map \( X(R) \to X(K) \) is bijective.

We generalize the \( S = \text{Spec } R \) case to Dedekind domains as part (ii) of the following:

**Theorem 3.2.13.** Let \( R \) be an integral domain, and let \( K = \text{Frac } R \). Let \( X \) be an \( R \)-scheme.

(i) If \( X \) is separated over \( R \), then \( X(R) \to X(K) \) is injective.

58
(ii) If $X$ is proper over $R$, and $R$ is a Dedekind domain, then $X(R) \to X(K)$ is bijective.

**Proof.**

(i) This is a special case of Corollary 2.3.22.

(ii) Proper schemes over $R$ or $K$ are of finite type, hence of finite presentation, since $R$ and $K$ are noetherian rings. Let $f \in X(K)$. We need to extend $f : \text{Spec } K \to X$ to an $R$-morphism $\text{Spec } R \to X$. Apply Theorem 3.2.1(iii) to find a dense open subscheme $U \subseteq \text{Spec } R$ such that $f$ extends to a $U$-morphism $f_U : U \to X_U$, or equivalently, an $R$-morphism $f_U : U \to X$. Since $R$ is noetherian of dimension $\leq 1$, the complement $(\text{Spec } R) - U$ is a finite union of closed points $p$. It suffices to extend $f_U$ to $U \cup \{p\} \to X$ for one $p$, since then we can repeat the extension argument for each missing point.

By Theorem 3.2.12, we can extend $f$ to a morphism $\text{Spec } R_p \to X$, and apply Remark 3.2.2 to spread it out to an $R$-morphism $f_V : V \to X_V \subseteq X$ for some dense open $V \subseteq \text{Spec } R$. The restrictions of $f_U$ and $f_V$ to $U \cap V$ must agree, by part (i) applied to each ring used in an affine cover of $U \cap V$. Thus we can glue to obtain an extension of $f$ to $U \cap V$, which contains both $U$ and $p$. □

**Remark 3.2.14.** The same argument proves Theorem 3.2.13 more generally when $R$ is replaced by an integral Dedekind scheme with function field $K$. Even more generally, if $X$ is a separated (resp. proper) $S$-scheme, and $T$ is an integral Dedekind scheme with a morphism to $S$, and $K = k(T)$, then $X(T) \to X(K)$ is an injection (resp. bijection): this statement can be reduced to the previous sentence by Proposition 2.3.15. For an important application, see Proposition 3.6.5(b).

**Warning 3.2.15.** Theorem 3.2.13(ii) does not hold for arbitrary integral domains $R$: see Exercise 3.3.

### 3.3. Flat morphisms

#### 3.3.1. Flat modules.

(References: [Har77, III.9] and [BLR90, §2.4])

**Definition 3.3.1.** Let $A$ be a commutative ring, and let $B$ be an $A$-module. Then $B$ is flat if the functor $\otimes_A B$ is exact: that is, whenever

$$0 \to M' \to M \to M'' \to 0$$

is an exact sequence of $A$-modules, the induced sequence

$$0 \to M' \otimes_A B \to M \otimes_A B \to M'' \otimes_A B \to 0$$

is exact.

59
Examples 3.3.2.

(i) Free modules are flat. In particular, any module over a field \( k \) (that is, a vector space) is flat.

(ii) A module over a discrete valuation ring or Dedekind domain is flat if and only if it is torsion-free.

(iii) Any localization \( S^{-1}A \) of \( A \) is flat.

3.3.2. Flat and faithfully flat morphisms.

Definition 3.3.3. A morphism of schemes \( f: X \to Y \) is flat at a point \( x \in X \) if \( \mathcal{O}_{X,x} \) is flat as an \( \mathcal{O}_{Y,f(x)} \)-module. Also, \( f \) is called flat if \( f \) is flat at every \( x \in X \).

Definition 3.3.4. A morphism of schemes \( f: X \to Y \) is faithfully flat if \( f \) is flat and surjective.

Remark 3.3.5. Let \( A \to B \) be a homomorphism of commutative rings. Then \( \text{Spec} B \to \text{Spec} A \) is flat if and only if \( B \) is flat over \( A \). Also, \( \text{Spec} B \to \text{Spec} A \) is faithfully flat if and only if \( B \) is flat over \( A \) and for any nonzero \( A \)-module \( M \) one has \( M \otimes_A B \neq 0 \). This explains the use of the word “faithfully”.

3.3.3. Dimension and relative dimension.

Definition 3.3.6. [EGA IV] Chapter 0, 14.1.2] Let \( X \) be a topological space. Its dimension \( \dim X \in \{-\infty, 0, 1, 2, \ldots, \infty\} \) is the supremum of the set of nonnegative integers \( n \) for which there exists an \( n \)-step chain \( X_0 \subset X_1 \subset \cdots \subset X_n \) of irreducible closed subsets of \( X \). If \( x \in X \), define the dimension of \( X \) at \( x \) as

\[
\dim_x X := \inf \{ \dim U : U \text{ is an open neighborhood of } x \text{ in } X \}. 
\]

Remark 3.3.7. The empty space is not irreducible. We have \( \dim X = -\infty \) if and only if \( X = \emptyset \).

Warning 3.3.8. The definition of \( \dim_x X \) differs from the definition in [Har77] III.9.5] for schemes, where it is defined as \( \dim \mathcal{O}_{X,x} \). For example, if \( x \) is the generic point of an integral \( k \)-variety \( X \), then \( \dim_x X = \dim X \) according to the definition above from [EGA IV] Chapter 0, 14.1.2], but \( \dim \mathcal{O}_{X,x} = 0 \) since \( \mathcal{O}_{X,x} \) is a field. See Theorem 3.3.10 for the relationship more generally.

Example 3.3.9. Let \( X \subseteq \mathbb{A}^3_k = \text{Spec} k[x,y,z] \) be the union of the plane \( z = 0 \) and the line \( x = y = 0 \), over a field \( k \). Let \( P \) be the point \((0,0,1)\) of \( X \). Then \( \dim X = 2 \), but \( \dim_P X = 1 \). See Figure 3.
THEOREM 3.3.10. Let $X$ be a scheme that is locally of finite type over a field $k$. Let $x \in X$. Then

$$\dim_x X = \dim \mathcal{O}_{X,x} + \text{tr deg}(k(x)/k).$$

PROOF. See [EGA IV$_2$] 5.2.3. □

DEFINITION 3.3.11. If $f : X \to S$ is a continuous map of topological spaces, and $x \in X$, define the relative dimension of $X$ over $S$ at $x$ as $\dim_x f := \dim_x f^{-1}(f(x))$.

PROPOSITION 3.3.12. Let $f : X \to S$ be a flat $k$-morphism between irreducible $k$-varieties. Then $\dim_x f = \dim X - \dim S$. In particular, $\dim_x f$ is independent of $x$.

PROOF. This is a special case of [Har77, III.9.6]. □

3.4. Fppf and fpqc morphisms

(Reference: [Vis05] §2.3)

The notions in this section will play an important role in the definition of “topologies” finer than the Zariski topology, for use in faithfully flat descent (Chapter 4) and in the construction of cohomology theories (Chapter 6).

DEFINITION 3.4.1. A morphism of schemes $X \to Y$ is fppf if it is faithfully flat and locally of finite presentation.

PROPOSITION 3.4.2. A morphism $f : X \to Y$ that is flat and locally of finite presentation is open; i.e., for every open subset $U \subseteq X$, the set $f(U)$ is open in $Y$.

PROOF. Here is a very brief sketch:
(1) Reduce to proving that $f(X)$ is open in $Y$ when $X$ and $Y$ are affine and $X \to Y$ is of finite presentation.

(2) Use Proposition 3.2.4 to assume moreover that $Y$ is noetherian.

(3) Chevalley’s theorem states for a finite-type morphism between noetherian schemes, $f(X)$ is constructible, i.e., a finite boolean combination of open subsets.

(4) Flatness implies that $f(X)$ is stable under generization; i.e., if $y_1, y_2 \in Y$ are such that the closure of $y_1$ in $Y$ contains $y_2$, and $y_2 \in f(X)$, then $y_1 \in f(X)$.

(5) In a noetherian scheme, a subset is open if and only if it is constructible and stable under generization [Har77, Exercise II.3.18(c)].

See [EGA IV$_2$, 2.4.6] for details.

**Definition 3.4.3** (Kleiman [Vis05, 2.34]). A morphism of schemes $X \to Y$ is fpqc if it is faithfully flat and every quasi-compact open subset of $Y$ is the image of a quasi-compact open subset of $X$.

**Example 3.4.4.** Let $Y$ be a positive-dimensional $k$-variety. For each $y \in Y$, there is a morphism $\text{Spec} \mathcal{O}_{Y,y} \to Y$. Let $X$ be the disjoint union $\coprod_{y \in Y} \text{Spec} \mathcal{O}_{Y,y}$. Then the natural morphism $X \to Y$ is faithfully flat but not fpqc.

**Remark 3.4.5.** Both fppf and fpqc are French acronyms: fppf stands for “fidèlement plat de présentation finie” and fpqc stands for “fidèlement plat quasi-compact”. Our (slightly nonstandard) definitions of fppf and fpqc are less restrictive than a direct translation would suggest; this is so that fppf and fpqc morphisms include Zariski open covering morphisms. See Proposition 3.8.2.

### 3.5. Smooth and étale morphisms

(Reference: [MO15, 5.3–5.4], [Ray70a], [BLR90, §2.2])

Section I.5 of [Har77] gives two equivalent definitions of “nonsingular” for varieties over an algebraically closed field. These definitions disagree over imperfect fields, so we will avoid the term “nonsingular”, and instead use “regular” and “smooth” for the two distinct notions.

**3.5.1. Regular schemes.** Recall the following definition:

**Definition 3.5.1.** A scheme $X$ is regular if $X$ is locally noetherian and $\mathcal{O}_{X,x}$ is a regular local ring for every $x \in X$.

**Remark 3.5.2.** The localization of a regular local ring at a prime ideal is a regular local ring [Eis95, 19.14]. Thus, for $X$ locally of finite type over a field or over $\mathbb{Z}$, one gets an equivalent definition if one checks the local rings at only the closed points $x$. 

62
Remark 3.5.3. Definition 3.5.1 agrees with the definition of nonsingular given on page 32 (resp. page 177) of [Har77] for quasi-projective integral schemes (resp. integral varieties) over an algebraically closed field $k$.

Remark 3.5.4. “Regular” is an absolute notion: if $X$ is an $S$-scheme, the question of whether $X$ is regular ignores the structure morphism $X \to S$. In contrast, “smooth” is relative: we will speak of an $S$-scheme $X$ being smooth over $S$, and this does depend on more than the structure of $X$ as a scheme.

Proposition 3.5.5. A regular scheme is a disjoint union of integral schemes.

Proof. Regular local rings are integral domains [Eis95, Corollary 10.14]. Apply Lemma 3.2.11. □

Corollary 3.5.6. A connected regular scheme is integral.

3.5.2. Inspiration from differential geometry. (This section is purely motivational.) The notion of smooth variety is an algebraic version of the notion of (smooth) manifold. In particular, we want the definition to have the following property: for a $\mathbb{C}$-variety $X$,

\[(3.5.7) \quad X \text{ is smooth over } \mathbb{C} \iff X^{an} \text{ is a manifold},\]

where the condition on the right means that $X^{an}$ can be covered by open subsets isomorphic as complex analytic spaces to open subsets of $\mathbb{C}^n$.

Warning 3.5.8. It is not enough to require that $X(\mathbb{C})$ be locally isomorphic as topological space to open subsets of $\mathbb{C}^n$: one problem with this is that this would not distinguish $X$ from its associated reduced variety $X_{\text{red}}$. Nonreduced varieties should never be considered smooth.

Stupid idea 3.5.9. We might try adapting the definition of manifold to the algebraic setting, and come up with the following “definition”:

“A $\mathbb{C}$-variety is smooth of dimension $r$ if and only if it is covered by Zariski open subschemes each isomorphic to an open subscheme of $\mathbb{A}_\mathbb{C}^r$.”

But this would be wrong, in the sense that it would violate (3.5.7): if $X$ is defined by $x^3 + y^3 = 1$ in $\mathbb{A}_\mathbb{C}^2$, then $X^{an}$ is a manifold, so $X$ should be smooth, but it turns out that $X$ is not birational to affine space, so it does not satisfy the “definition”. The Zariski topology is simply too coarse: not enough open sets.

Remark 3.5.10. Stupid idea 3.5.9 actually works if one uses the étale topology instead of the Zariski topology. But the definition of the étale topology requires the notion of étale morphism, which we have not yet defined. And in fact, one definition of étale morphism depends on the definition of smooth.
There is a different characterization of manifolds that does adapt well to the algebraic setting. A subset \( X \subseteq \mathbb{C}^n \) is a complex manifold of dimension \( r \) if and only if in a neighborhood of each \( x \in X \) it is locally the intersection of \( n - r \) analytic hypersurfaces \( H_{r+1}, \ldots, H_n \) meeting transversely. Here each \( H_i \) is defined as the zero set of a holomorphic function \( g_i \) defined on a neighborhood of \( x \) in \( \mathbb{C}^n \). The condition that the hypersurfaces meet transversely at \( x \) means that the \( n - r \) tangent spaces \( T_x H_i \) at \( x \) (each a subspace of codimension \( \leq 1 \) of the tangent space \( T_x \mathbb{C}^n \)) intersect in a subspace of codimension \( n - r \), that is, dimension \( r \). Dually, this means that the differentials \( dg_i(x) \) evaluated at \( x \) are linearly independent in the cotangent space of \( \mathbb{C}^n \) at \( x \). In terms of coordinates \( t_1, \ldots, t_n \) on \( \mathbb{C}^n \), this means that the rows of the \( (n - r) \times n \) Jacobian matrix \( J \) with entries \( J_{ij} := \frac{\partial g_i}{\partial t_j} \) evaluated at \( x \) are independent. In other words, \( J \) has rank \( n - r \) when evaluated at \( x \).

**Remark 3.5.11.** It is the implicit function theorem that shows that the linear independence of differentials makes \( X \) a manifold. More explicitly, if one extends the list \( g_{r+1}, \ldots, g_n \) to a list of holomorphic functions \( g_1, \ldots, g_n \) in a neighborhood of \( x \) in \( \mathbb{C}^n \) such that \( dg_1(x), \ldots, dg_n(x) \) form a basis for the cotangent space of \( \mathbb{C}^n \) at \( x \), then \( (g_1, \ldots, g_r) \) defines a biholomorphic map between an open neighborhood of \( x \) in \( X \) and an open subset of \( \mathbb{C}^r \). The functions \( g_1, \ldots, g_r \) restricted to \( X \) (or rather, to the open neighborhood of \( x \) in \( X \) on which they are defined) are called **local coordinates** at \( x \), because they correspond under the biholomorphic map to the standard coordinates on (an open subset of) \( \mathbb{C}^n \).

**3.5.3. Summary of the definitions of smooth.** A definition of “smooth” for morphisms \( X \to S \) between schemes of finite type over a field is given in [Har77, III.10], but in arithmetic geometry it is sometimes necessary to work in greater generality: for instance, \( S \) might be \( \text{Spec} \mathbb{Z}_p \).

So we want to define what it means for a morphism of schemes \( f : X \to S \) to be smooth, or in other words, what it means for an \( S \)-scheme \( X \) to be smooth (over \( S \)). There are several approaches, yielding equivalent definitions, each with its own virtues. We summarize three of them here:

1. **Generalize the differential criterion given at the beginning of [Har77, I.5] to make everything relative to a base scheme \( S \) instead of Spek.** This definition yields a practical criterion for testing smoothness. A variant of it is used as a starting point in [BLR90, §2.2]. See Section 3.5.4.

2. **Work fiber by fiber.** Roughly, first define a \( k \)-variety \( X \) to be smooth if and only if it is geometrically regular; then define a morphism \( f : X \to S \) to be smooth if and only if the fiber \( f^{-1}(s) \) is smooth over the residue field \( k(s) \) for each \( s \in S \). Actually in the first step one should work more generally with \( X \) locally of finite type over a field, and then for morphisms to an arbitrary \( S \), one needs technical conditions (locally of finite presentation, and flat) to make sure that the fibers are locally of
finite type and that the fibers form a decent family, respectively. This definition provides perhaps the clearest visualization of what a smooth $S$-scheme looks like, but is not as useful as a starting point for proving things. See Section 3.5.6.

(3) Characterize smooth morphisms by the “infinitesimal lifting property”. This definition, due to Grothendieck, is elegant, though less intuitive. Also, variants give definitions of the related adjectives G-unramified and étale. See Section 3.5.12.

3.5.4. Definition 1 of smooth: the differential criterion.

**Definition 3.5.12.** Let $r \in \mathbb{N}$. Let $f : X \to S$ be a morphism of schemes, and let $x \in X$.

(i) (Special case) Suppose that $f$ is

$$
\text{Spec} \frac{A[t_1, \ldots, t_n]}{(g_{r+1}, \ldots, g_n)} \longrightarrow \text{Spec} A.
$$

Then $f$ is **obviously smooth of relative dimension** $r$ at $x$ if and only if the matrix

$$
\left( \frac{\partial g_i}{\partial t_j} (x) \right) \in M_{n-r \times n}(k(x))
$$

has rank $n - r$.

(ii) (General case) An arbitrary $f$ is **smooth of relative dimension** $r$ at $x$ if and only if there exist open neighborhoods $U \subseteq X$ of $x$ and $V \subseteq S$ of $f(x)$ such that $f(U) \subseteq V$ and $f|_U : U \to V$ is isomorphic to a morphism that is obviously smooth of relative dimension $r$ at $x$.

**Remark 3.5.13.** For an $A$-morphism

$$
X := \text{Spec} \frac{A[t_1, \ldots, t_n]}{(g_{r+1}, \ldots, g_n)} \overset{f}{\longrightarrow} \text{Spec} A,
$$

$f$ is smooth of relative dimension $r$ at $x$ if and only if $f$ is obviously smooth of relative dimension $r$ at $x$. (One way to prove this is to give an intrinsic characterization of “obviously smooth”: e.g., $f$ as above is obviously smooth of relative dimension $r$ at $x$ if and only if $\mathcal{O}_{X,k(x),x}$ is a regular local ring.) Thus we can dispense with the made-up terminology “obviously smooth” and just say “smooth” from now on.

**Definition 3.5.14.** Let $f : X \to S$ be a morphism of schemes. We say that $X$ is **smooth over** $S$, or that $X$ is a **smooth $S$-scheme**, or that $f$ is **smooth**, if at each $x \in X$ the morphism is smooth of some relative dimension.

**Remark 3.5.15.** If $f : X \to S$ is smooth of relative dimension $r$ at $x$, then $f$ is of relative dimension $r$ at $x$. (In proving this, one can reduce first to the special case, and then to the case where $S = \text{Spec} k$ for a field $k$.)
Definition 3.5.16. The smooth locus of $f : X \to S$ is the subset

$$X^{\text{smooth}} := \{ x \in X : f \text{ is smooth at } x \} \subseteq X.$$ 

Its complement $X^{\text{sing}} := X - X^{\text{smooth}}$ is called the singular locus or nonsmooth locus.

Proposition 3.5.17. The subset $X^{\text{smooth}}$ is open in $X$.

Proof. We may assume we are in the special case of Definition 3.5.12. If the matrix of derivatives has maximal rank $n - r$ at a point $x$, then some $(n - r) \times (n - r)$ minor is nonvanishing at $x$, and will be nonvanishing in some open neighborhood $U$ of $x$. Then $U \subseteq X^{\text{smooth}}$. □

Warning 3.5.18. The smooth locus can be empty, even for nonempty varieties over a field. See Example 3.5.64.

Proposition 3.5.19. If $X \to S$ is smooth of relative dimension $r$, then the $\mathcal{O}_X$-module $\Omega_{X/S}$ is locally free of rank $r$.

Proof. The construction of $\Omega_{X/S}$ is local on $X$ and $S$, so we may reduce to the special case of Definition 3.5.12 and may assume that a particular $(n - r) \times (n - r)$ minor of $\left( \frac{\partial g_i}{\partial t_j}(x) \right)$ is a unit in $B := A[t_1, \ldots, t_n]/(g_{r+1}, \ldots, g_n)$. By [Eis95, §16.1], $\Omega_{B/A}$ is the quotient of the free $B$-module with basis $dt_1, \ldots, dt_n$ by the relations $\sum_{j=1}^n \frac{\partial g_i}{\partial t_j} dt_j$ for $i = r + 1, \ldots, n$. This quotient is a free $B$-module of rank $r$, with basis consisting of the $dt_j$ for which the index $j$ is not involved in the $(n - r) \times (n - r)$ minor above. □

Remark 3.5.20. There is a partial converse to Proposition 3.5.19. Suppose that $f : X \to S$ is a flat morphism between irreducible $k$-varieties. Let $r := \dim X - \dim S$. Then $f$ is smooth of relative dimension $r$ if and only if $\Omega_{X/S}$ is locally free of rank $r$.

Warning 3.5.21. If $\Omega_{X/S}$ is locally free of the wrong rank, then $X \to S$ is not smooth. For example, if $k$ is a field of characteristic $p$, then the $0$-dimensional irreducible $k$-scheme $X := \text{Spec } k[\epsilon]/(\epsilon^p)$ has $\Omega_{X/k}$ locally free of rank $1$. This $X$ is not smooth (of any relative dimension) over $k$.

3.5.5. Smooth vs. regular. The relationship between “smooth” and “regular” over arbitrary fields is given by the following generalization of [Har77, I.5.1]:

Proposition 3.5.22. Let $X$ be locally of finite type over a field $k$.

(i) $X$ is smooth if and only if $X$ is geometrically regular.

(ii) If $X$ is smooth, then $X$ is regular; the converse holds if $k$ is perfect.

(iii) For a closed point $x \in X$ with $k(x)/k$ separable, the variety $X$ is smooth at $x$ if and only if $X$ is regular at $x$ (i.e., $\mathcal{O}_{X,x}$ is a regular local ring).
Example 3.5.23 (Regular variety that is not smooth). Let $k$ be the imperfect field $\mathbb{F}_p(t)$, where $p$ is odd and $t$ is an indeterminate. Let $X$ be the curve $y^2 = x^p - t$ in $\mathbb{A}^2_k$, so $X = \text{Spec } k[x, y]/(f)$ with $f := y^2 - (x^p - t)$. Since $f$ is irreducible even in $\overline{k}[x, y]$, the curve $X$ is geometrically integral. We will show that $X$ is regular but not smooth. Let $P$ be the closed point of $X$ corresponding to the maximal ideal $(x^p - t, y)$ of $k[x, y]$. The subscheme of $X$ defined by $f = \partial f/\partial x = \partial f/\partial y = 0$ is $\{P\}$, so $X$ is smooth everywhere except at $P$ (where it is definitely not smooth). This implies that $X$ is regular except possibly at $P$, but we will find that $X$ is regular even at $P$. Let $\mathfrak{m}_P$ be the maximal ideal of $O_{X, P}$, so $k(P) := O_{X, P}/\mathfrak{m}_P \simeq k[x, y]/(x^p - t, y)$. We must compute the $k(P)$-dimension of

$$\frac{\mathfrak{m}_P}{\mathfrak{m}_P^2} \simeq \frac{(x^p - t, y)}{(x^p - t, y)^2 + (f)}.$$  

Now $\frac{(x^p - t, y)}{(x^p - t, y)^2}$ is a 2-dimensional $k(P)$-vector space spanned by $x^p - t$ and $y$ (not surprising, given that $\mathbb{A}^2_k$ is regular of dimension 2), and the image of $f$ in this vector space is nonzero, so

$$\dim \frac{\mathfrak{m}_P}{\mathfrak{m}_P^2} = \dim \frac{(x^p - t, y)}{(x^p - t, y)^2 + (f)} = 1 = \dim X = \dim O_{X, P}.$$  

Thus $O_{X, P}$ is a regular local ring. So $X$ is regular at $P$.

To summarize, $X$ is regular, and smooth everywhere except at $P$. By Proposition 3.5.22, $X$ is not geometrically regular: this can also be checked directly, by examining the point on $X_\overline{k}$ corresponding to the maximal ideal $(x - t^{1/p}, y)$ of $\overline{k}[x, y]$.

Example 3.5.24. Let $k$ be a field, let $S = \mathbb{A}^1_k = \text{Spec } k[t]$, and let $X$ be the $S$-scheme $\text{Spec } k[t][x, y]/(xy - t)$. In other words, $X$ is a family of hyperbolas depending on a parameter $t$, which degenerates to a union of two lines when $t = 0$. The Jacobian matrix for $X \to S$ is

$$\begin{pmatrix} y & x \end{pmatrix}.$$  

Thus the nonsmooth locus of $X \to S$ is the subscheme $y = x = xy - t = 0$ of $\text{Spec } k[t][x, y] = \mathbb{A}^3_k$. This consists of the single point $(0, 0, 0) \in \mathbb{A}^3(k)$. In other words, all the fibers of $X \to S$ are smooth except for the fiber above $t = 0$, which has a single singularity.

Although $X$ is not smooth over $S$, we have $k[t][x, y]/(xy - t) \simeq k[x, y]$ so $X \simeq \mathbb{A}^2_k$ (the projection $\mathbb{A}^3_k \to \mathbb{A}^2_k$ to the $(x, y)$-plane maps $X$ isomorphically onto its image), so $X$ is smooth over $k$. In particular $X$ is regular, even geometrically regular.

Example 3.5.25. Let $X = \text{Spec } \mathbb{Z}[x, y]/(xy - 7)$, and let $\pi$ be the unique morphism from $X$ to $\text{Spec } \mathbb{Z}$. The same computation as in the previous example shows that the nonsmooth locus of $\pi$ consists of the single point given by the maximal ideal $(x, y, 7)$ of $\mathbb{Z}[x, y]$; in geometric terms, it is the point $(0, 0)$ on the fiber above the prime $(7)$ of $\mathbb{Z}$. If $U$ is the open subset $\text{Spec } \mathbb{Z}[1/7]$ of $\text{Spec } \mathbb{Z}$, then $\pi^{-1}U \to U$ is smooth.

Again, one can check that $X$ is regular.
3.5.6. Definition 2 of smooth: geometrically regular fibers. For a morphism that is flat and locally of finite presentation, smoothness can be tested fiberwise:

**Proposition 3.5.26.** Let \( f : X \to S \) be a morphism that is locally of finite presentation. Let \( x \in X \) and let \( s = f(x) \). Let \( X_s \) be the fiber \( f^{-1}(s) \). Then \( f \) is smooth of relative dimension \( r \) at \( x \) if and only if \( f \) is flat at \( x \) and \( X_s \) is smooth of relative dimension \( r \) over the residue field \( k(s) \) at \( x \).

**Proof.** See Proposition 8 in [BLR 90, §2.4].

Combining Propositions 3.5.26 and 3.5.22 shows that Definition 3.5.12 is equivalent to the following:

**Definition 3.5.27.** (cf. [EGA IV, §6.8.1]) A morphism of schemes \( f : X \to S \) is smooth if all of the following hold:
- \( f \) is flat,
- \( f \) is locally of finite presentation, and
- for all \( s \in S \), the fiber \( X_s \) over \( k(s) \) is geometrically regular.

For \( x \in X \), the morphism \( f \) is called smooth at \( x \) if there is an open neighborhood \( U \) of \( x \) such that \( f|_U : U \to S \) is smooth.

3.5.7. Unramified morphisms. Let \( A \hookrightarrow B \) be an inclusion of discrete valuation rings, with uniformizers \( \pi_A \) and \( \pi_B \), respectively. In algebraic number theory, the extension \( B \) over \( A \) is called unramified if and only if the maximal ideal \((\pi_B)\) of \( B \) is generated by \( \pi_A \) and the residue field extension \( B/(\pi_B) \) over \( A/(\pi_A) \) is a finite separable extension (or separable algebraic if one is considering infinite extensions).

This definition can be generalized to local rings. Recall that a homomorphism \( f : A \to B \) between local rings with maximal ideals \( m_A \) and \( m_B \) is called local if \( f^{-1}(m_B) = m_A \) [Har 77, p. 73].

**Definition 3.5.28.** A local homomorphism of local rings \( f : A \to B \) with maximal ideals \( m_A \) and \( m_B \) is unramified if \( f(m_A)B = m_B \) and \( B/m_B \) is a finite separable extension of \( A/m_A \).

**Example 3.5.29.** Let \( A = \mathbb{C}[[z]] \) and let \( B = A[\sqrt{z}] = \mathbb{C}[[\sqrt{z}]] \). Let \( f : A \to B \) be the inclusion. Then \( m_A = (z) \), but \( f(m_A)B = (\sqrt{z})^2B \neq (\sqrt{z})B = m_B \), so \( B \) is not unramified over \( A \).

**Remark 3.5.30.** Definition 3.5.28 relates to the ordinary English meaning of “ramified” as “branched”: Example 3.5.29 is related to the fact that there is no single-valued branch of \( \sqrt{z} \) defined in a neighborhood of the origin; the map from the associated Riemann surface down to the complex plane is generically 2-to-1, with “the branches coming together” above \( z = 0 \).
Definition 3.5.31 ([SP Tag 02G4]). Let $f : X \to S$ be a morphism of schemes, and let $x \in X$. Then $f$ is **unramified at $x$** if $f$ is locally of finite type at $x$ and $\mathcal{O}_{S,f(x)} \to \mathcal{O}_{X,x}$ is an unramified homomorphism of local rings. Also, $f$ is called **unramified** if $f$ is unramified at every $x \in X$.

**Warning 3.5.32.** There is a variant in which “locally of finite type” is replaced by “locally of finite presentation”; following [SP Tag 02G4], we reserve the adjective **G-unramified** for this more restrictive variant. In fact, the original definition of unramified in [EGA IV, 17.3.1] is what we are calling G-unramified. The decision to require only locally of finite type was made in [Ray70a Chapitre I, Définition 4].

**Example 3.5.33.** Open and closed immersions are unramified. But not all closed immersions are G-unramified; this is one of the advantages of unramified over G-unramified.

See Definition 1 and Proposition 2 of [BLR90 §2.2] for some equivalent definitions.

**3.5.8. Étale morphisms.**

**Definition 3.5.34.** A morphism $f : X \to S$ is **étale at a point** $x \in X$ if it is flat at $x$ and G-unramified at $x$. Also, $f$ is **étale** if $f$ is étale at every $x \in X$.

Étale morphisms can be thought of as the algebraic analogue of locally biholomorphic maps in differential geometry. In fact, a morphism of $\mathbb{C}$-varieties $X \to Y$ is étale if and only if the induced morphism $X^{\text{an}} \to Y^{\text{an}}$ between complex analytic spaces is locally biholomorphic (that is, each $x \in X^{\text{an}}$ has an open neighborhood that is mapped isomorphically to its image).

Alternatively, étale morphisms can be thought of as generalizations of finite separable extensions of fields, as the following proposition suggests.

**Proposition 3.5.35.** Let $k$ be a field, and let $X$ be a $k$-scheme. The following are equivalent:

(i) $X$ is unramified over $k$.

(ii) $X$ is étale over $k$.

(iii) $X$ is a disjoint union of $k$-schemes of the form $\text{Spec } L$ where each $L$ is a finite separable extension of $k$.

**Proof.**

(i) $\iff$ (ii): Over a field, flatness is automatic, and locally of finite type coincides with locally of finite presentation.

(ii) $\Rightarrow$ (iii): Immediate from the definition of unramified.

(i) $\Rightarrow$ (iii): By definition, $X$ is locally of finite type. The question is local on $X$, so we may assume that $X = \text{Spec } A$ for some finitely generated $k$-algebra $A$. The definition of unramified implies that each local ring $\mathcal{O}_{X,x}$ is a finite separable extension of $k$, so $\dim A = 0$. 69
Hence $A$ is artinian [AM69 8.5], and is a finite product of local artinian rings [AM69 8.7], each of which is a finite separable extension of $k$.

**Corollary 3.5.36.** If $f: X \to S$ is an unramified morphism of schemes, then the relative dimension $\dim_x f$ is $0$ for all $x \in X$.

**Proof.** Let $s = f(x)$. Unramified morphisms are stable under base change, so the fiber $X_s$ is unramified over $\text{Spec} \mathbf{k}(s)$. Then $\dim X_s = 0$ by Proposition 3.5.35. □

The following characterization of étale morphisms is sometimes taken as a definition.

**Proposition 3.5.37.** A morphism $f: X \to S$ is étale at a point $x \in X$ if and only if it is smooth of relative dimension $0$ at $x$.

**Proof.** This follows from [BLR90 §2.4, Proposition 8]. □

The primitive element theorem states that a finite separable extension of a field $k$ is generated by one element. Proposition 3.5.39 is a generalization.

**Definition 3.5.38.** Let $A$ be a commutative ring. Let $p \in A[t]$ be a monic polynomial. Let $B = A[t]/(p)$. Let $C = B[q^{-1}]$ for some $q \in B$. If the image of $p'(t)$ in $C$ is in $C^\times$, then $\text{Spec} C \to \text{Spec} A$ is called a standard étale morphism.

Geometrically, the condition $p'(t) \in C^\times$ says that the fiber above each point of $\text{Spec} A$ looks like the set of zeros of a separable polynomial. See Figure 4 (in which we view $q$ as an element of $A[t]$ instead of its image in $A[t]/(p)$).
Proposition 3.5.39 (Local structure of an étale morphism). Let \( f : X \to S \) be a morphism of schemes, let \( x \in X \), and let \( s = f(x) \in S \). Then \( f \) is étale at \( x \) if and only if there exist affine open neighborhoods \( X' \subseteq X \) of \( x \) and \( S' \subseteq S \) of \( s \) such that \( f|_{X'} : X' \to S' \) is a standard étale morphism.

Proof. The proof relies on Zariski’s main theorem: see [Ray70a, V.§1, Théorème 1] and [BLR90, §2.3, Proposition 3]. □

3.5.9. Fundamental groups.

(Reference: [Sza09])

3.5.9.1. Fundamental groups in topology. Let \( X \) be a topological space that is reasonably nice (e.g., path connected, locally path connected, and locally simply connected). A cover of \( X \) is a map of topological spaces \( Y \xrightarrow{p} X \) such that \( X \) can be covered by open subsets \( U \) such that \( p^{-1}U \to U \) is isomorphic to a disjoint union of copies of \( U \) each mapping by the identity to \( U \). A morphism of covers is a map of topological spaces over \( X \). The covers of \( X \) form a category \( \text{Covers}_X \). For \( x \in X \), the fiber functor \( F_x : \text{Covers}_X \to \text{Sets} \) is the functor sending a cover \( Y \xrightarrow{p} X \) to the fiber \( p^{-1}(x) \).

Theorem 3.5.40. The following groups are naturally isomorphic:

(i) The group of homotopy classes of loops in \( X \) based at \( x \).
(ii) The group of deck transformations of the universal cover \( \tilde{X} \to X \).
(iii) The automorphism group of the fiber functor \( F_x \).

The fundamental group \( \pi_1(X,x) \) of the pointed topological space \( (X,x) \) is any of the three groups in Theorem 3.5.40. Then \( F_x \) can be upgraded to a functor \( F'_x : \text{Covers}_X \to \{\pi_1(X,x)\text{-sets}\} \), which turns out to be an equivalence of categories.

The space \( X \) is called simply connected if the only connected cover of \( X \) is given by the identity map \( X \to X \). For any \( x \in X \), this condition is equivalent to \( \pi_1(X,x) = \{1\} \).

There is a variant of \( \pi_1(X,x) \) in which \( \text{Covers}_X \) is replaced by the category \( \text{FCovers}_X \) of covers with finite fibers. The universal cover may not exist in \( \text{FCovers}_X \) (consider \( X = \mathbb{C}^* \); for each \( n \geq 1 \) the \( n \)th power map \( \mathbb{C}^* \xrightarrow{p} \mathbb{C}^* \) defines a cover, and no finite cover can dominate them all). So the variant of the fundamental group should be defined either as the inverse limit of the deck transformation groups of the finite Galois covers of \( X \), or as the automorphism group of the restriction \( F_x|_{\text{FCovers}_X} \). Both approaches lead to the same group \( \hat{\pi}_1(X,x) \). This group \( \hat{\pi}_1(X,x) \) is isomorphic to the profinite completion of \( \pi_1(X,x) \), i.e., the inverse limit of all finite quotients of \( \pi_1(X,x) \).

3.5.9.2. The étale fundamental group. Which of the three definitions in Theorem 3.5.40 works best in the algebraic setting? Not (i): loops are not a good notion in a space with the Zariski topology. For (ii) or (iii), we need an algebraic analogue of covers. Ideally, the
analogue should be such that algebraic covers of a $\mathbb{C}$-variety $X$ roughly correspond to covers of the topological space $X(\mathbb{C})$.

A first attempt might be to apply the topological definition of cover directly to $X$ with the Zariski topology. But there are often not enough Zariski locally trivial covers. For example, the complex manifold $\mathbb{C}^\times$ has universal cover $\mathbb{C} \xrightarrow{\exp} \mathbb{C}^\times$ and fundamental group $\mathbb{Z}$, but the corresponding algebraic variety $\mathbb{A}_\mathbb{C}^1 \setminus \{0\}$ has no connected Zariski locally trivial cover.

Étale morphisms come to the rescue. Actually, étale morphisms are not quite restrictive enough, since they include open immersions like $\mathbb{A}_\mathbb{C}^1 \setminus \{0\} \hookrightarrow \mathbb{A}_\mathbb{C}^1$ that do not induce a cover of topological spaces. Instead we use finite étale morphisms. (The morphism $\mathbb{A}_\mathbb{C}^1 \setminus \{0\} \hookrightarrow \mathbb{A}_\mathbb{C}^1$ has finite fibers, but is not finite, since $k[x, x^{-1}]$ is not a finite $k[x]$-module.)

To explain why a finite étale morphism is the algebraic analogue of a topological cover with finite fibers, we state the generalized Riemann existence theorem. Let $X$ be a $\mathbb{C}$-variety. Let $\mathbb{C}^\text{an}$ be the associated complex analytic space; its underlying topological space is $X(\mathbb{C})$. Let $\mathbf{FEt}_X$ be the category of finite étale covers of $X$. There is a corresponding notion of finite étale covers of $\mathbb{C}^\text{an}$, and we let $\mathbf{FEt}^{\text{an}}_X$ be the corresponding category.

**Theorem 3.5.41** (Generalized Riemann existence theorem [SGA 1 Théorème XII.5.1]). Let $X$ be a $\mathbb{C}$-variety. Then the natural functors $\mathbf{FEt}_X \to \mathbf{FEt}^{\text{an}}_X \to \text{FCovers}_{X(\mathbb{C})}$ are equivalences of categories.

**Remark 3.5.42.** Unfortunately, infinite topological covers such as $\mathbb{C} \xrightarrow{\exp} \mathbb{C}^\times$ have no algebraic analogue, and can only be approximated by their finite subcovers.

Now we are prepared to define the algebraic analogue of the fundamental group. Let $X$ be any scheme. Let $x$ be a geometric point of $X$, i.e., a morphism $x : \text{Spec } \Omega \to X$ for some separably closed field $\Omega$. Pulling back a finite étale morphism $Y \xrightarrow{p} X$ by $x : \text{Spec } \Omega \to X$ yields a finite disjoint union of copies of $\text{Spec } \Omega$ (Proposition 3.5.35), and forgetting the scheme structure yields a set $p^{-1}(x)$. The fiber functor $F_x : \mathbf{FEt}_X \to \text{Sets}$ sends an object $Y \xrightarrow{p} X$ to $p^{-1}(x)$.

**Definition 3.5.43.** The étale fundamental group $\pi_1^{\text{et}}(X, x)$ is the group $\text{Aut} F_x$. (Alternative terminology/notation: algebraic fundamental group, $\pi_1^{\text{alg}}(X, x)$, $\hat{\pi}_1(X, x)$.)

For a connected scheme $X$ with a geometric point $x$, as $(Y, y)$ varies over pointed connected (finite) Galois étale covers of $(X, x)$, the Galois groups $\text{Gal}(Y/X)$ form an inverse system whose inverse limit is $\pi_1^{\text{et}}(X, x)$, so $\pi_1^{\text{et}}(X, x)$ is a profinite group.

**Example 3.5.44.** If $X$ is a $\mathbb{C}$-variety and $x \in X(\mathbb{C})$, then the generalized Riemann existence theorem (Theorem 3.5.41) shows that $\pi_1^{\text{et}}(X, x)$ is the profinite completion of $\pi_1(X(\mathbb{C}), x)$.
Definition 3.5.45. Let $X$ be a connected variety over a separably closed field. Then $X$ is **algebraically simply connected** if it has no nontrivial connected finite étale cover. For any geometric point $x: \text{Spec }\Omega \to X$, this is equivalent to the condition that $\pi_1^e(X, x) = \{1\}$.

Warning 3.5.46. There exists an algebraically simply connected $\mathbb{C}$-variety $X$ such that the topological space $X(\mathbb{C})$ is not simply connected. That is, there exists a connected $\mathbb{C}$-variety such that $\pi_1(X, x)$ is nontrivial but has trivial profinite completion. To see this, combine Example 3.5.44 with the following two facts:

1. There exists an infinite finitely presented group $G$ with no nontrivial finite quotients [Hig51].
2. For any finitely presented group $G$, there exist an integral $\mathbb{C}$-variety $X$ and $x \in X(\mathbb{C})$ such that $\pi_1(X(\mathbb{C}), x) \simeq G$ [Sim11, Theorem 12.1].

3.5.10. Local coordinates. The following proposition should be compared with the discussion in Remark 3.5.11.

Proposition 3.5.47. Let $f: X \to S$ be smooth of relative dimension $r$ at a point $x \in X$, and let $s = f(x)$. Then the following are equivalent for elements $g_1, \ldots, g_r \in \mathcal{O}_{X,x}$:

(i) The differentials $dg_1(x), \ldots, dg_r(x)$ form a basis for the ($r$-dimensional) cotangent space $\Omega_{X/S,x} \otimes k(x)$.

(ii) There is an open neighborhood $U$ of $x$ in $X$ to which the $g_i$ extend, such that the $S$-morphism $(g_1, \ldots, g_r): U \to \mathbb{A}_S^r$ is étale.

Moreover, such $g_1, \ldots, g_r$ exist.

Proof. See Proposition 11 and Remark 12 in [BLR90, §2.2]. 

Definition 3.5.48. An $r$-tuple $(g_1, \ldots, g_r)$ satisfying the equivalent conditions of Proposition 3.5.47 is called a **system of local coordinates at** $x$.

Remark 3.5.49. Suppose that in the setting of Proposition 3.5.47, we have $S = \text{Spec }k$ and $x \in X(k)$. Then we have an isomorphism of $r$-dimensional $k$-vector spaces

\[
\frac{m_x}{m_x^2} \to \Omega_{X/k,x} \otimes k(x) \\
\quad g \mapsto dg(x).
\]

Thus for $g_1, \ldots, g_r$ vanishing at $x$, we have that $g_1, \ldots, g_r$ are local coordinates at $x$ if and only if their images in $m_x/m_x^2$ form a basis.

Local coordinates can be used to reduce questions about smooth schemes to the case of étale schemes. For example:

Proposition 3.5.50. Suppose that $X \to S$ is a smooth morphism of schemes.
(i) If $S$ is reduced, then $X$ is reduced.
(ii) If $S$ is normal, then $X$ is normal.
(iii) If $S$ is regular, then $X$ is regular.

Sketch of proof. Each statement is local on $X$. Proposition 3.5.47 says that locally $X \to S$ factors into an étale morphism and a morphism of the type $\mathbb{A}^n_S \to S$. Thus we reduce to proving the statements for étale morphisms of the type described in Proposition 3.5.39 and for morphisms of the type $\text{Spec } A[t] \to \text{Spec } A$. For these, it is a calculation: see [Ray70a, VII.§2] for some more details. □

3.5.11. Example: étale schemes over a normal scheme.

(Reference: [SGA 1, I.10])

We now classify étale schemes $Y$ over a normal locally noetherian scheme $X$. By Proposition 3.5.50(ii), any such $Y$ is normal and locally noetherian too. We may assume that $X$ and $Y$ are connected, and hence integral by Lemma 3.2.11(i) ⇒ (iii). For simplicity, we also restrict to the case where $Y \to X$ is separated; otherwise we could get more étale $X$-schemes by doubling some closed points of $Y$, for example.

Theorem 3.5.51. Let $X$ be a normal connected locally noetherian scheme. Let $K = k(X)$.

(a) Let $K'$ be a finite separable extension of $K$. Let $X'$ be the normalization of $X$ in $K'$. Then $X' \to X$ is finite.

(b) Let $X' \to X$ be as in (a). Let $U' \subseteq X'$ be a nonempty open subscheme. If $U'$ is unramified over $X$, then $U'$ is a separated connected étale $X$-scheme ("separated" here means "separated over $X".)

(c) Every separated connected étale $X$-scheme $Y$ arises as in (b).

(d) An étale $X$-scheme $U'$ as in (b) is finite over $X$ if and only if $U' = X'$.

Proof. 

(a) The question is local on $X$, so assume that $X$ is affine. Now this is [Ser79, I.§4, Proposition 8].

(b) For the proof that $U' \to X$ is étale, see [SGA 1, I.9.11]. The composition $U' \to X' \to X$ of an open immersion and finite morphism is separated. Since $U'$ is a nonempty open subscheme of the integral scheme $X'$, it is connected.

(c) An étale morphism is locally quasi-finite, so this follows from Zariski’s main theorem: see [EGA IV 3, 8.12.11].
(d) If $U' = X'$, then $U'$ is finite over $X$ by (a). Conversely, if $U'$ is finite over $X$, then $U'$ is finite over $X'$, and hence proper over $X'$, so the open subscheme $U'$ is closed in $X'$. Since $X'$ is connected, $U' = X'$.

**Definition 3.5.52.** In the context of Theorem 3.5.51(a), call $K' \supseteq K$ unramified above $X$ if the normalization $X' \to X$ is unramified.

**Corollary 3.5.53 (Fundamental group of a normal scheme).** Let $X$ be a normal connected locally noetherian scheme. Let $K = k(X)$. Let $\Omega$ be a separably closed field containing $K$. Let $\eta \colon \text{Spec} \Omega \to X$ be the associated geometric point. Let $L$ be the compositum of all finite separable extensions of $K$ in $\Omega$ that are unramified above $X$. Then $\pi_1^{\text{et}}(X, \eta) \simeq \text{Gal}(L/K)$.

**Proof.** By Theorem 3.5.51(c,d), the finite étale $X$-schemes are the normalizations of $X$ in finite separable extensions $K'$ of $K$, so $\pi_1^{\text{et}}(X, \eta)$ is the inverse limit of the groups $\text{Gal}(K'/K)$ for the finite Galois extensions of this type.

**Example 3.5.54.** Let $k$ be a field. A choice of separable closure gives a a geometric point $\eta \colon \text{Spec} k_s \to \text{Spec} k$, and $\pi_1^{\text{et}}(\text{Spec} k, \eta) \simeq \text{Gal}(k_s/k)$.

**Example 3.5.55.** Let $O_{K,S}$ be a ring of $S$-integers in a global field $K$ (Definition 1.1.1). Fix a geometric point $\eta \colon \text{Spec} K_s \to \text{Spec} O_{K,S}$. In this case, the field $L \subseteq K_s$ of Corollary 3.5.53 is classically called the maximal Galois extension of $K$ unramified outside $S$. Then $\pi_1^{\text{et}}(\text{Spec} O_{K,S}, \eta) \simeq \text{Gal}(L/K)$.

The following will be used in Section 8.4.6:

**Lemma 3.5.56 (cf. Har00 proof of Lemma 5.2(1)).** For a normal geometrically integral $k$-variety $X$ with a $k$-point $x$, the following are equivalent:

(i) $X_{k_s}$ is not algebraically simply connected; i.e., $\pi_1^{\text{et}}(X_{k_s}, x) \neq \{1\}$.

(ii) $X_{k_s}$ has a nontrivial connected finite étale cover.

(iii) $X_{k_s}$ has a nontrivial geometrically integral finite étale cover.

(iv) $X$ has a nontrivial geometrically integral finite étale cover.

**Proof.** For each finite separable extension $L \supseteq k$, the variety $X_L$ is normal by Proposition 3.5.50(ii), so $X_{k_s}$ is normal too.

(iv) $\Rightarrow$ (iii): If $Y \to X$ is a nontrivial geometrically integral finite étale cover, then so is $Y_{k_s} \to X_{k_s}$.

(iii) $\Rightarrow$ (ii): Geometrically integral implies connected.

(i) $\iff$ (ii): This is the definition of algebraically simply connected.

(iii) $\Rightarrow$ (iii): We show that every connected finite étale cover $Y \to X_{k_s}$ is geometrically integral. First, $Y$ is integral by the arguments preceding Theorem 3.5.51, so $Y$ is geometrically
irreducible by Proposition 3.5.50.[iii]⇒[iv]. On the other hand, \( \mathcal{Y}_k \) is étale over the reduced variety \( X_k \), so \( \mathcal{Y}_k \) is reduced by Proposition 3.5.50.[iii]. Thus \( \mathcal{Y} \) is geometrically integral.

\( \text{[iii]} \Rightarrow \text{[iv]}: \) By Theorem 3.5.51.[c, d], nontrivial connected finite étale covers of \( X \) are the normalizations of \( X \) in the finite separable extensions of \( k(X) \) unramified above \( X \), and likewise for \( X_k \). Let \( \mathcal{Y} \to X_k \) be a nontrivial geometrically integral finite étale cover. By replacing \( k(\mathcal{Y}) \) by its Galois closure over \( k(X) \), and \( \mathcal{Y} \) by the corresponding normalization of \( X \), we may assume that \( k(\mathcal{Y}) \) is Galois over \( k(X) \); by the proof of \( \text{[iii]} \Rightarrow \text{[iii]} \), \( \mathcal{Y} \) is still geometrically integral.

We claim that \( \mathcal{Y} \to X_k \) is the base change of a geometrically integral finite étale cover \( Y \to X \). To construct \( Y \to X \), we will construct \( k(\mathcal{Y}) \) and then take the normalization of \( X \) in \( k(\mathcal{Y}) \). First, the tower of fields \( k(\mathcal{Y}) \supseteq k(X_k) \subseteq k(X) \) yields an exact sequence

\[
1 \to \text{Gal}(k(\mathcal{Y})/k(X_k)) \to \text{Gal}(k(\mathcal{Y})/k(X)) \to \text{Gal}(k(X_k)/k(X)) \to 1. \tag{3.5.57}
\]

Define the fiber \( \mathcal{Y}_x \) as the set of points in \( \mathcal{Y}(k_x) \) above \( x \). The group \( \text{Gal}(k(\mathcal{Y})/k(X)) \) acts on \( \mathcal{Y}_x \), and its subgroup \( \text{Gal}(k(\mathcal{Y})/k(X_k)) \) acts simply transitively since \( \mathcal{Y} \to X_k \) is Galois étale. Therefore a choice of \( y \in \mathcal{Y}_x \) splits \( \text{[3.5.57]} \): the stabilizer \( S := \text{Stab}_{\text{Gal}(k(\mathcal{Y})/k(X))}(y) \) maps isomorphically to \( \text{Gal}(k(X_k)/k(X)) \). Thus the extension \( k(\mathcal{Y}) \supseteq k(X_k) \) arises from \( k(\mathcal{Y})^S \supseteq k(X_k)^S = k(X) \) by base change, i.e., by applying \( \otimes_{k(\mathcal{Y})} k(X_k) \) or equivalently \( \otimes_{k(x)} k \).

Taking normalizations of \( X \) in these fields shows that \( \mathcal{Y} \to X_k \) is the base change of some \( Y \to X \). Since \( \mathcal{Y} \to X_k \) is finite étale and nontrivial, so is \( Y \to X \). Since \( \mathcal{Y} \) is geometrically integral, so is \( Y \).

\[ \square \]

**3.5.12. Definition 3 of smooth: the infinitesimal lifting property.** Here is yet another definition of smooth. Its equivalence with Definition 3.5.12 is proved in Proposition 6 in [BLR90, §2.2]. Alternatively, see [EGA IV, §17.5.2].

**Definition 3.5.58.** [EGA IV, §17.1.1, 17.3.1]. A morphism \( f: X \to S \) is smooth if and only if both of the following hold:

(i) \( f \) is locally of finite presentation, and

(ii) for every affine scheme \( \text{Spec} \ A \) equipped with a morphism to \( S \), and for every nilpotent ideal \( I \subset A \), the natural map \( X(A) \to X(A/I) \) is surjective.

(Here we think of \( X \), \( \text{Spec} \ A \), and \( \text{Spec} \ A/I \) as \( S \)-schemes, so for instance, \( X(A/I) \) should be interpreted as \( \text{Hom}_S(\text{Spec} \ A/I, X) \). To say that \( I \) is nilpotent means that \( I^n = 0 \) for some \( n \)).

**Remark 3.5.59.** Property (ii) is called the **infinitesimal lifting property**, and a morphism satisfying it alone is called formally smooth. One gets an equivalent condition if one allows only ideals \( I \) for which \( I^2 = 0 \).

**Example 3.5.60.** Let \( k \) be a field, and let \( X \) be the \( k \)-variety \( xy = 0 \) in \( \mathbb{A}^2_k \). We will show that \( X \) does not satisfy property (ii), and hence is not smooth. Take \( A = k[\epsilon]/(\epsilon^3) \)
and $I = (e^2) \subseteq A$, so $A/I = k[e]/(e^2)$. Then the point $(e, e) \in A^2(A/I)$ lies on $X(A/I)$, but there is no way to lift this to a point in $X(A)$: such a lift would have to be of the form $(e + ae^2, e + be^2)$ for some $a, b \in k$, but $(e + ae^2)(e + be^2) = e^2 \neq 0$ in $A$.

This example can be interpreted geometrically. Let $A_2 := k[e]/(e^2)$. Giving an element of $X(A_2)$, i.e., a morphism $\text{Spec } A_2 \rightarrow X$, is the same as giving a point $P \in X(k)$ with a tangent vector at $P$. More generally, for any $n$, morphisms $\text{Spec } A_n \rightarrow X$ are called jets. Let $P$ be the origin $(0, 0) \in X(k)$; then the tangent space $T_{X,P} = T_{A^2,P}$ is 2-dimensional. The element $(e, e) \in X(A_2)$ corresponds to a tangent vector at $P$ pointing along the line $y = x$: see Figure 5. Such a tangent vector, lying along neither of the two branches of $X$ at $P$, will not extend to a higher order jet in $X$.

**Remark 3.5.61.** If one replaces “surjective” in Theorem 3.5.58 by “injective” or “bijective”, one gets equivalent definitions for the concepts of G-unramified or étale morphisms, respectively [EGA IV 4, §17.1.1, 17.3.1].

**Theorem 3.5.62 (Hensel’s lemma).**

Let $A$ be a complete noetherian local ring with maximal ideal $m$.

(a) If $X$ is smooth over $\text{Spec } A$, then the reduction map $X(A) \rightarrow X(A/m)$ is surjective.

(b) If $X$ is étale over $\text{Spec } A$, then the reduction map $X(A) \rightarrow X(A/m)$ is bijective.

To see what Theorem 3.5.62 has to do with the Hensel’s lemma in algebraic number theory, see what it says when $A = \mathbb{Z}_p$ and $X = \text{Spec } \mathbb{Z}_p[t]/(f)$ where $f \in \mathbb{Z}_p[t]$ is a monic polynomial such that $f$ modulo $p$ is a separable polynomial in $\mathbb{F}_p[t]$.

**Proof of Theorem 3.5.62.** If $X$ is smooth (resp. étale) over $\text{Spec } A$, then by the infinitesimal lifting property, $X(A/m^{n+1}) \rightarrow X(A/m^n)$ is surjective (resp. bijective) for each $n \geq 1$. The theorem will follow if we can verify the technical point $X(A) = \varprojlim X(A/m^n)$. (The reader is invited to skip the rest of this proof.)
For any local ring $A$ and scheme $X$, there is a bijection

$$\{\text{morphisms } \text{Spec } A \to X\} = \{(x, \phi) \mid x \in X \text{ and } \phi: \mathcal{O}_{X,x} \to A \text{ is a local homomorphism}\},$$

in which $x$ represents the image of the closed point of $\text{Spec } A$ in $X$ [EGA I 2.4.4]. Thus for our $A$-scheme $X$,

$$X(A) = \{(x, \phi) \mid x \in X \text{ and } \phi: \mathcal{O}_{X,x} \to A \text{ is a local } A\text{-algebra homomorphism}\},$$

and

$$X(A/m^n) = \{(x, \phi) \mid x \in X \text{ and } \phi: \mathcal{O}_{X,x} \to A/m^n \text{ is a local } A\text{-algebra homomorphism}\}$$

for any $n \geq 1$. This, together with the fact that $A$ is the projective limit of $A/m^n$ in the category of rings, implies that the natural map $X(A) \to \varprojlim X(A/m^n)$ is bijective. □

3.5.13. Smooth varieties over a field.

**Proposition 3.5.63.** The smooth locus of a geometrically reduced $k$-variety $X$ is open and dense in $X$.

**Proof.** Openness was proved in Proposition 3.5.17. For the denseness, see Proposition 16 in §2.2 of [BLR90]. □

**Example 3.5.64.** Here we show that the “geometrically reduced” hypothesis in Proposition 3.5.63 cannot be dropped. Let $k$ be the imperfect field $\mathbb{F}_p(t)$. Let $X$ be the curve $x^p - ty^p = 0$ in $\mathbb{A}^2_k$. The Jacobian matrix is identically zero, so $X^{\text{smooth}} = \emptyset$.

**Proposition 3.5.65.** Let $k$ be a field, and let $X$ be a $k$-variety. Suppose that $X$ is smooth at the point $x \in X(k)$, and let $t_1, \ldots, t_r$ be local coordinates at $x$. Replace $t_i$ by $t_i - t_i(x)$ to make each new $t_i$ vanish at $x$. Then the natural map $k[[t_1, \ldots, t_r]] \to \widehat{\mathcal{O}}_{X,x}$ from the formal power series ring to the completion of the local ring of $X$ at $x$ is an isomorphism.

**Proof.** The local ring $\mathcal{O}_{X,x}$ is a regular local ring of dimension $r$ containing its residue field $k$. Therefore its completion $\widehat{\mathcal{O}}_{X,x}$ is too, and the Cohen structure theorem implies $\widehat{\mathcal{O}}_{X,x} \simeq k[[t_1, \ldots, t_r]]$ (see Mat80 Corollary 2 to 28.J.). □

**Proposition 3.5.66.** If a $k$-variety is smooth and geometrically connected, then it is geometrically integral.

**Proof.** Let $X$ be the variety. By Proposition 3.5.22, smooth is equivalent to geometrically regular, so Corollary 3.5.6 applies to $X_{\overline{k}}$. □

For convenience, we make the following definition:

**Definition 3.5.67.** A $k$-variety is **nice** if it is smooth, projective, and geometrically integral.
Remark 3.5.68. The literature contains many theorems about varieties that are “smooth, projective, and geometrically connected”. These hypotheses look weaker than “nice”, but in fact they are equivalent, by Proposition 3.5.66.

3.5.13.1. Separably closed fields.

Proposition 3.5.69. If $X$ is a smooth $k$-variety over a separably closed field $k$, then $X(k)$ is Zariski dense in $X$.

Proof. The question is local on $X$, so by Proposition 3.5.47, we may assume that there is an étale morphism $g : X \to \mathbb{A}^r_k$. We may also assume that $X$ is nonempty. It suffices to prove $X(k) \neq \emptyset$, since then we can apply the same argument to each dense open subscheme of $X$.

By Proposition 3.4.2 $g(\mathbb{X})$ is open in $\mathbb{A}^r_k$. Since separably closed fields are infinite, $\mathbb{A}^r(k)$ is dense in $\mathbb{A}^r_k$. In particular, there is a $k$-point $v$ in $g(X)$. The nonempty étale $k$-scheme $g^{-1}(v)$ is a disjoint union of $k$-points by Proposition 3.5.35. Thus $X$ has a $k$-point. □

The hypothesis of Proposition 3.5.69 can be weakened slightly:

Corollary 3.5.70. If $X$ is a geometrically reduced $k$-variety over a separably closed field $k$, then $X(k)$ is Zariski dense in $X$.

Proof. Combine Propositions 3.5.63 and 3.5.69. □

Example 3.5.71. Here we show that the “geometrically reduced” hypothesis in Corollary 3.5.70 cannot be dropped. Let $k$ be an imperfect separably closed field. Choose $t \in k - k^p$. Let $X$ be the curve $x^p - ty^p = 0$ in $\mathbb{A}^2_k$. Then $X(k)$ consists of the single point $(0, 0)$, and hence $X(k)$ is not Zariski dense in $X$.

3.5.13.2. Local fields.

Proposition 3.5.72. Let $k$ be a local field. Let $f : Y \to X$ be a morphism between $k$-varieties.

(i) If $f$ is étale, then the induced map of topological spaces $Y(k) \to X(k)$ is a local homeomorphism (for the analytic topology).

(ii) If $f$ is smooth, then the map $Y(k) \to X(k)$ is open.

Proof.

(i) By Proposition 3.5.39 we may assume that $f : Y \to X$ is a standard étale morphism Spec$(A[t]/(p))[q^{-1}] \to \text{Spec } A$ as in Definition 3.5.38 where $A$ is a quotient of a polynomial ring $R := k[x_1, \ldots, x_n]$. Lift $p \in A[t]$ to some $\tilde{p} \in R[t]$. Then there is an affine open subset of Spec$R[t]/(\tilde{p})$ whose projection to Spec$R = \mathbb{A}^n$ is a standard étale morphism whose restriction above Spec$A$ is $f$. So we reduce to the case of a standard
étale morphism \( Y \to X = \mathbb{A}^n \). The result now is a special case of the implicit function theorem over \( k \).

(ii) Proposition [3.5.47] lets us reduce to proving openness for étale morphisms and projections \( X \times \mathbb{A}^n \to X \). The étale case follows from [3.5.72], and the projection case follows from the definition of the product topology. \( \square \)

The classical Krasner’s lemma [Lan94, II, §2, Proposition 3] is a statement about local fields \( k \) that implies that if the coefficients of a monic separable polynomial are perturbed, then the multiset of zeros varies continuously, irreducibility is locally preserved, and the field extension generated by the zeros is locally constant [Lan94, II, §2, Proposition 4]. Since any monic separable polynomial in \( \mathbb{Q}_p[x] \) can be approximated by monic polynomials in \( \mathbb{Q}[x] \), this implies that any degree \( d \) extension of \( \mathbb{Q}_p \) is \( \mathbb{Q}_p(\alpha) \) for some \( \alpha \) that is algebraic of degree \( d \) over \( \mathbb{Q} \). In particular, the copy of \( \overline{\mathbb{Q}} \) in \( \overline{\mathbb{Q}}_p \) is dense, and the homomorphism \( \text{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p) \to \text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \) sending \( \sigma \) to \( \sigma|_{\overline{\mathbb{Q}}} \) is injective (its image is a decomposition group).

The following is a generalization of the statement above that the field extension generated by the zeros is locally constant.

PROPOSITION 3.5.73 (Krasner’s lemma). Let \( k \) be a local field. Let \( f: Y \to X \) be a finite étale morphism of \( k \)-varieties. Then the isomorphism type of the étale \( k \)-scheme \( f^{-1}(x) \) is locally constant as \( x \) varies over \( X(k) \) in the analytic topology.

PROOF. We may assume that \( X \) is connected, so that \( f \) has constant degree, say \( d \). Let \( x_0 \in X(k) \). Let \( L \supseteq k \) be a finite Galois extension over which \( f^{-1}(x_0) \) splits, say into points \( y_1, \ldots, y_d \in Y(L) \). Let \( f_L: Y(L) \to X(L) \) be the map on \( L \)-points. By Proposition [3.5.72], there exist open neighborhoods \( Y_i \subseteq Y(L) \) of \( y_i \) and \( U_i \subseteq X(L) \) of \( x_0 \) such that \( f_L \) restricts to a homeomorphism \( Y_i \to U_i \). We may assume that \( \sigma Y_i = Y_j \) whenever \( \sigma \in \text{Gal}(L/k) \) and \( \sigma y_i = y_j \). By shrinking the \( U_i \) (and correspondingly the \( Y_i \)), we may assume that the \( Y_i \) are disjoint, and that the \( U_i \) are all equal, say to \( U \). The disjoint union of the homeomorphisms \( f_L|_{Y_i}: Y_i \to U \simeq U \times \{y_i\} \) is a \( \text{Gal}(L/k) \)-equivariant homeomorphism \( h: \bigcup Y_i \to U \times f^{-1}_L(x_0) \) of degree \( d \) covers of \( U \). Thus if \( u \in U \cap X(k) \), then restricting the domain and codomain of \( h \) to the fibers above \( u \) yields an isomorphism of \( \text{Gal}(L/k) \)-sets, so the corresponding étale \( k \)-schemes are isomorphic too; these are \( f^{-1}(u) \) and \( f^{-1}(x_0) \) since both have degree \( d \). \( \square \)

PROPOSITION 3.5.74. Let \( k \) be a local field. Let \( X \) be an irreducible \( k \)-variety. If \( X \) has a smooth \( k \)-point \( x \), then \( X(k) \) is Zariski dense in \( X \).

PROOF. By Proposition [3.5.47], we may replace \( X \) by an open subscheme to assume that there is an étale morphism \( \pi: X \to \mathbb{A}_k^n \). By Proposition [3.5.72], the image \( \pi(X(k)) \) is a nonempty open subset of \( \mathbb{A}^n(k) \). No nonzero polynomial can vanish on such an open subset, so \( \pi(X(k)) \) is Zariski dense in \( \mathbb{A}_k^n \). So if \( Y \) is the Zariski closure of \( X(k) \) in \( X \), then \( \dim \pi(Y) = r \). This implies \( \dim Y \geq r \), so \( Y = X \). \( \square \)
Remark 3.5.75. One can strengthen the conclusion of Proposition 3.5.74 to assert that any open neighborhood $U$ of $x$ in $X(k)$ contains $k$-points outside any given countable union of closed subvarieties $Y_i \subseteq X$. To prove this, after reducing to the case $X = \mathbb{A}^r$ as before, one can proceed in any of the following ways:

- apply the Baire category theorem to the nowhere dense subsets $Y_i(k)$ of $X(k)$;
- equip $\mathbb{A}^r(k)$ with Haar measure and observe that $U$ has positive measure while each set $Y_i(k)$ has measure 0;
- or use induction on $r$, by fibering $\mathbb{A}^r(k)$ into lines and using the uncountability of any nonempty open subset of each line $\mathbb{A}^1(k)$.

This strengthening will be used in the proof of Theorem 7.7.4.


Definition 3.5.76. Let $R$ be a discrete valuation ring, and let $K = \text{Frac} R$. Let $X$ be a smooth proper $K$-variety. We say that $X$ has good reduction if there exists a smooth proper $R$-model of $X$. In this case, the special fiber is a smooth proper variety over the residue field.

Example 3.5.77. The $K$-variety in Example 3.2.9 has good reduction, because the scheme $\text{Proj} \mathbb{Z}_7[x,y,z]/(xy - z^2)$ is a smooth proper $R$-model.

Warning 3.5.78. Let $X$ be a smooth proper $K$-variety. Let $\hat{R}$ and $\hat{K}$ denote the completions of $R$ and $K$, respectively. If $X_R$ is a smooth proper $R$-model of $K$, then $X_R \times_R \hat{R}$ is a smooth proper $\hat{R}$-model for $X_{\hat{K}}$. So if $X$ has good reduction, then so does $X_{\hat{K}}$. But the converse can fail, as we now explain by modifying Example 5.3] Mat15. Let $p, a, b, c, F$ be as in Example 5.3], except with $c$ a nonsquare integer that becomes a square in $\mathbb{Z}_p$. Let $R = \mathbb{Z}_p$. Let $X = \text{Proj} \mathbb{Z}_p[x, y, z, w]/(F)$. Then

(i) the generic fiber is a smooth quartic surface $X \subseteq \mathbb{P}^3_\mathbb{Q}$ (a K3 surface) with $\text{Pic} X \simeq \mathbb{Z}$;
(ii) the special fiber is a singular quartic surface over $\mathbb{F}_p$ whose singularities are ordinary double points; and
(iii) there are non-Cartier Weil divisors $C_+$ and $C_-$ on $X_{\mathbb{Z}_p}$ (defined, in fact, on $X_{\mathbb{Z}_p} \sqrt{c}$) such that blowing up either results in a smooth proper scheme over $\mathbb{Z}_p$.

Facts [i] and [ii] imply that $X$ does not extend to a smooth proper scheme over $\mathbb{Z}_p$, by the argument in Art74, p. 330. Fact [iii] says that $X_{\mathbb{Q}_p}$ does extend to a smooth proper scheme over $\mathbb{Z}_p$.

Remark 3.5.79. In the context of Definition 3.5.76, it can happen that $X$ does not extend to a smooth proper $R$-scheme, but does extend to a smooth proper $R$-algebraic space Art74.
In fact, the notion of good reduction would have better properties if it were defined in terms of algebraic spaces: see \cite{Mat15} for more examples of this.

3.5.14.2. Dedekind domains.

**Definition 3.5.80.** Let $R$ be a Dedekind domain, and let $K = \text{Frac} R$. Let $p$ be a nonzero prime of $R$. A smooth proper $K$-variety $X$ has **good reduction at $p$** if $X$ has a smooth proper $R_p$-model. And $X$ has **good reduction** if it has good reduction at every $p$.

3.5.15. Regular proper models. When a smooth proper model does not exist, one can seek models with weaker properties.

For example, if $R$ is a complete discrete valuation ring, and $X$ is a nice $K$-curve, then $X$ always has a regular proper $R$-model. Let us sketch a construction. Choose an embedding of $X$ in $\mathbb{P}^n_K$ for some $n$. We have $\mathbb{P}^n_K \hookrightarrow \mathbb{P}^n_R$, and the Zariski closure of $X$ in $\mathbb{P}^n_R$ is a proper $R$-model $X'_R$ of $X$. But $X'_R$ need not be smooth. The normalization of $X'_R$ is finite over $X_R$, so it is another proper $R$-model $X''_R$, but now it is regular except at isolated closed points. By “resolution of singularities for arithmetic surfaces”, alternately blowing up singularities and normalizing eventually produces a regular proper model. (In fact, it is even projective.) See \cite{Art86b} for an exposition of Lipman’s proof of an even more general version.

If moreover $X$ has genus $\geq 1$, then among all regular proper $R$-models, there is a unique one satisfying a certain minimality property: see Section 9.3.1.6. It is called the **minimal regular proper model**. This result is analogous to the theory of minimal models for surfaces over fields, which is discussed in \cite{Har77}, pp. 418–419.

It is conjectured that a nice $K$-variety $X$ of any dimension has a regular proper $R$-model. This conjecture is a version of what could be called “resolution of singularities for arithmetic schemes”.

3.5.16. Néron models.

(References: \cite{BLR90}, \cite{LT16})

Let $R$ be a discrete valuation ring. Let $K = \text{Frac} R$. Let $X$ be a nice $K$-variety. If $X$ has good reduction, i.e., $X$ has a smooth proper $R$-model $\mathcal{X}$, then $\mathcal{X}(R) \simeq X(K)$ by the valuative criterion for properness. But even if $X$ has bad reduction, it might have a smooth not-necessarily-proper $R$-model $\mathcal{N}$ satisfying $\mathcal{N}(R) \simeq X(K)$. To determine $\mathcal{N}$ uniquely, we would want to specify not just $\mathcal{N}(R)$, but the whole functor of points. Actually, if we insist that $\mathcal{N}$ be smooth over $R$, then it suffices to specify its functor of points restricted to smooth $R$-schemes, by Yoneda’s lemma (Lemma 2.3.4) applied in the category of smooth $R$-schemes. This motivates the following definition, which we give in the more general context of Dedekind domains (and which could be generalized further to integral Dedekind schemes):
**Definition 3.5.81.** Let $R$ be a Dedekind domain. Let $K = \operatorname{Frac} R$. Let $X$ be a smooth $K$-variety. A **Néron model** of $X$ is a smooth $R$-scheme $\mathcal{N}$ with an isomorphism $\mathcal{N}_K \simeq X$ such that for every smooth $R$-scheme $T$, the induced map $\mathcal{N}(T) \to X(T_K)$ is a bijection. (Some authors require also that $\mathcal{N}$ be of finite type, and otherwise call $\mathcal{N}$ a **Néron lift-model**, where lift stands for “locally of finite type” [LT16].)

As mentioned above, Yoneda’s lemma implies that $\mathcal{N}$ is unique if it exists. Moreover, if $X$ is a group scheme (see Section 5.1) and $\mathcal{N}$ exists, then the functor of points of $\mathcal{N}$ factors through **Groups**, so $\mathcal{N}$ is a group object in the category of smooth $R$-schemes; that is, $\mathcal{N}$ is a smooth group scheme over $R$.

Néron has his name attached to the concept because in 1964 he proved that $\mathcal{N}$ exists when $X$ is an abelian variety over the fraction field of a discrete valuation ring: see Section 5.7.5.

Here is a more recent result, in a different direction:

**Theorem 3.5.82 (Liu and Tong).** Let $S$ be an integral Dedekind scheme. Let $K = k(S)$. Let $X$ be a nice curve over $K$ of positive genus. Let $\mathcal{X} \to S$ be the minimal regular proper model of $X$ (see Section 9.3.1.6). Then the smooth locus $\mathcal{X}^{\text{smooth}}$ of $\mathcal{X} \to S$ is a Néron model of $X$.

**Proof.** See [LT16, Theorem 1.1].

3.6. **Rational maps**

3.6.1. **Rational maps and domain of definition.**

(Reference: [EGA I, §7])

**Definition 3.6.1 ([EGA I, 7.1.2]).** Let $X$ and $Y$ be $S$-schemes. Consider pairs $(U, \phi)$ where $U$ is a dense open subscheme of $X$ and $\phi: U \to Y$ is an $S$-morphism. Call pairs $(U, \phi)$ and $(V, \psi)$ equivalent if $\phi$ and $\psi$ agree on a dense open subscheme of $U \cap V$. A **rational map** $X \dashrightarrow Y$ is an equivalence class of such pairs. In other words,

\[
\{\text{rational maps } X \dashrightarrow Y\} := \lim_{\longrightarrow U} \operatorname{Hom}_S(U, Y),
\]

where $U$ ranges over dense open subschemes of $X$ ordered by reverse inclusion.

**Definition 3.6.2 ([EGA I, 7.2.1]).** The **domain of definition** of a rational map is the union of the $U$ where $(U, \phi)$ ranges over the equivalence class. It is an open subscheme of $X$.

**Definition 3.6.2** is useful mainly when $X$ is reduced and $Y$ is separated:

**Proposition 3.6.3.** Let $W$ be the domain of definition of a rational map $X \dashrightarrow Y$, where $X$ is reduced and $Y$ is separated. Then there is a unique $\xi: W \to Y$ such that $(W, \xi)$ belongs to the equivalence class.
Proof. If \((U, \phi)\) and \((V, \psi)\) are equivalent, so \(\phi\) and \(\psi\) agree on a dense open subscheme of \(U \cap V\), then by Corollary \[2.3.23\] they agree on all of \(U \cap V\). Therefore all the \((U, \phi)\) can be glued to give \((W, \xi)\). \(\square\)

Remark 3.6.4. One can drop the hypothesis that \(X\) is reduced in Proposition \[3.6.3\] if one replaces “dense” by the stronger property “scheme-theoretically dense” everywhere in Definition \[3.6.1\]. This leads to the notion of pseudo-morphism, a variant of the notion of rational map. See \[EGA IV\] \[20.2.1\].

3.6.2. Rational points over a function field.

Proposition 3.6.5. Let \(X\) be an integral \(k\)-variety, and let \(Y\) be an arbitrary \(k\)-variety. Let \(K = k(X)\).

(a) The natural map
\[
\{\text{rational maps from } X \text{ to } Y\} \longrightarrow Y(K)
\]
\[
[\phi: U \rightarrow Y] \longmapsto (\text{the composition } \text{Spec } K \hookrightarrow U \overset{\phi}{\rightarrow} Y)
\]
is a bijection.

(b) If moreover \(X\) is a regular curve and \(Y\) is proper, then we get bijections
\[
\text{Hom}_{k} (X, Y) \sim \{\text{rational maps from } X \text{ to } Y\} \sim Y(K).
\]

Proof. (a) Every dense open subscheme of \(X\) contains a dense affine open subscheme; i.e., the inverse system \((\text{Spec } A_{i})\) of dense affine open subschemes of \(X\) is cofinal in the system of all dense open subschemes. Thus we have bijections
\[
\{\text{rational maps from } X \text{ to } Y\} = \lim_{\longrightarrow} Y(U) \quad \text{(by definition)}
\]
\[
\simeq \lim_{\longrightarrow} Y(A_{i}) \quad \text{(by cofinality)}
\]
\[
\simeq Y(\lim_{\longrightarrow} A_{i}) \quad \text{(by Remark \[3.1.11\])}
\]
\[
= Y(K) \quad \text{(since } \lim_{\longrightarrow} A_{i} = K).\]

(b) The first bijection comes from the valuative criterion for properness: the map \(Y(X) \rightarrow Y(K)\) is bijective by Remark \[3.2.14\] The second bijection was given already in (a). \(\square\)

3.6.3. Dominant rational maps.

Definition 3.6.6. A rational map \(X \dashrightarrow Y\) is dominant if and only if for some (or equivalently, for each) representative \((U, \phi)\), the image \(\phi(U)\) is dense in \(Y\).
Corollary 3.6.7. (cf. [Har77, I.4.4]) The functor

\[
\begin{align*}
\{ & \text{integral } k\text{-varieties,} \\
& \text{dominant rational maps} \} \\
\mapsto & \{ \text{finitely generated field extensions of } k, \}
\end{align*}
\]

\[\text{opp} \quad X \mapsto \mathcal{O}(X) \]

is an equivalence of categories.

Proof. A rational map \(X \to Y\) is dominant if and only if it maps the generic point of \(X\) to the generic point of \(Y\); thus we have a functor from left to right. Restricting the bijection in Proposition 3.6.5(a) to the dominant rational maps \(X \to Y\) shows that the functor is fully faithful. Every finitely generated field extension of \(k\) is isomorphic to the function field of an integral \(k\)-variety (cf. Proposition 2.2.13); i.e., the functor is essentially surjective. \(\square\)

Definition 3.6.8. If \(X\) is an integral \(k\)-variety, the set of birational maps \(X \to X\) forms a group \(\text{Bir} X\). By Corollary 3.6.7, \(\text{Bir} X\) is isomorphic to the group \(\text{Aut}(k(X)/k)\) of automorphisms of the function field over \(k\).

Example 3.6.9. The group \(\text{Bir} \mathbb{P}^n\) is also called the Cremona group.

Definition 3.6.10. If \(\pi: X \to Y\) is a dominant rational map between integral \(k\)-varieties of the same dimension, then \(k(X)\) may be viewed as a finite extension of \(k(Y)\), and we define the degree of \(\pi\) as \(\deg \pi := [k(X) : k(Y)]\).

3.6.4. Lang–Nishimura theorem. If \(\pi: X \to Y\) is a morphism of \(k\)-varieties, and \(X\) has a \(k\)-point \(x\), then \(Y\) has a \(k\)-point, namely \(\pi(x)\). If \(\pi\) is only a rational map, this argument fails, since \(\pi\) might not be defined at \(x\), but surprisingly the same conclusion can be drawn, under mild hypotheses. The following theorem is due to Lang [Lan54] and Nishimura [Nis55].

Theorem 3.6.11 (Lang–Nishimura theorem). Let \(X \to Y\) be a rational map between \(k\)-varieties, where \(Y\) is proper. If \(X\) has a smooth \(k\)-point, then \(Y\) has a \(k\)-point.

Proof. Let \(x\) be the given smooth \(k\)-point on \(X\). Replacing \(X\) by an open neighborhood of \(x\), we may assume that \(X\) is integral. Let \(n = \dim X\). Proposition 3.5.65 gives the isomorphism in the chain of embeddings

\[
\mathcal{O}_{X,x} \hookrightarrow \mathfrak{O}_{X,x} \simeq k[[t_1, \ldots, t_n]] \hookrightarrow F := k((t_1))(t_2) \cdots ((t_n)),
\]

Since \(F\) is a field (an iterated formal Laurent series field), the fraction field \(\text{Frac} \mathcal{O}_{X,x} = k(X)\) embeds in \(F\). By Proposition 3.6.5(a), the rational map gives an element of \(Y(k(X))\), and hence an element of \(Y(F)\). Applying Lemma 3.6.12 \(n\) times shows that \(Y\) has a \(k\)-point. \(\square\)
Lemma 3.6.12. Let $Y$ be a proper $k$-variety. Let $L$ be a field extension of $k$, and let $L((t))$ be the formal Laurent series field over $L$. If $Y$ has an $L((t))$-point, then $Y$ has an $L$-point.

Proof. By the valuative criterion for properness (Theorem 3.2.12), the element of $Y(L((t)))$ extends to an element of $Y(L[[t]])$, which reduces modulo $t$ to an element of $Y(L)$.

Remark 3.6.13. The Lang–Nishimura theorem can be explained geometrically as follows. If $\dim_x X > 0$, then one can show that $X$ contains an integral curve $C$ such that
- $x$ is a smooth point of $C$, and
- $C$ meets the domain of definition of the rational map $\phi$.

The valuative criterion for properness shows that $\phi|_C : C \to Y$ extends to be defined at $x$. It maps $x$ to a $k$-point of $Y$. (The reason that we did not present the proof this way is that the existence of $C$ is not immediate.)

Remark 3.6.14. For another proof of Theorem 3.6.11 see Exercise 3.11.

Remark 3.6.15. In Theorem 3.6.11, one cannot conclude that $Y$ has a smooth $k$-point.

The Lang–Nishimura theorem implies that the property of having a $k$-point is a birational invariant of smooth, proper, integral $k$-varieties:

Corollary 3.6.16. Let $X$ and $Y$ be smooth, proper, integral $k$-varieties that are birational to each other. Then $X$ has a $k$-point if and only if $Y$ has a $k$-point.

3.7. Frobenius morphisms

(Reference: [SGA 5, XV])

Let $p$ be a prime number. Let $X$ be a scheme of characteristic $p$, i.e., a scheme with $p\mathcal{O}_X = 0$. Then the absolute Frobenius morphism is the morphism of schemes $F_X : X \to X$ that is the identity on topological spaces and that induces the $p^{\text{th}}$-power homomorphism $f \mapsto f^p$ on each ring $\mathcal{O}_X(U)$.

If $S$ is a scheme of characteristic $p$, and $X$ is an $S$-scheme, then let $X^{(p)}$ be the base extension of $X$ by $F_S$; then the universal property of the fiber product gives a morphism $F_{X/S} : X \to X^{(p)}$ called the relative Frobenius morphism:

\[ X \xrightarrow{F_{X/S}} X^{(p)} \xrightarrow{\alpha} X \]

\[ S \xrightarrow{F_S} S \]
As the diagram shows, \( F_{X/S} \) is an \( S \)-morphism, but \( F_X \) is generally not an \( S \)-morphism because it lies over \( F_S \): \( S \to S \) instead of the identity \( 1_S \).

**Example 3.7.2.** Let \( k \) be a field of characteristic \( p \). Let \( S = \text{Spec} \, k \) and let \( X \) be a \( k \)-variety. Then \( X^{(p)} \) is the \( k \)-variety obtained by replacing the coefficients in the equations defining \( X \) by their \( p \)th powers. Write \( F_{X/k} = F_{X/S} \). On regular functions, the three morphisms along the top of (3.7.1) act as follows:

\[
\begin{align*}
F_{X/k} &: \text{identity on constants (elements of } k\text{), raises variables to the } p \text{th power} \\
\alpha &: \text{raises constants to the } p \text{th power, identity on variables} \\
F_X &: \text{raises } \textit{everything} \text{ to the } p \text{th power}.
\end{align*}
\]

Of these three morphisms, usually only \( F_{X/k} \) is a morphism of \( k \)-varieties; it is a finite morphism.

**Remark 3.7.3.** If \( X \) is an integral variety over a field \( k \) of characteristic \( p \), then the degree of \( F_{X/k} : X \to X^{(p)} \) is \( p^{\dim X} \) (see Definition 3.6.10). In particular, if \( \dim X > 0 \), then \( F_{X/k} \) is not an isomorphism, and hence not an automorphism even if \( X^{(p)} \simeq X \) over \( k \).

**Remark 3.7.4.** If we specialize (3.7.1) to the case where \( S = \text{Spec} \, \mathbb{F}_p \), then \( F_S \) is the identity, so \( X^{(p)} \simeq X \) as an \( \mathbb{F}_p \)-scheme via \( \alpha \).

The following will be used later, in the proof of Proposition 7.5.17.

**Lemma 3.7.5.** If \( X \to S \) is an étale morphism of schemes of characteristic \( p \), then the diagram

\[
\begin{array}{ccc}
X & \xrightarrow{F_X} & X \\
\downarrow & & \downarrow \\
S & \xrightarrow{F_S} & S
\end{array}
\]

is cartesian; that is, the upper left \( X \) is the fiber product of the rest of the diagram.

**Proof.** By [SGA 5, XV, Proposition 2(c)(2)], \( F_{X/S} \) is an isomorphism. \( \square \)

**Remark 3.7.6.** Let \( q = p^n \) for some \( n \geq 1 \). Under the same hypotheses as above, one can define an absolute \( q \)-power Frobenius morphism \( X \to X \), a scheme \( X^{(q)} \), and a relative \( q \)-power Frobenius morphism \( X \to X^{(q)} \) over \( S \) in the same way, by replacing \( p \) by \( q \).

### 3.8. Comparisons

Given a family of morphisms \( (X_i \to Y)_{i \in I} \), we may glue along the empty subsets of the \( X_i \) to obtain a single morphism \( \coprod_{i \in I} X_i \to Y \). Here \( \coprod_{i \in I} X_i \) is the disjoint union scheme.
**Definition 3.8.1.** A *Zariski open covering morphism* is a morphism \( \coprod_{i \in I} X_i \to Y \) obtained as a disjoint union of open immersions \( X_i \to Y \) whose images form an open covering of \( Y \). (This terminology is not standard, but it will be convenient to have.)

**Proposition 3.8.2.** Let \( f : X \to Y \) be a morphism of schemes. Each of the following statements implies the next:

- \( f \) is a Zariski open covering morphism.
- \( f \) is étale and surjective.
- \( f \) is fppf.
- \( f \) is fpqc.

**Proof.** We leave this to the reader, as Exercise 3.13.

Proposition 3.8.2 suggests that fpqc morphisms may be considered generalizations of open coverings. This point of view will prevail in Chapters 4 and 6.

**Exercises**

3.1. Let \( A \) be a commutative ring. Let \( I \) be an ideal in the polynomial ring \( A[t_1, \ldots, t_n] \) for some \( n \geq 0 \). Prove that \( A[t_1, \ldots, t_n]/I \) is a finitely presented \( A \)-algebra if and only if \( I \) is a finitely generated ideal.

3.2. Which of the following morphisms are flat? Faithfully flat?

- (a) \( \text{Spec} \ Z[1/2] \to \text{Spec} \ Z. \)
- (b) \( \text{Spec} \ (Z \times \mathbb{Z}/2) \to \text{Spec} \ Z. \)
- (c) \( \text{Spec} \ \mathbb{C}[x, y]/(xy - 1) \to \text{Spec} \ \mathbb{C}[x]. \)
- (d) \( \text{Spec} \ \mathbb{C}[x, y]/(xy) \to \text{Spec} \ \mathbb{C}[x]. \)
- (e) \( \text{Spec} \ \mathbb{C}[x, y]/(y^2 - x^3) \to \text{Spec} \ \mathbb{C}[x]. \)
- (f) \( X \to \mathbb{A}^2_c, \) where \( X \) is the blow-up of \( \mathbb{A}^2_c \) at the origin.

3.3. Give an example of an integral domain \( R \) and fraction field \( K \) such that the natural map \( \text{Spec} \ (R) \to \text{Spec} \ (K) \) is not a bijection.

3.4. Let \( k \) be a global field, and let \( \Omega_k, \mathcal{O}_{k,S}, k_v, \mathcal{O}_v, \) and \( A \) be as in Section 1.1.3. Let \( X \) be a \( k \)-variety.

- (a) Prove that there is a finite subset \( S \subset \Omega_k, \) a separated scheme \( \mathcal{X} \) of finite type over \( \mathcal{O}_{k,S}, \) and an isomorphism \( \mathcal{X}_k \cong X; \) fix these.
- (b) Explain why \( \mathcal{X} (\mathcal{O}_v) \) may be identified with a subset of \( X (k_v) \) for each \( v \notin S. \)
- (c) Prove that there is a bijection

\[
X (A) \to \coprod'_{v \in \Omega_k} (X (k_v), \mathcal{X} (\mathcal{O}_v)).
\]

(Hint: Use Remark 3.1.11 and prove the following)
Lemma: If $Y$ is a quasi-compact and quasi-separated $A$-scheme for some ring $A$, and $(R_i)_{i \in I}$ is a collection of local $A$-algebras, then the natural map $Y(\prod R_i) \to \prod Y(R_i)$ is a bijection.

Even with this hint, the problem is hard.)

(d) Prove that if moreover $X$ is proper over $k$, then the natural map

$$X(A) \to \prod_{v \in \Omega_k} X(k_v)$$

is a bijection.

3.5. Give an example of a prime $p$ and a nice $\mathbb{Q}_p$-variety $X$ with proper $\mathbb{Z}_p$-models $\mathcal{X}$ and $\mathcal{X}'$ such that their special fibers are isomorphic and such that $\mathcal{X}$ is regular and $\mathcal{X}'$ is not.

3.6. Let $X$ be a variety over a field $k$. Show that it is possible to find finitely many locally closed subvarieties $Y_i$ of $X$ (i.e., open subvarieties of closed subvarieties) such that each $Y_i$ is smooth and geometrically integral and $\bigcup Y_i(k) = X(k)$.

3.7. Give an example of a prime $p$ and a geometrically integral curve $X$ over $\mathbb{Q}_p$ such that $X(\mathbb{Q}_p)$ consists of a single point.

3.8. Let $R$ be a Dedekind domain, let $K = \text{Frac } R$, and let $X$ be a smooth proper $K$-scheme. Suppose that for each nonzero prime $p$ of $R$, the scheme $X$ has good reduction at $p$. Prove that there is a smooth proper $R$-model of $X$.

3.9. Let $\phi: X \to Y$ be a rational map from a regular $k$-variety to a proper $k$-variety. Prove that there is a closed subset $Z \subseteq X$ of codimension $\geq 2$ in $X$ such that $\phi$ extends to a morphism from $X - Z$ to $Y$.

3.10. For a proper variety $X$ over a global field $k$, explain why strong approximation with respect to $\emptyset$ is equivalent to weak approximation.

3.11. Give a proof of the Lang–Nishimura theorem by induction on $\dim X$, along the following lines: Blow up the smooth $k$-point on $X$ and apply the inductive hypothesis to the restriction of the rational map to the exceptional divisor $E$. (This proof is due to János Kollár and Endre Szabó [RY00, Proposition A.6].)

3.12. Show that the Lang–Nishimura theorem can fail if either of the following changes is made:

(a) The assumption that $Y$ is proper is dropped.

(b) The given $k$-point on $X$ is not assumed to be smooth.

3.13. Prove Proposition 3.8.2 comparing Zariski open covering, étale and surjective, fppf, and fpqc morphisms.

3.14. The inclusions $k[x] \to k[x, x^{-1}]$ and $k[x] \to k[[x]]$ define a morphism $f$ from the disjoint union $X := \text{Spec } k[x, x^{-1}] \amalg \text{Spec } k[[x]]$ to $Y := \text{Spec } k[x]$. Show that $f$ is fpqc but not fppf.
Faithfully flat descent

Suppose that one wants to carry out a construction of a variety over a base field $k$. Sometimes all one can do directly is to construct its analogue $X'$ over some field extension $k'$. Then one is faced with deciding whether $X'$ is the base extension of some $k$-variety $X$, and if so, to construct $X$. This is a special case of the problem known as descent.

Weil gave necessary and sufficient conditions for descending a quasi-projective variety over a Galois extension $k' \supseteq k$. Later, Grothendieck noticed that these conditions were analogous to the conditions for reconstructing an object from local data by glueing; this led him to a common generalization.

4.1. Motivation: glueing sheaves

4.1.1. A glueing problem. Let $S$ be a topological space, and let $\{S_i\}_{i \in I}$ denote an open covering of $S$. Suppose we are given a sheaf $\mathcal{F}_i$ on $S_i$ for each $i$. Under what conditions is there a sheaf $\mathcal{F}$ on $S$ such that $\mathcal{F}|_{S_i} \simeq \mathcal{F}_i$? (Cf. Exercise II.1.22 of [Har77].)

4.1.2. Solution: the glueing conditions. If $\mathcal{F}$ exists, then the restrictions of $\mathcal{F}|_{S_i}$ and $\mathcal{F}|_{S_j}$ to $S_{ij} := S_i \cap S_j$ must be isomorphic (both isomorphic to $\mathcal{F}|_{S_{ij}}$). Thus we should at least insist that

\begin{equation}
\text{(4.1.1)} \quad \text{For all } i \text{ and } j, \text{ we are given an isomorphism } \phi_{ij} : \mathcal{F}_i|_{S_{ij}} \rightarrow \mathcal{F}_j|_{S_{ij}}.
\end{equation}

Can we then glue the $\mathcal{F}_i$ via the $\phi_{ij}$? On a triple intersection $S_{ijk} := S_i \cap S_j \cap S_k$, the sheaves $\mathcal{F}_i|_{S_{ijk}}$, $\mathcal{F}_j|_{S_{ijk}}$, $\mathcal{F}_k|_{S_{ijk}}$ are identified in pairs by $\phi_{ij}$, $\phi_{jk}$, and $\phi_{ik}$, forming a triangle of identifications. For these identifications to be compatible, we should insist that the composition of two sides of the triangle gives the third, i.e., that we have the following “cocycle condition”:

\begin{equation}
\text{(4.1.2)} \quad \text{For all } i, j, k, \text{ we have } \phi_{jk} \circ \phi_{ij} = \phi_{ik} \text{ on } S_{ijk}.
\end{equation}

In the case where $\mathcal{F}$ exists, each $\phi_{ij}$ is the identity, so these are automatically satisfied. The glueing theorem states that given sheaves $\mathcal{F}_i$ on $S_i$, if there exist isomorphisms as in (4.1.1) satisfying (4.1.2), then up to isomorphism there exists a unique sheaf $\mathcal{F}$ on $S$ with isomorphisms $\phi_i : \mathcal{F}|_{S_i} \rightarrow \mathcal{F}_i$ such that $\phi_i$ and $\phi_j$ identify the identity on $\mathcal{F}|_{S_{ij}}$ with $\phi_{ij}$.
Example 4.1.3. Let $k$ be a field, and let $S = \mathbb{P}^1_k$, which is covered by two affine open subsets $S_1 = \text{Spec } k[t] \simeq \mathbb{A}^1_k$ and $S_2 = \text{Spec } k[t^{-1}] \simeq \mathbb{A}^1_k$ whose intersection is $S_{12} = \text{Spec } k[t, t^{-1}] \simeq \mathbb{A}^1_k - \{0\}$. Let $M_1 = k[t]$ and $M_2 = k[t^{-1}]$ be free rank 1 modules over $k[t]$ and $k[t^{-1}]$, respectively. Let $\mathcal{F}_1 = \tilde{M}_1$ and $\mathcal{F}_2 = \tilde{M}_2$ be the corresponding sheaves on $S_1$ and $S_2$. Let $d \in \mathbb{Z}$. The isomorphism

$$M_1 \otimes_{k[t]} k[t, t^{-1}] = k[t, t^{-1}] \xrightarrow{t^{-d}} k[t, t^{-1}] = M_2 \otimes_{k[t^{-1}]} k[t, t^{-1}]$$

given by multiplication by $t^{-d}$ induces an isomorphism of sheaves $\phi_{12} : \mathcal{F}_1|_{S_{12}} \to \mathcal{F}_2|_{S_{12}}$. Let $\phi_{11}$ and $\phi_{22}$ be the identity, and let $\phi_{21}$ be $\phi_{12}^{-1}$. Then (4.1.2) is trivially satisfied, so we can glue to get a sheaf $\mathcal{F}$ on $\mathbb{P}^1_k$. In fact, $\mathcal{F}$ is $\mathcal{O}(d)$.

Remark 4.1.4. One can also glue morphisms of sheaves, in the following sense. Let $S$ be a topological space, and let $\{S_i\}_{i \in I}$ denote an open covering of $S$. Let $\mathcal{F}$ and $\mathcal{G}$ be two sheaves on $S$. For each $i \in I$, let $\phi_i : \mathcal{F}|_{S_i} \to \mathcal{G}|_{S_i}$ be a morphism of sheaves. If for every $i, j \in I$, the restrictions of $\phi_i$ and $\phi_j$ to $S_{ij}$ are equal, then there exists a unique morphism $\phi : \mathcal{F} \to \mathcal{G}$ such that $\phi|_{S_i} = \phi_i$ for each $i \in I$. (In fact, this statement holds very generally, for sheaves on any site.)

4.1.3. Rewriting the glueing conditions. We can restate the glueing conditions by introducing the disjoint union $S' := \bigsqcup S_i$. Let $\pi : S' \to S$ be the “open covering morphism” that on each $S_i$ is the inclusion. To give the $\mathcal{F}_i$ on all the $S_i$ is equivalent to giving a single sheaf $\mathcal{F}'$ on $S'$. The question is whether there exists a sheaf $\mathcal{F}$ on $S$ such that the sheaf $\pi^{-1}\mathcal{F}$ on $S'$ is isomorphic to the given $\mathcal{F}'$.

The fiber product $S'' := S' \times_S S'$ equals the disjoint union of $S_i \times_S S_j = S_i \cap S_j =: S_{ij}$ over all $i, j$. Let $p_1 : S'' \to S'$ and $p_2 : S'' \to S'$ be the two projections. The sheaf $p_1^{-1}\mathcal{F}'$ restricted to the piece indexed by $ij$ corresponds to the sheaf $\mathcal{F}_1|_{S_{ij}}$. Thus, asking for the $\phi_{ij}$ as in (4.1.1) is equivalent to asking that

(4.1.5) We are given an isomorphism $\phi : p_1^{-1}\mathcal{F}' \to p_2^{-1}\mathcal{F}'$ of sheaves on $S''$.

Let $S''' := S' \times_S S' \times_S S'$. Let $p_{13} : S''' \to S''$ be the projection onto the first and third coordinates, and so on. Then $p_{13}^{-1}\phi$ is an isomorphism of sheaves on $S'''$. The cocycle condition (4.1.2) can now be rewritten as

$$p_{13}^{-1}\phi = p_{23}^{-1}\phi \circ p_{12}^{-1}\phi.$$ 

4.2. Faithfully flat descent for quasi-coherent sheaves

The idea behind faithfully flat descent is that, in the context of schemes, in place of the Zariski open covering morphisms $S' \to S$ of Section 4.1.3 we can use the much more general fpqc morphisms defined in Section 3.4. We develop this first for quasi-coherent sheaves, by
analogy with the conditions in Section 4.1.3. The operation $p^{-1}$ on sheaves is replaced by $p^*$, which is the appropriate operation for quasi-coherent sheaves.

4.2.1. Descent data. Let $p: S' \to S$ be an fpqc morphism of schemes. Let $\mathcal{F}'$ denote a quasi-coherent $S'$-module (that is, a quasi-coherent sheaf of $\mathcal{O}_{S'}$-modules). Define $S''$ and $S'''$ as in Section 4.1.3, using fiber product of schemes instead of fiber products of topological spaces. Define the projections $p_1$, $p_{13}$, and so on as before.

**Definition 4.2.1.** With notation as in the previous paragraph, a descent datum on $\mathcal{F}'$ is an isomorphism $\phi: p_1^* \mathcal{F}' \to p_2^* \mathcal{F}'$ of $S''$-modules satisfying the cocycle condition

$$p_{13}^* \phi = p_{23}^* \phi \circ p_{12}^* \phi.$$

A morphism of quasi-coherent $S'$-modules with descent data $(\mathcal{F}', \phi) \to (\mathcal{G}', \psi)$ is a morphism of $S'$-modules $f: \mathcal{F}' \to \mathcal{G}'$ such that

$$
\begin{array}{ccc}
p_1^* \mathcal{F}' & \xrightarrow{p_1^* f} & p_1^* \mathcal{G}' \\
\phi & \downarrow & \downarrow \psi \\
p_2^* \mathcal{F}' & \xrightarrow{p_2^* f} & p_2^* \mathcal{G}'
\end{array}
$$

commutes.

**Remark 4.2.2.** There is an elegant reinterpretation of the notion of descent datum in terms of simplicial schemes. See [SP, Tag 0248] for an introduction.

If $\mathcal{F}$ is a quasi-coherent $S$-module, then $p^* \mathcal{F}$ has a natural descent datum $\phi_{\mathcal{F}}$, consisting of the canonical isomorphism

$$p_1^*(p^* \mathcal{F}) \simeq (p \circ p_1)^* \mathcal{F} = (p \circ p_2)^* \mathcal{F} \simeq p_2^*(p^* \mathcal{F}).$$

4.2.2. The descent theorem for quasi-coherent sheaves. We now have the main theorem of descent theory, in the context of quasi-coherent modules.

**Theorem 4.2.3 (Grothendieck).** If $p: S' \to S$ is an fpqc morphism, then the functor

$$\{\text{quasi-coherent } S\text{-modules}\} \to \{\text{quasi-coherent } S'\text{-modules with descent data}\},$$

$$\mathcal{F} \mapsto (p^* \mathcal{F}, \phi_{\mathcal{F}})$$

is an equivalence of categories.

The proof takes only a few pages. It reduces to a statement about modules over rings generalizing Theorem 1.3.11. See [Gro95a, Theorem 1] or [BLR90, Section 6.1] for details.
4.3. Faithfully flat descent for schemes

We now consider the problem of descending schemes instead of quasi-coherent sheaves. Let \( p : S' \to S \) be fpqc. Let \( X' \) be an \( S' \)-scheme. Under what conditions is \( X' \) isomorphic to an \( S' \)-scheme of the form \( p^*X \) for some \( S \)-scheme \( X \)? (We use the notation \( p^*X = X \times_S S' \).)

4.3.1. Descent data for schemes. The answer is almost the same as for sheaves. A descent datum on an \( S' \)-scheme \( X' \) is an \( S'' \)-isomorphism \( \phi : p_1^*X' \to p_2^*X' \) satisfying the usual cocycle condition. The pairs \( (X', \phi) \) are the objects of a category as before. If \( X \) is an \( S \)-scheme, then \( p^*X \) has a canonical descent datum \( \phi_X \). Call \( \phi \) effective if \( (X', \phi) \cong (p^*X, \phi_X) \) for some \( S \)-scheme \( X \). Ideally every descent datum would be effective, as happened for quasi-coherent sheaves, but this is not quite true for schemes; see Section 6.7 of [BLR90] for a counterexample.

4.3.2. Open subschemes stable under a descent datum.

Definition 4.3.1. Let \( X' \) be an \( S' \)-scheme, and let \( \phi : p_1^*X' \to p_2^*X' \) be a descent datum. An open subscheme \( U' \subseteq X' \) is called stable under \( \phi \) if \( \phi \) induces a descent datum on \( U' \), that is, if \( \phi \) restricts to an isomorphism \( p_1^*U' \to p_2^*U' \) of \( S'' \)-schemes.

The idea behind this definition is that the stable open subschemes of \( X' \) are the ones that are supposed to be of the form \( p^*U \) for an open subscheme \( U \) of \( X \), if \( X \) exists.

4.3.3. The descent theorem for schemes.

Definition 4.3.2. [EGA II] 1.6.1] A morphism \( f : X \to S \) is affine if \( f^{-1}S_0 \) is affine for each affine open subscheme \( S_0 \) of \( S \). In this case, call \( X \) an affine \( S \)-scheme.

Warning 4.3.3. An affine \( S \)-scheme is not necessarily affine as a scheme; “relatively affine” might be clearer terminology.

Definition 4.3.4. [EGA II] 5.1.1] A scheme is quasi-affine if it is an open subscheme of an affine scheme and is quasi-compact. A morphism \( f : X \to S \) is quasi-affine if \( f^{-1}S_0 \) is quasi-affine for each affine open subscheme \( S_0 \) of \( S \).

Theorem 4.3.5. Let \( p : S' \to S \) be an fpqc morphism of schemes.

(i) The functor \( X \mapsto p^*X \) from \( S \)-schemes to \( S' \)-schemes with descent data is fully faithful.
(ii) The functor \( X \mapsto p^*X \) from quasi-affine \( S \)-schemes to quasi-affine \( S' \)-schemes with descent data is an equivalence of categories.
(iii) Suppose that \( S \) and \( S' \) are affine. Then a descent datum \( \phi \) on an \( S' \)-scheme \( X' \) is effective if and only if \( X' \) can be covered by quasi-affine open subschemes which are stable under \( \phi \).
Remark 4.3.6. Parts (ii) and (iii) hold also if quasi-affine is replaced by affine everywhere. Part (iii) will be used primarily to show that certain descent data are effective (the “if” part), so it is preferable to have the more widely applicable criterion.

The proof of Theorem 4.3.5 reduces to the proof of Theorem 4.2.3. See [Gro95a, B.1, Theorem 2], [BLR90, Section 6.1, Theorem 6], and [SP, Tag 0247] for details.

4.3.4. Descending properties of morphisms. When an $S$-scheme $X$ is base extended to an $S'$-scheme $X'$, we know that $X'$ inherits many properties from $X$. Conversely, when an $S'$-scheme $X'$ is descended to an $S$-scheme $X$, one hopes that $X$ inherits properties from $X'$. Fortunately, this is the case in fpqc descent, for many properties.

Theorem 4.3.7. Let “blah” denote a property for which a positive answer is listed in the “fpqc descent” column of Table 1. Let $S' \to S$ be an fpqc morphism. For any $S$-scheme $X$, let $X' = X_{S'}$.

(i) Let $X$ be an $S$-scheme. If the base extension $X' \to S'$ is blah, then the original morphism $X \to S$ is blah.
(ii) More generally, if $X \to Y$ is a morphism of $S$-schemes and its base extension $X' \to Y'$ by $S' \to S$ is blah, then the original morphism $X \to Y$ is blah.

PROOF.
(i) See the references in Table 1.
(ii) Since the morphism $S' \to S$ is fpqc, Table 1 implies that its base extension $Y' \to Y$ is fpqc. Now the result follows from (i). □

Remark 4.3.8. It is easy to understand why the surjectivity implicit in fpqc is a hypothesis for a statement like Theorem 4.3.7(ii). If $S' \to S$ were not surjective, the morphism $X \to S$ could have bad behavior above points of $S$ not in the image of $S'$, and this behavior would not be seen in the base extension $X' \to S'$.

4.4. Galois descent

Let $k$ be a field, and let $k'$ be a finite Galois extension of $k$. Let $S = \text{Spec } k$ and $S' = \text{Spec } k'$. Then $S' \to S$ is fpqc, so we can apply Theorem 4.3.5(iii) to say something about descending $k'$-schemes to $k$-schemes.
Remark 4.4.1. This case was developed by Weil. Later Grothendieck generalized it to the fpqc descent we presented first.

Let $G = \text{Gal}(k'/k)$. The left action of $G$ on $k'$ induces a right action of $G$ on $S'$: each $\sigma \in G$ induces an automorphism $\sigma^*$ of $S'$.

**Proposition 4.4.2.**

(i) Giving a descent datum on a $k'$-scheme $X'$ is equivalent to giving a right action of $G$ on $X'$ compatible with the right action of $G$ on $S'$, i.e., to giving a collection of isomorphisms $\tilde{\sigma}: X' \to X'$ for $\sigma \in G$ such that

\[
\begin{array}{ccc}
X' & \xrightarrow{\tilde{\sigma}} & X' \\
\downarrow & & \downarrow \\
S' & \xrightarrow{\sigma^*} & S'
\end{array}
\]

commutes for each $\sigma \in G$ and $\tilde{\sigma} \tau = \tilde{\tau} \tilde{\sigma}$ for all $\sigma, \tau \in G$;

(ii) An isomorphism between $k'$-schemes with descent data is a $k'$-isomorphism that is equivariant for the $G$-actions in part (i).

(iii) An open subscheme $U'$ of a $k'$-scheme $X'$ is stable under a descent datum described as in part (i) if and only if $\tilde{\sigma}(U') = U'$ for all $\sigma \in G$.

**Proof.** Since $k'/k$ is Galois, we have an isomorphism

\[
k' \otimes_k k' \xrightarrow{\sim} \prod_{\sigma \in G} k'
\]

\[
a \otimes b \mapsto (a \cdot \sigma b)_{\sigma \in G}.
\]

This induces isomorphisms

\[
S'' \simeq \prod_{\sigma \in G} \text{Spec } k' =: S' \times G.
\]

\[
S''' \simeq S' \times S'' \simeq S' \times S' \times G \simeq S' \times G \times G.
\]

Plugging these into the definition of descent datum and doing some straightforward calculations yields the results. See [BLR90, §6.2B] for the details. $\square$

The morphisms $\tilde{\sigma}$ are not morphisms of $k'$-schemes, since they lie over the $\sigma^*$ instead of the identity. If desired, we can rewrite the conditions in Proposition 4.4.2 in terms of $k'$-morphisms. Recall from Section 2.2 that we can transform a $k'$-scheme by an element $\sigma \in G$.

**Proposition 4.4.4.** Let $X'$ be a $k'$-scheme.
(i) Giving a descent datum on $X'$ is equivalent to giving a collection of $k'$-isomorphisms $f_\sigma : \sigma X' \to X'$ for $\sigma \in G$ satisfying the "cocycle condition" $f_\sigma f_\tau = f_\sigma \cdot \sigma(f_\tau)$ for all $\sigma, \tau \in G$.

(ii) An isomorphism between varieties with descent data, say $X'$ with $(f_\sigma)_{\sigma \in G}$ and $Y'$ with $(g_\sigma)_{\sigma \in G}$, is a $k'$-isomorphism $b : X' \to Y'$ such that $f_\sigma = b^{-1} g_\sigma(\sigma b)$ for all $\sigma \in G$.

(iii) An open subscheme $U' \subseteq X'$ is stable under a descent datum described as in part (i) if and only if $f_\sigma(\sigma U') = U'$ for all $\sigma \in G$.

PROOF. We will use Proposition 4.4.2.

(i) Because of the isomorphism $\sigma X' \to X'$ lying over $\sigma^*$, giving an isomorphism $\tilde{\sigma} : X' \to X'$ over $\sigma^*$ is equivalent to giving a $k'$-isomorphism $f_\sigma : \sigma X' \to X'$, as shown in the following commutative diagram:

(Squares are cartesian, and we use dotted arrows to denote $k'$-morphisms.) The diagram shows that $\tilde{\sigma}_\tau = \tilde{\tau} \tilde{\sigma}$ is equivalent to $f_{\sigma \tau} = f_\sigma \cdot \sigma(f_\tau)$.

(ii) A $k'$-isomorphism $b : X' \to Y'$ is $G$-equivariant if and only if for every $\sigma \in G$, the 3-dimensional diagram formed by two copies of (4.4.5), one for $X'$ and one for $Y'$, connected by vertical isomorphisms given by $b : X' \to Y'$ and $\sigma b : \sigma X' \to \sigma Y'$, commutes,
or equivalently,
\[
\begin{array}{ccc}
\sigma X' & \xrightarrow{f_\sigma} & X' \\
\sigma b & \downarrow & b \\
\sigma Y' & \xrightarrow{g_\sigma} & Y'
\end{array}
\]
commutes.

(iii) The diagram (4.4.5) shows that \( \tilde{\sigma}(U') = U' \) if and only if \( f_\sigma(U') = U' \).

Corollary 4.4.6. Let \( k'/k \) be a finite Galois extension of fields. Let \( X' \) be a quasi-projective \( k' \)-scheme. Suppose that we are given \( k' \)-isomorphisms \( f_\sigma : \sigma X' \to X' \) for \( \sigma \in G \) satisfying \( f_{\sigma\tau} = f_\sigma \cdot \sigma(f_\tau) \) for all \( \sigma, \tau \in G \). Then \( X' = X_{k'} \) for some \( k \)-scheme \( X \).

Proof. As in the proof of Proposition 4.4.4 giving the \( f_\sigma \) is equivalent to giving a right action of \( G \) on \( X' \). By Theorem 4.3.5, it suffices to show that \( X' \) can be covered by \( G \)-invariant quasi-affine open subsets. Fix an embedding \( X' \hookrightarrow \mathbb{P}^n_{k'} \). Given \( x' \in X' \), we can choose a hypersurface \( H \subset \mathbb{P}^n_{k'} \) that does not meet the \( G \)-orbit of \( x' \). (In fact, if \( k' \) is infinite, then a hyperplane suffices.) Let \( U' = X' - H \). Then \( \bigcap_{\sigma \in G} \tilde{\sigma}(U') \) is a quasi-affine open subset of \( X' \) containing \( x' \). \( \square \)

Remark 4.4.7. More generally, a finite and faithfully flat morphism of schemes \( p : S' \to S \) equipped with a finite group \( G \) of automorphisms of \( S' \) as an \( S \)-scheme (acting on the right) is called a Galois covering with Galois group \( G \) if the morphism \( S' \times G \to S'' \) given by \((\text{id}, \sigma)\) on the piece \( S' \times \{\sigma\} \) for each \( \sigma \in G \) is an isomorphism of schemes (cf. (4.4.3)). Propositions 4.4.2 and 4.4.4 continue to hold in this setting. Corollary 4.4.6 holds too, provided that we assume that \( S \) is affine (so that \( S' \) is affine too): this condition is used to construct the hypersurface \( H \) in the proof.

Remark 4.4.8. Sometimes the scheme \( X' \) to be descended to \( k \) is over \( k_s \) instead of a finite Galois extension of \( k \). In that case, assuming that \( X' \) is finitely presented, we may use that \( k_s \) is the direct limit of its finite Galois subextensions to obtain \( X' \) as the base extension of a scheme over a finite Galois extension of \( k \) before applying Galois descent.

4.5. Twists

(Reference: Section III.1 of \cite{Ser02})

Let \( X \) be a quasi-projective \( k \)-variety. Let \( k'/k \) be a Galois extension of fields, and let \( G = \text{Gal}(k'/k) \).

Definition 4.5.1. A \( k'/k \)-twist (or \( k'/k \)-form) of \( X \) is a \( k \)-variety \( Y \) such that there exists an isomorphism \( \phi : X_{k'} \sim Y_{k'} \). A twist of \( X \) is a \( k_s/k \)-twist of \( X \).
The set of $k$-isomorphism classes of $k'/k$-twists of $X$ is a pointed set, with neutral element given by the isomorphism class of $X$. The action of $\mathfrak{G}$ on $k'$ induces an action of $\mathfrak{G}$ on the automorphism group $\text{Aut} X_{k'}$.

**Theorem 4.5.2.** There is a natural bijection of pointed sets

$$\frac{\{k'/k\text{-twists of }X\}}{\text{k-isomorphism}} \xrightarrow{\sim} \text{H}^1(\mathfrak{G}, \text{Aut} X_{k'}).$$

**Warning 4.5.3.** It is the automorphism group of $X_{k'}$, not $X$, that appears. Also, the group $\text{Aut} X_{k'}$ may be nonabelian, so it may be necessary to use nonabelian group cohomology as in [Ser02, I.§5].

**Proof of Theorem 4.5.2.** We may assume that $k'/k$ is finite, since at the end we can take a direct limit of both sides.

For each $\sigma \in \mathfrak{G}$, we identify $\sigma X_{k'}$ with $X_{k'}$. To give a $k'/k$-twist of $X$ is to descend $X_{k'}$ to a $k$-variety. By Theorem 4.3.5 and the fact that $X_{k'}$ is quasi-projective, this is the same as giving a descent datum on $X_{k'}$. By Proposition 4.4.4(i) this is the same as giving a 1-cocycle $\mathfrak{G} \to \text{Aut} X_{k'}$.

By Theorem 4.3.5(i), two such twists are $k$-isomorphic if and only if the descent data are isomorphic, which by Proposition 4.4.4(ii) holds if and only if the 1-cocycles are cohomologous.

**Remark 4.5.4.** Explicitly, given a $k'/k$-twist $Y$, an associated 1-cocycle is constructed as follows: choose a $k'$-isomorphism $\phi: X_{k'} \xrightarrow{\sim} Y_{k'}$ and define

$$f_\sigma := \phi^{-1}(\sigma \phi) \in \text{Aut} X_{k'}.$$

**Warning 4.5.5.** Given an element of $\text{H}^1(\mathfrak{G}, \text{Aut} X_{k'})$, one gets an isomorphism class of $k'/k$-twists, but there is no natural way to select a particular twist in that isomorphism class. Thus, strictly speaking, it is incorrect to speak of “the twist associated to a cohomology class.”

To determine a twist, one should select a cocycle representing that cohomology class.

**Important Remark 4.5.6.** Although we used quasi-projective $k$-varieties in Theorem 4.5.2, an analogous result holds for twists of many other “$k$-objects”, where $\text{Aut} X_{k'}$ now denotes the automorphism group of $X_{k'}$ as a $k'$-object. (To make this precise, one should specify a category of $k$-objects, a corresponding category of $k'$-objects, a notion of base extension, etc., satisfying certain axioms.) To get injectivity of the natural map in Theorem 4.5.2, one needs that $\mathfrak{G}$-invariant morphisms between base extensions of $k$-objects descend. To get surjectivity one needs that descent data on $k'$-objects be effective. These conditions (especially the latter) can sometimes fail.
4.5.1. Severi–Brauer varieties.

Definition 4.5.7. A Severi–Brauer variety over $k$ is a twist of the $k$-variety $\mathbb{P}^{n-1}_k$ for some $n \geq 1$.

Example 4.5.8. The 1-dimensional Severi–Brauer varieties over $k$ are exactly the nice genus 0 curves over $k$.

Because Severi–Brauer varieties are twists, it is natural (but not necessary) to use cohomology to study them. First, $\text{Aut} \mathbb{P}^{n-1}_k = \text{PGL}_n(k_s)$, which is also the automorphism group of the matrix algebra $M_n(k_s)$. Applying Theorem 4.5.2 and recalling material from Section 1.5.5, we get

\[
\begin{array}{ccc}
\{(n-1)\text{-dimensional Severi–Brauer varieties}/k\} & \longrightarrow & \text{Br } k \\
\downarrow & & \downarrow \\
\{n^2\text{-dimensional Azumaya } k\text{-algebras}\} & \leftarrow & \text{H}^1(\mathfrak{G}_k, \text{PGL}_n(k_s))
\end{array}
\]

Remark 4.5.9. One can show also that if $X$ is a $k$-variety such that $X_k \simeq \mathbb{P}^{n-1}_k$, then $X_{k_s} \simeq \mathbb{P}^{n-1}_{k_s}$ already; i.e., $X$ is a Severi–Brauer variety. This can be viewed as a consequence of the triviality of the fppf cohomology set $\text{H}^1(k_s, \text{PGL}_n)$ (cf. Remark 6.6.3 and Theorem 6.4.6(iii)), or it can be related to the fact that an Azumaya algebra over a separably closed field is split.

Proposition 4.5.10 (Châtelet). The following are equivalent for an $(n-1)$-dimensional Severi–Brauer variety $X$ over a field $k$:

(i) $X \simeq \mathbb{P}^{n-1}_k$.
(ii) $X$ is birational to $\mathbb{P}^{n-1}_k$.
(iii) $X(k) \neq \emptyset$.

Proof. 
(i)$\Rightarrow$(ii): Trivial.
(ii)$\Rightarrow$(iii): This follows from the Lang–Nishimura theorem: see Corollary 3.6.16.
(iii)$\Rightarrow$(i): Suppose that $X(k) \neq \emptyset$. Then $(X \text{ equipped with the given } k\text{-point})$ may be viewed as a twist of $(\mathbb{P}^{n-1}_k \text{ equipped with a } k\text{-point } P)$. Without loss of generality, $P = (1 : 0 : \cdots : 0)$; then the automorphisms of $(\mathbb{P}^{n-1}_k, P)$ over $k_s$ are the automorphisms of
\( \mathbb{P}^{n-1}_{k_v} \) that fix \( P \). They form a subgroup of \( \text{PGL}_n(k) \):

\[
\text{Aut}(\mathbb{P}^{n-1}_{k_v}, P) = \begin{pmatrix} * & * & \cdots & * \\ 0 & * & \cdots & * \\ \vdots & \vdots & \ddots & \vdots \\ 0 & * & \cdots & * \end{pmatrix} \text{ mod } k_v^* \cong \begin{pmatrix} 1 & * & \cdots & * \\ 0 & * & \cdots & * \\ \vdots & \vdots & \ddots & \vdots \\ 0 & * & \cdots & * \end{pmatrix}.
\]

The “forget the first row and column” map is a homomorphism from the group on the right onto \( \text{GL}_{n-1}(k_v) \), and we obtain a \( \mathfrak{G}_k \)-equivariant exact sequence

\[
0 \to (k_v)^{n-1} \to \text{Aut}(\mathbb{P}^{n-1}_{k_v}, P) \to \text{GL}_{n-1}(k_v) \to 0.
\]

The \( H^1 \) of the groups at each end are trivial, so in the middle \( H^1(\mathfrak{G}_k, \text{Aut}(\mathbb{P}^{n-1}_{k_v}, P)) \) is trivial too. Thus \( (\mathbb{P}^{n-1}_{k_v}, P) \) has no nontrivial twists. In particular, \( X \cong \mathbb{P}^{n-1}_{k_v} \). \qed

**Theorem 4.5.11 (Châtelet).** Severi–Brauer varieties over global fields satisfy the local-global principle.

**Proof.** Let \( X \) be the variety, and let \( x \) be the corresponding element of \( \text{Br } k \). Let \( n - 1 = \dim X \). By Proposition 4.5.10,

\[
X(k) \neq \emptyset \iff X \cong \mathbb{P}^{n-1}_k \iff x = 0.
\]

The variety \( X_{k_v} \) is a Severi–Brauer variety over \( k_v \) corresponding to the image \( x_v \) of \( x \) in \( \text{Br } k_v \), so we similarly have

\[
X(k_v) \neq \emptyset \iff x_v = 0.
\]

Thus the result follows from the injectivity of

\[
\text{Br } k \to \bigoplus_v \text{Br } k_v,
\]

which was mentioned in Section 1.5.9. \qed

**4.5.1.1. Rational maps between Severi–Brauer varieties.**

**Proposition 4.5.12.** Let \( X \) and \( Y \) be positive-dimensional Severi–Brauer varieties over a field \( k \). Let \( x, y \in \text{Br } k \) be the corresponding Brauer classes. Let \( f : X \to Y \) be a rational map. Let \( U \subseteq X \) be the domain of definition of \( f \). The composition

\[
\mathbb{Z} = \text{Pic } Y_{k_v} \xrightarrow{f^*} \text{Pic } U_{k_v} \xleftarrow{\sim} \text{Pic } X_{k_v} = \mathbb{Z}
\]

(in which the identifications at each end associate 1 to the ample generator \( \mathcal{O}(1) \) of the Picard group of each projective space over \( k_v \)) is multiplication by some nonnegative integer \( m \). Then \( y = mx \).
Sketch of proof. For any nice \( k \)-variety \( X \), the exact sequences

\[
0 \to \frac{\kappa(X_k)^\times}{k_s^\times} \to \text{Div} X_{k_s} \to \text{Pic} X_{k_s} \to 0
\]

\[
0 \to k_s^\times \to \kappa(X_k)^\times \to \frac{\kappa(X_k)^\times}{k_s^\times} \to 0
\]

define connecting homomorphisms

\[
H^0(\mathcal{G}_k, \text{Pic} X_{k_s}) \to H^1\left(\mathcal{G}_k, \frac{\kappa(X_k)^\times}{k_s^\times}\right) \to H^2(\mathcal{G}_k, k_s^\times)
\]

whose composition is a homomorphism \((\text{Pic} X_{k_s})^{\mathcal{G}_k} \to \text{Br} k\). Moreover, given a rational map \( X \dashrightarrow Y \), we obtain a commutative diagram

\[
\begin{array}{ccc}
(\text{Pic} Y_{k_s})^{\mathcal{G}_k} & \longrightarrow & \text{Br} k \\
\downarrow & & \downarrow \\
(\text{Pic} X_{k_s})^{\mathcal{G}_k} & \longrightarrow & \text{Br} k
\end{array}
\]

(4.5.13)

Finally, in the case where \( X \) is a positive-dimensional Severi–Brauer variety corresponding to an Azumaya algebra \( A \), we have \((\text{Pic} X_{k_s})^{\mathcal{G}_k} \simeq \mathbb{Z}\), and a computation proves a theorem of Lichtenbaum stating that the class of \( \mathcal{O}(1) \) (corresponding to \( 1 \in \mathbb{Z} \)) maps to the class of \( A \) in \( \text{Br} k \): see [GS06, 5.4.10]. Chasing elements in diagram (4.5.13) yields

\[
1 \longrightarrow y \\
m \downarrow \quad \downarrow \\
m \longrightarrow mx.
\]

\[\square\]

\[\text{Warning 4.5.14.}\] The quantity \( m \) appearing in Proposition 4.5.12 acts strangely:

- It is not directly related to the notion of degree in Definition 3.6.10.
- It is not multiplicative with respect to composition of rational maps.
- For a birational map, \( m \) need not be 1.

Example 4.5.15. If \( f : \mathbb{P}^2 \dashrightarrow \mathbb{P}^2 \) is the quadratic transformation

\[
(x : y : z) \mapsto \left(\frac{1}{x} : \frac{1}{y} : \frac{1}{z}\right) = (yz : zx : xy),
\]

then \( m = 2 \). But \( f \circ f \) is the identity, which has \( m = 1 \).

Corollary 4.5.16. Let \( X \) and \( Y \) be Severi–Brauer varieties over a field \( k \). Let \( x, y \in \text{Br} k \) be the corresponding Brauer classes. If \( X \) and \( Y \) are birational, then \( x \) and \( y \) generate the same subgroup of \( \text{Br} k \).
Remark 4.5.17. Amitsur [Am55] conjectured a converse to Corollary 4.5.16, namely, that if \( X \) and \( Y \) are Severi–Brauer varieties of the same dimension whose classes generate the same subgroup of \( \text{Br} k \), then \( X \) and \( Y \) are birational. For some partial results towards Amitsur’s conjecture, see [Roq64, Tre91].

Remark 4.5.18. Integral varieties \( X \) and \( Y \) are called stably birational if \( X \times \mathbb{P}^m \) and \( Y \times \mathbb{P}^n \) are birational for some \( m, n \geq 0 \). Even over \( \mathbb{C} \), stably birational varieties of the same dimension need not be birational [BCTSSD85]. Exercise 4.6 asks for a proof of the following weak form of Amitsur’s conjecture: if \( X \) and \( Y \) are Severi–Brauer varieties of the same dimension whose classes generate the same subgroup of \( \text{Br} k \), then \( X \) and \( Y \) are stably birational.

4.6. Restriction of scalars

(Reference: Section 7.6 of [BLR90])

Let \( L/k \) be a finite extension of fields, and let \( X \) be an \( L \)-variety. We want to construct a \( k \)-variety \( \mathcal{X} \) whose arithmetic over \( k \) mimics the arithmetic of \( X \) over \( L \). In particular, we want a bijection \( \mathcal{X}(k) \simeq X(L) \). But this condition is not enough to determine \( \mathcal{X} \) uniquely.

Definition 4.6.1. Let \( L \) be a finite extension of a field \( k \), and let \( X \) be an \( L \)-variety. The restriction of scalars (also called Weil restriction) \( \mathcal{X} = \text{Res}_{L/k}(X) \), if it exists, is a \( k \)-variety characterized by the existence of bijections \( \mathcal{X}(S) \to X(S \times_k L) = \text{Hom}_L(S \times_k L, X) \), for each \( k \)-scheme \( S \), varying functorially in \( S \).

"Functorially in \( S \)" means that if \( f : S \to T \) is a \( k \)-morphism, and \( f_L : S \times_k L \to T \times_k L \) is its base extension to \( L \), then the diagram

\[
\begin{array}{ccc}
\mathcal{X}(T) & \longrightarrow & X(T \times_k L) \\
\downarrow f & & \downarrow f_L \\
\mathcal{X}(S) & \longrightarrow & X(S \times_k L)
\end{array}
\]

commutes. In other words, the restriction of scalars, if it exists, is a \( k \)-scheme representing the functor \( S \mapsto X(S \times_k L) \).

If \( X \) is an affine \( L \)-variety, then \( \mathcal{X} := \text{Res}_{L/k} X \) exists as an affine \( k \)-variety, and can be described explicitly as follows. Write \( X = \text{Spec} L[x_1, \ldots, x_n]/(f_1, \ldots, f_m) \). Choose a basis \( e_1, \ldots, e_s \) of \( L \) over \( k \). Introduce new variables \( y_{ij} \) with \( 1 \leq i \leq n \) and \( 1 \leq j \leq s \), and substitute

\[
x_i = \sum_{j=1}^s y_{ij} e_j
\]

for all \( i \) into \( f_r \) for each \( r \), so that

\[
f_r(x_1, \ldots, x_n) = F_{r,1} e_1 + \cdots + F_{r,s} e_s
\]
where each $F_{r,\ell}$ is a polynomial in $k[y_{ij}]$. Then $\mathcal{X} = \text{Spec } k[y_{ij}]/(\{F_{r,\ell}\})$.

**Example 4.6.2.** Let $k = \mathbb{Q}$, $L = \mathbb{Q}(\sqrt{2})$, and let $X$ be the curve in $\mathbb{A}_L^2$ defined by $x_1x_2 + (5 + 7\sqrt{2}) = 0$. Substituting

$$x_1 = y_{11} + y_{12}\sqrt{2}$$

$$x_2 = y_{21} + y_{22}\sqrt{2}$$

we get

$$(y_{11}y_{21} + 2y_{12}y_{22} + 5) + (y_{11}y_{22} + y_{12}y_{21} + 7)\sqrt{2} = 0$$

so $\mathcal{X}$ is the surface in $\mathbb{A}_\mathbb{Q}^4$ defined by the system of equations

$$y_{11}y_{21} + 2y_{12}y_{22} + 5 = 0$$

$$y_{11}y_{22} + y_{12}y_{21} + 7 = 0.$$ 

The fact that $\mathcal{X}(\mathbb{Q})$ equals $X(L)$ is almost a tautology. To show more generally that $\mathcal{X}(S)$ equals $X(S_L)$ for any $k$-scheme $S$, one uses the fact that $\mathcal{O}_{S_L}(S_L) = \mathcal{O}_S(S) \otimes_k L$, which follows easily from the construction of the fiber product.

For non-affine varieties, the restriction of scalars is harder to construct, and sometimes it even fails to exist!

**Proposition 4.6.3.** Let $L/k$ be a finite extension of fields, and let $X$ be an $L$-variety. If every finite subset of $X$ is contained in some affine open subset of $X$, then $\text{Res}_{L/k} X$ exists.

**Proof.** This is a special case of Theorem 4 in [BLR90 §7.6]. The idea of the proof is to take the restriction of scalars of each affine subvariety of $X$, and then to use descent to show that they can be glued. □

**Remark 4.6.4.** To see why one must use affine open subvarieties containing finite subsets instead of just affine open subvarieties forming a covering of $X$, do Exercise 4.8

**Important Remark 4.6.5.** Any quasi-projective variety $X$ over $L$ satisfies the hypothesis of Proposition 4.6.3.

Restriction of scalars can often be used to reduce questions about varieties over a large field to questions about (higher-dimensional) varieties over smaller fields. For example, it is known [Mil72 Theorem 1] that if $L$ is a finite separable extension of a global field $k$, and $A$ is an abelian variety over $L$, then the full Birch and Swinnerton-Dyer conjecture holds for $A$ over $L$ (see Conjecture 5.7.33 and Remark 5.7.34) if and only if it holds for the abelian variety $\text{Res}_{L/k} A$ over $k$. This lets one reduce the conjecture for abelian varieties over global fields to the conjecture for abelian varieties over $\mathbb{Q}$ and $\mathbb{F}_p(t)$. 

103
REMARK 4.6.6. One can generalize the notion of restriction of scalars to $\text{Res}_{S'/S}$ where $S'$ is a finite and locally free scheme over a base scheme $S$. (Our discussion corresponds to the special case $S = \text{Spec } k$ and $S' = \text{Spec } L$.)

REMARK 4.6.7 (Greenberg transform). Let $R$ be a discrete valuation ring, with uniformizer $\pi$ and perfect residue field $k$. Let $R_n = R/\pi^n R$. For example, $R_n$ could be the ring $W_n(k)$ of length $n$ Witt vectors (see [Ser79 II.§6]). The level $n$ Greenberg functor takes a scheme $X$ locally of finite type over $R_n$ and returns a $k$-scheme $X$, called the Greenberg transform: see [BLR90 p. 276] for more details. The Greenberg transform acts very much like the restriction of scalars, but cannot be considered as a special case even of the generalized restriction of scalars in Remark 4.6.6 because $R_n$ need not be a $k$-algebra.

EXAMPLE 4.6.8 (Jet spaces). If $X$ is a finite-type scheme over a field $k$, and $A := k[[t]]/(t^{n+1})$, then $\text{Res}_{A/k} X_A$ exists as a finite-type $k$-scheme and is called the $n$th jet space of $X$ [BLR90 p. 276]. This could also be viewed as a special case of the Greenberg transform, at least when $k$ is perfect.

Exercises

4.1. (Field of moduli not a field of definition) Let $\sigma \in \text{Gal}(\mathbb{C}/\mathbb{R})$ denote complex conjugation. Let $a_0, \ldots, a_6 \in \mathbb{C}$ be such that $\sigma a_{6-j} = (-1)^{j+1}a_j$ for $0 \leq j \leq 6$. Let $f(x) = a_6x^6 + \cdots + a_0$. Assume that $f(x)$ is a separable polynomial of degree 6. Let $X$ be the smooth projective model of the affine curve $y^2 = f(x)$ over $\mathbb{C}$. Assume that the only nontrivial automorphism of $X$ is the hyperelliptic involution $\iota$, induced by the automorphism $(x, y) \mapsto (x, -y)$ of the affine curve.
(a) Prove that $X$ is isomorphic to $\sigma X$ as a $\mathbb{C}$-variety, where $\sigma$ is the nontrivial element of $\text{Gal}(\mathbb{C}/\mathbb{R})$.
(b) Prove that $X$ is not the base extension of a curve defined over $\mathbb{R}$.
(c) Prove that the hypotheses of the problem can actually be satisfied! (Hint: For a suitable choice of $a_i$, prove $\text{Aut } X = \{1_X, \iota\}$ by using that any automorphism of $X$ induces an automorphism of $X/\iota \simeq \mathbb{P}^1$ preserving the six branch points.)

4.2. (Twists of a superelliptic curve) Let $k$ be a field, and let $n$ be a positive integer such that $\text{char } k \nmid n$. Fix $f(x) \in k[x]$ such that $y^n - f(x) = 0$ defines a geometrically integral affine curve over $k$; let $X$ be its smooth projective model. Assuming that every automorphism of $X_{\overline{k}}$ fixes the rational function $x$, describe the set of twists of $X$ up to $k$-isomorphism.

4.3. (Rational points on a quadratic twist of an elliptic curve) Let $k$ be a field. Let $E$ be an elliptic curve over $k$ with equation $y^2 = x^3 + ax + b$; i.e., $E$ is the projective closure of that affine curve, and $E$ is smooth (so $\text{char } k \neq 2$). Let $d \in k^x \setminus k^{x2}$, let $L = k(\sqrt{d})$, and let $\sigma$ be the nontrivial element of $\text{Gal}(L/k)$. Let $E'$ be the elliptic curve over $k$ with equation $dy^2 = x^3 + ax + b$. Prove that $E'(k)$ is isomorphic to the group $\{ P \in E(L) : \sigma P = -P \}$. 104
4.4. Let $k$ be a field, and let $k(t)$ be the rational function field over $k$. Let $E$ be an elliptic curve over $k$ with Weierstrass equation $y^2 = x^3 + ax + b$. Let $E'$ be the elliptic curve over $k(t)$ with Weierstrass equation $(t^3 + at + b)y^2 = x^3 + ax + b$. Prove that $E'(k(t)) \simeq (\text{End } E) \oplus E[2](k)$ as abelian groups.

4.5. Let $X$ be a nice genus 0 curve over a global field $k$. Use the description of $\text{Br } k$ to prove the following:
   (a) The curve $X$ has a $k$-point if and only if $X$ has a $k_v$-point for every place $v$ of $k$.
   (b) The number of places $v$ for which $X(k_v) = \emptyset$ is finite and even.

4.6. Let $X$ and $Y$ be Severi–Brauer varieties of dimension $n - 1$ whose classes in $\text{Br } k$ generate the same subgroup. Prove that $X \times \mathbb{P}^{n-1}, X \times Y$, and $Y \times \mathbb{P}^{n-1}$ are all birational to each other. (Hint: use Proposition [4.5.10].)

4.7. Let $L/k$ be a finite Galois extension of fields, with Galois group $G$. Let $X$ be an $L$-variety. Assume that the $k$-variety $\mathcal{X} := \text{Res}_{L/k} X$ exists. Prove that $\mathcal{X}_L \simeq \prod_{\sigma \in G} \sigma X$ as $L$-varieties.

4.8. Let $X = \mathbb{P}^1_C$. Let $U = X - \{0\}$ and $V = X - \{\infty\}$ be the standard copies of $\mathbb{A}^1_C$ whose union is $X$. Prove that the union of the open subschemes $\text{Res}_{C/R} U$ and $\text{Res}_{C/R} V$ does not equal $\text{Res}_{C/R} X$.

4.9. (Inseparable restriction of scalars) Let $L = \mathbb{F}_p(t)$ and $k = \mathbb{F}_p(t^p)$. Let $X$ be the $L$-scheme $\text{Spec } L[x]/(x^p - t)$. Compute $\text{Res}_{L/k} X$. (The answer may surprise you!)
CHAPTER 5

Algebraic groups

5.1. Group schemes

(References: Vis05 §2.2, Wat79)

5.1.1. Category-theoretic definition of groups. Let pt be an empty product of sets; in other words, pt is a terminal object in the category Sets, i.e., a one-element set.

A group can be interpreted as a set $G$ equipped with maps $m: G \times G \to G$ (multiplication), $i: G \to G$ (inverse), and $e: pt \to G$ (identity) satisfying the group axioms, namely the commutativity of the following diagrams, where $1: G \to G$ is the identity on $G$:

- **Associativity:**
  \[
  \begin{array}{ccc}
  G \times G \times G & \xrightarrow{m \times 1} & G \times G \\
  \downarrow{1 \times m} & & \downarrow{m} \\
  G \times G & \xrightarrow{m} & G
  \end{array}
  \]

- **Identity (left and right):**
  \[
  \begin{array}{ccc}
  pt \times G & \xrightarrow{e \times 1} & G \times G \\
  \downarrow{m} & & \downarrow{m} \\
  G & & G
  \end{array}
  \quad \text{and} \quad
  \begin{array}{ccc}
  G \times pt & \xrightarrow{1 \times e} & G \times G \\
  \downarrow{m} & & \downarrow{m} \\
  G & & G
  \end{array}
  \]

- **Inverse (left and right):**
  \[
  \begin{array}{ccc}
  \quad G & \xrightarrow{(i,1)} & G \times G \\
  \downarrow{m} & & \downarrow{m} \\
  \quad pt & \xrightarrow{e} & G
  \end{array}
  \quad \text{and} \quad
  \begin{array}{ccc}
  G & \xrightarrow{(1,i)} & G \times G \\
  \downarrow{m} & & \downarrow{m} \\
  \quad pt & \xrightarrow{e} & G
  \end{array}
  \]

The definitions of commutativity, group homomorphism, (right or left) action of a group on a set (i.e., $G$-set), and $G$-equivariant map (i.e., morphism of $G$-sets) are category-theoretic too.

5.1.2. Group objects. Let $C$ be a category with finite products: i.e., for any $n \geq 0$ and for any objects $G_1, \ldots, G_n$ of $C$, there is an object $G$ equipped with a morphism to each $G_i$ such that any other object $H$ equipped with a morphism to each $G_i$ admits a unique
morphism to $G$ compatible with the morphisms $G \to G_i$. For $n = 0$, an empty product is the same thing as a terminal object of $\mathcal{C}$.

Then a **group object** in $\mathcal{C}$ is an object $G$ equipped with morphisms $m, i, e$ satisfying the group axioms listed in Section 5.1.1.

**Example 5.1.1.** A group object in $\textbf{Sets}$ is a group.

**Example 5.1.2.** A group object in the category of topological spaces with continuous maps is a **topological group**. (Actually, many authors require a topological group to be Hausdorff; if one wants this, one should start with the full subcategory of Hausdorff topological spaces.)

The definitions of commutative group object, homomorphism of group objects, action of a group object $G$ on an object, and $G$-equivariant morphism are defined by the same diagrams used for $\textbf{Sets}$. In particular, the group objects in $\mathcal{C}$ form their own category.

**5.1.3. Group schemes.**

**Definition 5.1.3.** A **group scheme** $G$ over a scheme $S$ is a group object in the category of $S$-schemes.

In the category of $S$-schemes, products are fiber products over $S$, and the terminal object is the $S$-scheme $S$. So, for example, a **homomorphism of group schemes** $G \to H$ over $S$ is an $S$-morphism respecting the multiplication morphisms $m_G$ and $m_H$, that is, an $S$-morphism $\phi: G \to H$ making

$$
\begin{array}{ccc}
G \times_S G & \xrightarrow{m_G} & G \\
(\phi, \phi) & \downarrow & \downarrow \phi \\
H \times_S H & \xrightarrow{m_H} & H
\end{array}
$$

commute.

**Remark 5.1.4.** If $S = \text{Spec } R$, and $G = \text{Spec } A$ is an **affine** group scheme over $R$, then $m, i, e$ correspond to $R$-algebra homomorphisms with their own names,

$$
\begin{align*}
\Delta: A &\to A \otimes_R A & \text{(comultiplication)} \\
S: A &\to A & \text{(antipode)} \\
\epsilon: A &\to R & \text{(counit)},
\end{align*}
$$

satisfying opposite axioms. Together with the $R$-algebra structure on $A$, given by the structure homomorphism $R \to A$ and multiplication $A \otimes_R A \to A$, this makes $A$ into a **commutative Hopf algebra** over $R$. In fact, the axioms defining commutative Hopf algebra are such that one obtains an equivalence of categories

$$
\{\text{affine group schemes over } R\}^{\text{opp}} \longrightarrow \{\text{commutative Hopf algebras over } R\}.
$$
A subgroup scheme of a group scheme $G$ is a group scheme $H$ that is also a closed subscheme of $G$, and for which the inclusion $H \to G$ is a homomorphism.

If $k$ is a field, a group variety over $k$ is a group object in the category of $k$-varieties.

Group varieties form a full subcategory of the category of group schemes.

5.1.4. Functor of points of a group scheme. Intuitively, to make a $k$-variety $G$ into a group scheme, one would want a morphism $G \times G \to G$ giving the set $G(k)$ the structure of a group; this is a valid description if $k$ is algebraically closed and $G$ is reduced. More generally, to describe a group law on an $S$-scheme $G$, one should use the whole functor of points instead of just $G(S)$. This leads to an equivalent definition of group scheme that is perhaps closer to geometric intuition:

Proposition 5.1.7. Let $G$ be an $S$-scheme. Equipping $G$ with the structure of a group scheme over $S$ is equivalent to equipping the set $G(T)$ with a group structure for each $S$-scheme $T$ such that for any $S$-morphism $T' \to T$, the map of sets $G(T) \to G(T')$ is a group homomorphism. Equivalently, making $G$ a group scheme over $S$ is equivalent to giving a functor $G : \text{Schemes}_S^\text{opp} \to \text{Groups}$ completing the commutative diagram

\[
\begin{array}{ccc}
\text{Schemes}_S^\text{opp} & \xrightarrow{h_G} & \text{Sets} \\
\downarrow g & & \downarrow \text{forgetful} \\
\text{Groups} & & \\
\end{array}
\]

Proof. This is just Yoneda’s lemma (Lemma 2.3.4): to give compatible multiplication maps $G(T) \times G(T) \to G(T)$ is to give an $S$-morphism $G \times G \to G$, and so on. □

Homomorphisms of group schemes, group scheme actions, and equivariant morphisms can be described similarly. For example, giving a right action of a group scheme $G$ on an $S$-scheme $X$ is equivalent to giving a collection of compatible group actions $X(T) \times G(T) \to X(T)$ (in the category of sets), one for each $S$-scheme $T$. Such an action is faithful if for every $S$-scheme $T$ and $g \in G(T)$ not equal to 1, there exists $T' \to T$ and $x \in X(T')$ such that $gx \neq x$ (here $gx$ is defined by mapping $g$ to an element of $G(T')$ before acting).

Warning 5.1.8. If $G$ acts faithfully on $X$, it does not follow that $G(T)$ acts faithfully on $X(T)$ for each $T$. A group scheme $G$ acting on a nontrivial torsor $X$ gives a counterexample. (See Definition 5.12.3)

Various properties of a group scheme are also conveniently described in terms of its functor of points. For instance, a subgroup scheme $H$ of $G$ is normal if and only if $H(T)$ is a normal subgroup of $G(T)$ for every $S$-scheme $T$. 108
5.1.5. Examples of group schemes.

1. The additive group scheme $\mathbb{G}_a$ over a ring $A$ is $A_1 = \text{Spec } A[t]$ with $m: \mathbb{G}_a \times \mathbb{G}_a \to \mathbb{G}_a$ given in coordinates by $(t_1, t_2) \mapsto t_1 + t_2$; that is, $m$ corresponds to the $A$-algebra homomorphism

$$A[t] \to A[t_1] \otimes_A A[t_2]$$

$$t \mapsto t_1 \otimes 1 + 1 \otimes t_2.$$

Similarly $i$ is given by $t \mapsto -t$, and $e$ corresponds to the ring homomorphism $A[t] \to A$ mapping $t$ to $0$.

2. The multiplicative group scheme $\mathbb{G}_m$ over $A$ is defined the same way, but using $\text{Spec } A[t, t^{-1}]$ with $m$ given in coordinates by $(t_1, t_2) \mapsto t_1 t_2$, and so on.

3. For each $n \geq 0$, the group scheme $\text{GL}_n$ over a ring $A$ is $\text{Spec } A[x_{11}, x_{12}, \ldots, x_{nn}, 1/\det]$, where $\det$ is the determinant of the $n \times n$ matrix with indeterminate entries $x_{11}, \ldots, x_{nn}$. (One defines $m$, $i$, and $e$ in the obvious way.) One has $\text{GL}_1 \cong \mathbb{G}_m$.

4. Similarly the group scheme $\text{SL}_n$ over a ring $A$ is $\text{Spec } A[x_{11}, x_{12}, \ldots, x_{nn}]/(\det - 1)$.

5. Let $U_n$ be the closed subgroup scheme of $\text{GL}_n$ such that for every scheme $S$, the set $U_n(S)$ is the set of upper triangular matrices in $\text{GL}_n(S)$ with $1$s on the diagonal.

6. When one has a group scheme over $\mathbb{Z}$, one can base extend to get a corresponding group scheme over any scheme $S$. Thus for instance, one can define $\mathbb{G}_{a,S}, \text{SL}_{n,S},$ and so on.

7. Let $G$ be a group, and let $S$ be a scheme. For each $\sigma \in G$, let $S_\sigma$ be a copy of $S$. Then $\coprod_{\sigma \in G} S_\sigma$ can be made a group scheme over $S$, by letting $m$ map $S_\sigma \times_S S_\tau$ isomorphically to $S_{\sigma \tau}$ for each $\sigma, \tau \in G$. This is called a constant group scheme.

8. An elliptic curve over a field $k$ is an example of a group scheme of finite type over $k$.

DEFINITION 5.1.9. If $G$ is a group scheme over $S$ such that $\mathcal{O}_G$ is locally free of rank $r$ as an $\mathcal{O}_S$-module, then the order of $G$ is $\#G := r$.

EXAMPLE 5.1.10. If $G_S$ is the constant group scheme over $S$ associated to a finite group $G$, then $\#G_S = \#G$.

EXAMPLE 5.1.11. If $G$ is a finite group scheme over a field $k$, then $G = \text{Spec } A$ for some finite-dimensional $k$-algebra $A$, and $\#G := \dim_k A$.

5.1.6. Kernels.

DEFINITION 5.1.12. The kernel $K$ of a homomorphism of group schemes $\phi: G \to H$ is $\phi^{-1}(e)$, where $e: S \to H$ is the identity of $H$. More explicitly, $\ker \phi$ is the $S$-group scheme $G \times_H S$, where in the fiber product $S$ is viewed as an $H$-scheme via $e$. The $m$, $i$, and $e$ for $\ker \phi$ are induced from the $m$, $i$, and $e$ of $G$ by base extension. Alternatively, one can describe
as the group scheme whose functor of points is given by \( K(T) := \ker(G(T) \to H(T)) \).

Sometimes one thinks of the kernel as the inclusion morphism from \( K \) into \( G \), instead of as a group scheme in isolation.

**Example 5.1.13.** Let \( \mathbb{G}_m \) be the multiplicative group scheme over \( \mathbb{Z} \). Let \( n \in \mathbb{Z}_{>0} \). Then we have an endomorphism \( [n] : \mathbb{G}_m \to \mathbb{G}_m \) given in coordinates by \( t \mapsto t^n \). Its kernel is called \( \mu_n \). As a scheme, \( \mu_n = \text{Spec} \mathbb{Z}[t]/(t^n - 1) \). The multiplication is given by \( (t, u) \mapsto tu \), as for \( \mathbb{G}_m \). For any commutative ring \( R \), the group \( \mu_n(R) \) is \( \{ r \in R : r^n = 1 \} \) under multiplication.

Let \( G \) be a group scheme over a field \( k \) of characteristic \( p \). Then the relative Frobenius morphism \( F_{G/k} : G \to G^{(p)} \) is a homomorphism of group schemes over \( k \). If \( G \) is the base change of a group scheme over \( \mathbb{F}_p \), then \( G^{(p)} \approx G \), so \( F_{G/k} \) can be viewed as an endomorphism of \( G \), the Frobenius endomorphism.

**Example 5.1.14.** Let \( k \) be a field of characteristic \( p \). Let \( \mathbb{G}_a \) be the additive group scheme over \( k \). The Frobenius endomorphism \( \mathbb{G}_a \to \mathbb{G}_a \) is described in coordinates by \( t \mapsto t^p \). Its kernel is called \( \alpha_p \). As a scheme, \( \alpha_p = \text{Spec} k[t]/(t^p) \). The “multiplication” is given by \( (t, u) \mapsto t + u \). We have \( \# \alpha_p = p \). For any \( k \)-algebra \( R \), the group \( \alpha_p(R) \) is \( \{ r \in R : r^p = 0 \} \) under addition.

**5.1.7. Quotients and cokernels.**

**Warning 5.1.15.** The notions of quotient and cokernel are trickier to define, because even when \( A \) is a normal subgroup scheme of a group scheme \( B \) the functor \( T \mapsto B(T)/A(T) \) might not be representable.

**Example 5.1.16.** Let \( \mathbb{G}_m \) be the multiplicative group scheme over \( \mathbb{Q} \). The squaring map \( \mathbb{G}_m \to \mathbb{G}_m \) is scheme-theoretically surjective, so it should be considered a surjective homomorphism, but it is certainly not true that every \( q \in \mathbb{G}_m(\mathbb{Q}) = \mathbb{Q}^\times \) is in the image of \( \mathbb{G}_m(\mathbb{Q}) \to \mathbb{G}_m(\mathbb{Q}) \). What is true is that each \( q \in \mathbb{G}_m(\mathbb{Q}) \) is in the image of \( \mathbb{G}_m(k) \to \mathbb{G}_m(k) \) for some finite extension \( k \supseteq \mathbb{Q} \) depending on \( q \). Similarly, we want to consider

\[
1 \to \mu_2 \to \mathbb{G}_m \to \mathbb{G}_m \to 1
\]

to be exact, even though the resulting sequence of rational points is only left exact. One can show that the functor \( T \mapsto \mathbb{G}_m(T)/\mu_2(T) \) is not representable, but the quotient group scheme \( \mathbb{G}_m/\mu_2 \) should be defined so that it is isomorphic to \( \mathbb{G}_m \).

**Important Remark 5.1.17.** Over an arbitrary base scheme, fppf base extensions play the role of the finite extension of fields \( k \supseteq \mathbb{Q} \) in Example 5.1.16.

Motivated by Example 5.1.16, we make the following definitions, in the context of fppf group schemes over \( S \) (i.e., group schemes \( G \) over \( S \) such that the structure morphism \( G \to S \) is fppf).
Definition 5.1.18. Let $B$ and $C$ be fppf group schemes over $S$. A homomorphism $B \to C$ over $S$ is **surjective** if for every $S$-scheme $T$ and element $c \in C(T)$, there is an fppf morphism $T' \to T$ such that the image of $c$ in $C(T')$ is the image of some $b \in B(T')$. Call a sequence of homomorphisms of fppf group schemes

$$A \xrightarrow{f} B \xrightarrow{g} C$$

**exact** (at $B$) if $g \circ f$ is the trivial homomorphism and the induced homomorphism $A \to \ker g$ is surjective. If $A$ is the kernel of a surjective homomorphism of fppf group schemes $B \to C$, then define the **quotient** $B/A$ to be $C$, and call $B$ an **extension** of $C$ by $A$; in this case,

$$1 \to A \to B \to C \to 1$$

is exact. More generally, the **cokernel** of a homomorphism $A \to B$ of fppf group schemes is an fppf group scheme $C$ equipped with a homomorphism $B \to C$ such that

$$A \to B \to C \to 1$$

is exact.

Warning 5.1.19. For a homomorphism of group schemes to be surjective, it is not enough that it induce a surjection on the underlying topological spaces. For example, over a field of characteristic $p$, the homomorphism from the trivial group scheme to $\mu_p$ is not surjective.

Warning 5.1.20. As in Example 5.1.16, a surjective homomorphism need not induce a surjective map on rational points, and an exact sequence of $S$-group schemes need not induce an exact sequence of their groups of $S$-points. We will see in Chapter 6 that the obstruction can be measured by cohomology.

5.2. Fppf group schemes over a field

(References: [Bor91], [PR94], [Spr98])

Let $k$ be a field. Flatness over $k$ is automatic, and $k$ is noetherian, so a $k$-scheme is fppf if and only if it is locally of finite type.

Definition 5.2.1. An **algebraic group** over a field $k$ is a group scheme of finite type over $k$.

Warning 5.2.2. Some authors require also that the group scheme be smooth over $k$.

5.2.1. Connected component.

Definition 5.2.3. The **connected component** (or identity component) $G^0$ of an fppf group scheme $G$ over a field $k$ is the connected component of $G$ containing the identity point $1$. 

111
**Proposition 5.2.4.** If \( G \) is an fppf group scheme over \( k \), then \( G^0 \) is a closed and open normal subgroup scheme of \( G \). Moreover, \( G^0 \) is of finite type (an algebraic group) and is geometrically irreducible.

**Proof.** If any two irreducible components of \( G_{\bar{k}} \) intersected, then there would be some \( \bar{k} \)-points in the intersection of two such components, and some not, contradicting the fact that the group \( G(\bar{k}) \) acts transitively by translations on \( G(\bar{k}) \). Thus irreducible components of \( G_{\bar{k}} \) are the same as connected components of \( G_{\bar{k}} \). Since \( G^0 \) has a \( k \)-point, Proposition 2.3.24 shows that \( G^0 \) is geometrically connected, and hence geometrically irreducible by the previous sentence. In a scheme locally of finite type over a field, any connected component is open and closed, and any irreducible component is of finite type, so \( G^0 \) has these properties.

The proof of Proposition 2.3.24 shows that \( G^0 \times G^0 \) is connected, so the multiplication \( m: G \times G \to G \) maps \( G^0 \times G^0 \) into the connected component containing \( m(1,1) = 1 \), which is \( G^0 \). Similarly, the inverse morphism \( i: G \to G \) restricts to a morphism \( G^0 \to G^0 \), and \( 1 \in G^0(\bar{k}) \). These make \( G^0 \) a subgroup scheme of \( G \).

The conjugation action \( G \times G \to G \) sending \( (g,h) \) to \( ghg^{-1} \) maps \( \{g\} \times G^0 \) into \( G^0 \) for every \( g \in G(\bar{k}) \), and the same holds after arbitrary field extension, so it maps \( G \times G^0 \) into \( G^0 \). In other words, \( G^0 \) is normal in \( G \). \(\square\)

Because of Proposition 5.2.4, the theory of fppf group schemes over a field \( k \) is almost the same as the theory of algebraic groups over \( k \).

**5.2.2. Quotients.**

**Theorem 5.2.5 (Existence of quotient group schemes).** If \( A \) is a closed normal subgroup scheme of an fppf group scheme \( B \) over a field \( k \), then the closed immersion \( A \to B \) fits in a uniquely determined exact sequence of fppf group schemes

\[
1 \to A \to B \to C \to 1.
\]

**Proof.** This is a special case of \([SGA 3]\) VI \( A \). One constructs \( C \) by first constructing its functor of points \( h_C \) as the fppf-sheafification (see Definition 6.3.21) of the functor \( T \mapsto B(T)/A(T) \) on \( k \)-schemes. \(\square\)

**Remark 5.2.6.** One can generalize Theorem 5.2.5 to the case where the subgroup scheme \( A \) is not normal in \( B \). Then the quotient \( C := B/A \) is not a group scheme, but only a \( k \)-scheme with a left \( B \)-action, a left homogeneous space of \( B \) with a \( k \)-point; see Remark 5.12.7 for the definition of homogeneous space.

**Proposition 5.2.7.** Let \( 1 \to A \to B \to C \to 1 \) be an exact sequence of fppf group schemes over a field \( k \). Then
(a) (Properties inherited by quotients) For any of the following properties, if $B$ has it, so does $C$: connected, reduced, finite type, smooth, étale, unramified, finite, affine.

(b) (Properties inherited by extensions) Let “blah” be a property that is stable under composition, base extension, and fpqc descent (see Table 7). If $A$ and $C$ are blah (over $k$), so is $B$.

**Proof.**

(a) Any image of a connected space is connected. For reduced, see [SGA 3, VI B 9.2(ix)]. For finite type, smooth, étale, unramified, and finite (which over a field is equivalent to quasi-finite), see [SGA 3, VI B 9.2(xii)]. For affine, see [SGA 3, VI B 11.7].

(b) The diagram

\[
\begin{array}{cccccc}
A & \xleftarrow{\text{pr}_1} & A \times B & \xrightarrow{m} & B \\
& & \downarrow & & \\
& & \text{Spec } k & \xleftarrow{\text{pr}_2} & C \\
\text{Spec } k & \xleftarrow{\text{fpqc}} & B & \xrightarrow{\text{blah}} & \text{Spec } k,
\end{array}
\]

is cartesian (for the square on the right, check on $T$-valued points). If the first vertical arrow $A \to \text{Spec } k$ is blah, then so are the second (base extension) and the third (fpqc descent). If $C \to \text{Spec } k$ is blah too, then the composition $B \to C \to \text{Spec } k$ is blah. □

**Definition 5.2.8.** Let $G$ be an algebraic group. A (finite) composition series of $G$ is a chain of subgroups

\[\{1\} = G_0 \leq G_1 \leq \cdots \leq G_n = G\]

in which $G_i$ is a closed normal subgroup scheme of $G_{i+1}$ for $0 \leq i < n$. The groups $G_{i+1}/G_i$ are called the successive quotients of the composition series.

**5.2.3. Quotients and homomorphisms.**

**Theorem 5.2.9.** Let $f : G \to H$ be a homomorphism of algebraic groups. Then $f$ factors into homomorphisms

\[G \xrightarrow{q} \frac{G}{\ker f} \xleftarrow{i} H,\]

where $q$ is the canonical quotient homomorphism, and $i$ is a closed immersion.

**Proof.** See [Gro62, page 212-17, Corollary 7.4]. □

**Corollary 5.2.10.** Let $f : G \to H$ be a homomorphism of algebraic groups. Then $\ker f$ is the trivial group scheme if and only if $f$ is a closed immersion.
Proof. If \( \ker f \) is trivial, then \( f \) equals the closed immersion \( i \) in Theorem 5.2.9. Conversely, if \( f \) is a closed immersion, then \( f: G(S) \to H(S) \) is injective for every \( k \)-scheme \( S \), so \( \ker f \) is trivial. \qed

Definition 5.2.11. A homomorphism satisfying the equivalent conditions of Corollary 5.2.10 is called an embedding of algebraic groups.

Theorem 5.2.12. The category of commutative algebraic groups over a field \( k \) (a full subcategory of the category of group schemes over \( k \)) is an abelian category.

Proof. This is a consequence of Theorem 5.2.9; see [SGA 3], VI A 5.4, Théorème. \qed

5.2.4. Center, centralizer, and normalizer. Let \( k \) be a field. Let \( H \) be a subgroup scheme of an fppf group scheme \( G \) over \( k \). Let \( S \) be a \( k \)-scheme. Let \( g' \in G(T) \), we interpret \( gg' \in G(T) \) by mapping \( g \) into \( G(T) \) before multiplying. Say that \( g \) centralizes \( H \) if for every \( S \)-scheme \( T \) and every \( h \in H(T) \), the identity \( gh = hg \) holds in \( G(T) \). Say that \( g \) normalizes \( H \) if for every \( S \)-scheme \( T \) and every \( h \in H(T) \), we have \( ghg^{-1} \in H(T) \). Let \( C_G(H) \) be the functor sending a \( k \)-scheme \( S \) to the set of \( g \in G(S) \) that centralize \( H \). Let \( N_G(H) \) be the functor sending a \( k \)-scheme \( S \) to the set of \( g \in G(S) \) that centralize \( H \).

Theorem 5.2.13. The functors \( C_G(H) \) and \( N_G(H) \) are represented by closed subgroup schemes of \( G \), called the centralizer of \( H \) in \( G \) and the normalizer of \( H \) in \( G \).

Proof. See [SGA 3], VIII.6.7. \qed

The center of \( G \) is the closed subgroup scheme \( Z := C_G(G) \).

Warning 5.2.14. The group \( Z(k) \) might be smaller than the center of \( G(k) \): see Exercise 5.1.

Remark 5.2.15. Because centralizers, normalizers, and centers are defined functorially, their formation automatically respects base field extension.

5.2.5. Smoothness.

Theorem 5.2.16. For an fppf group scheme \( G \) over a field \( k \), the following are equivalent:

(i) \( G \) is smooth over \( k \).

(ii) \( G \) is geometrically reduced.

(iii) The local ring of \( G_\overline{k} \) at the identity is reduced.

(iv) Either \( \text{char } k = 0 \), or \( \text{char } k = p > 0 \) and \( F_{G/k}: G \to G^{(p)} \) is surjective.
Proof. None of the conditions are affected by base field extension, so assume that $k$ is algebraically closed.

(i)⇒(ii): Smooth implies reduced by Proposition 3.5.50[(i)].

(ii)⇒(iii): Trivial.

(iii)⇒(ii): Translating by elements of $G(k)$ shows that the local ring of $G$ at each $k$-point is reduced. For algebraically closed $k$, this implies that $G$ is reduced.

(ii)⇒(i): By Proposition 3.5.63, the smooth locus is open and dense. In particular, $G$ is smooth at some $k$-point. By translation, $G$ is smooth at every $k$-point. Since $k$ is algebraically closed, the only open subscheme of $G$ containing $G(k)$ is $G$ itself.

(i)⇔(iv): See [SGA 3i VII 8.3.1]. ☐

Remark 5.2.17. In (iv), one could replace the relative $p$-power Frobenius morphism by the relative $q$-power Frobenius morphism for any power $q$ of $p$.

Corollary 5.2.18 (Cartier). Every fpqc group scheme over a field of characteristic 0 is smooth.

More generally:

Proposition 5.2.19 (cf. [SGA 3i VII 8.3]). Any fpqc group scheme $G$ over a field $k$ is an extension of a smooth group scheme by a finite group scheme.

Proof. Because of (iii) in Theorem 5.2.16, we may replace $G$ by its connected component to assume that $G$ is of finite type. If char $k = 0$, then $G$ is already smooth. Otherwise, let $F_G$ be the absolute Frobenius morphism. By noetherianity, the descending chain of scheme-theoretic images $F^n_G(G)$ must stabilize. In other words, we may fix $n$ such that $F_G: F^n_G(G) \rightarrow F^n_G(G)$ is surjective. The relative $p^n$-power Frobenius morphism $F$ is isomorphic to $(F_G)^n$ as a morphism of abstract schemes without $k$-structure. Thus $F(G)$ satisfies Theorem 5.2.16[(iv)], so $F(G)$ is smooth. On the other hand, ker $F$ is 0-dimensional and of finite type, hence finite. Therefore

$$1 \rightarrow \text{ker } F \rightarrow G \xrightarrow{F} F(G) \rightarrow 1$$

is an extension of the required type. ☐

5.2.6. Quasi-projectivity.

Theorem 5.2.20. Every algebraic group over a field $k$ is quasi-projective.

Proof. Chow proved that smooth algebraic groups (and even their homogeneous spaces) are quasi-projective [Cho57]. This can be extended to arbitrary algebraic groups $G$ by using Proposition 5.2.19 see [Con02 Corollary 1.2]. ☐

Because of Theorem 5.2.20, fpqc descent involving algebraic groups is automatically effective.
5.3. Affine algebraic groups

An algebraic group whose underlying scheme is affine is also called a linear algebraic group, because of the following.

**Theorem 5.3.1.** An algebraic group $G$ is affine if and only if it embeds in $GL_n$ for some $n \geq 0$.

**Proof.** Since $GL_n$ itself is affine, any closed subgroup of $GL_n$ is affine.

Conversely, suppose that $G$ is affine, say $G = \text{Spec } A$. Let $A^*$ be the space of $k$-linear functionals $A \to k$. Below, fiber products and tensor products are over $k$. For any $k$-vector space $V$ and $k$-algebra $R$, let $V_R = V \otimes R$. The proof will proceed in three steps.

1. **Find a finite-type affine $k$-scheme $X = \text{Spec } B$ with a faithful right $G$-action.** Let $X$ be $G$ with the right translation action. For later use, note that we have the translation action of $G(k)$ on $A$ and $B$, and the induced action on $A^*$.

2. **Show that each $b \in B$ is contained in a finite-dimensional $G$-invariant subspace $V \subseteq B$; here “$G$-invariant” means that for each $k$-algebra $R$, the $G(R)$-action on $B_R$ preserves $V_R$.**

   The action morphism $X \times G \to X$ corresponds to a homomorphism $B \to A \otimes B$, which induces $A^* \otimes B \to B$. Let $V$ be the image of the composition

   
   $\left(5.3.2\right) \quad A^* \overset{\otimes b}{\longrightarrow} A^* \otimes B \longrightarrow B.$

   Let each $g \in G(k)$ act as $g \otimes 1$ on $A \otimes B$ and $A^* \otimes B$. The associative axiom for the $G$-action on $X$ shows that $B \to A \otimes B$ is $G(k)$-equivariant, so the maps in (5.3.2) are $G(k)$-equivariant. Thus $V$ is $G(k)$-invariant. The construction of $V$ respects base change to any $k$-algebra $R$, and the same argument shows that $V_R$ is $G(R)$-invariant.

   The identity in $G(k)$ corresponds to a $k$-algebra homomorphism $A \to k$, and may be viewed as an element of $A^*$. It is mapped by (5.3.2) to $b$. Thus $b \in V$.

   Concretely, if $B \to A \otimes B$ maps $b$ to $\sum a_i \otimes b_i$, where the $a_i$ are chosen to be $k$-independent, then $V$ is the $k$-span of the $b_i$, so $V$ is finite-dimensional.

3. **Find a finite-dimensional subspace $W \subseteq B$ such that $G(R)$ acts faithfully on $W_R$ for all $R$.**

   Let $B_0$ be a finite set of generators for $B$ as a $k$-algebra. For each $b \in B_0$, construct a $V = V_b$ as in Step 2, and let $W$ be their sum. If $g \in G(R)$ acts trivially on $W_R$, then $g$ acts trivially on $B_0$ and on the $R$-algebra $B_R$ it generates, but $G$ acts faithfully on $X$, so $g = 1$.

   Yoneda’s lemma now produces a homomorphism $G \to GL_{\dim W}$. By Corollary 5.2.10, it is an embedding.

**Remark 5.3.3.** It is not known whether affine finite-type group schemes over $k[\epsilon]/(\epsilon^2)$ embed in $GL_n$ over that ring.
5.4. Unipotent groups

5.4.1. Powers of the additive group. Algebraic groups isomorphic to $G_n^a := (G_a)^n$ for some $n \in \mathbb{N}$ are sometimes called vector groups or vectorial groups.

**Proposition 5.4.1.** If $k$ is a field of characteristic 0, then $G_n^a$ as an algebraic group has no nontrivial twists.

**Proof.** An endomorphism of $G_a$ is a polynomial map $t \mapsto f(t)$ where $f \in k[t]$ satisfies $f(t + u) = f(t) + f(u)$ in $k[t,u]$. Since $\text{char } k = 0$, the binomial theorem shows that the only such $f$ are the homogeneous linear polynomials. In other words, $\text{End } G_a = k$. Similarly, $\text{End } G_{a,k} = k$. Thus $\text{End } G_{a,k} = M_n(k)$, and $\text{Aut } G_{a,k} = (M_n(k))^\times = GL_n(k)$. Finally, $H^1(\mathfrak{g}_k, GL_n(k)) = 0$ by Remark 1.3.16. □

**Remark 5.4.2.** A more difficult argument shows that Proposition 5.4.1 holds also for fields of characteristic $p > 0$. This follows from [KMT74, Theorem 1.5.1, proof of Lemma 2.1.1].

**Warning 5.4.3.** There exists an inseparable extension of fields $L/k$ and an algebraic group $G \not\simeq G_a$ over $k$ such that $G_L \simeq G_{a,L}$. See Exercise 5.4 and [Rus70]. More generally, Section 2.6 of [KMT74] classifies, over any field $k$, all algebraic groups over $k$ that become isomorphic to $G_a^a$ after base extension to $k$.

5.4.2. Unipotent elements.

**Definition 5.4.4.** Let $k$ be a field. An element $u$ of $\text{GL}_n(k)$ is called unipotent if it satisfies one of the following equivalent conditions:

- The eigenvalues of $u$ are all 1.
- One has $(u - 1)^n = 0$.
- The element $u$ is conjugate in $\text{GL}_n(k)$ to a matrix in $U_n(k)$.

More generally, if $G$ is an affine algebraic group, an element $u \in G(\overline{k})$ is called unipotent if for every $n$ and every homomorphism $G_{\overline{k}} \to (\text{GL}_n)_{\overline{k}}$, the image of $u$ in $\text{GL}_n(\overline{k})$ is unipotent.

**Remark 5.4.5.** To check that an element $u \in G(\overline{k})$ is unipotent, it suffices to check that its image under any one embedding $G_{\overline{k}} \hookrightarrow (\text{GL}_n)_{\overline{k}}$ is unipotent: this follows from the “multiplicative Jordan decomposition”: see Theorem 2.4.8 and Corollary 2.4.9 of [Spr98].

5.4.3. Unipotent groups.

**Definition 5.4.6.** Let $G$ be an algebraic group over $k$. Then $G$ is called unipotent if $G_{\overline{k}}$ admits a composition series in which each successive quotient is isomorphic to a closed subgroup of $G_{a,\overline{k}}$.

**Examples 5.4.7.**
(i) Any power of $G_a$ is unipotent.
(ii) For each $n \geq 0$, the algebraic group $U_n$ in Section 5.1.5 is unipotent.
(iii) If $\text{char } k = p > 0$, then the constant group scheme $\mathbb{Z}/p\mathbb{Z}$ is unipotent.
(iv) If $\text{char } k = p > 0$, then $\alpha_p$ is unipotent.
(v) Suppose that $\text{char } k = p$. For $n \geq 0$, there is a connected algebraic group (even a ring scheme) $W_n$ over $\mathbb{F}_p$ such that $W_n(A)$ is the additive group of length-$n$ Witt vectors with coordinates in $A$ for each $\mathbb{F}_p$-algebra $A$: see [Ser79, p. 44]. It is unipotent by induction on $n$: there is a surjective homomorphism $W_{n+1} \to W_n$ with kernel isomorphic to $G_a$ (not surprising, given that there is a surjective homomorphism $\mathbb{Z}/p^{n+1}\mathbb{Z} \to \mathbb{Z}/p^n\mathbb{Z}$ with kernel isomorphic to $\mathbb{F}_p$ as an abelian group).

Theorem 5.4.8 (Characterizations of unipotent groups). The following three conditions are equivalent for an algebraic group $G$ over a field $k$:

(i) The group $G$ is unipotent.
(ii) There is an embedding of $G$ in $U_n$ for some $n \geq 0$.
(iii) The group $G$ admits a composition series (over $k$) such that
    (a) if $\text{char } k = 0$, then each successive quotient is $G_a$, and
    (b) if $\text{char } k = p$, then each successive quotient is one of $\alpha_p$, $G_a$, or a twist of $(\mathbb{Z}/p\mathbb{Z})^n$ for some $n \geq 1$.

These conditions imply

(iv) Every element of $G(\bar{k})$ is unipotent in the sense of Definition 5.4.4

If $G$ is smooth, then all four conditions are equivalent.

Proof.

(i)$\iff$(ii)$\iff$(iii): See [SGA 3II, XVII, Théorème 3.5(i,ii,v)]. Stronger statements about the composition series are available in [SGA 3II, XVII, Théorème 3.5(iii,iv)]. A standard specialization argument [SGA 3II, XVII, Proposition 1.2] shows that unipotence is unchanged by extension of the ground field, so we now know that (iii) and (iv) are unchanged as well.

(iii)$\implies$(iv): If $g \in G(\bar{k}) \leq U_n(\bar{k})$, then $g$ is unipotent by Remark 5.4.5.

(iv)$\implies$(iii) for smooth $G$: Since both (ii) and (iii) are unchanged by base extension from $k$ to $\bar{k}$, we may assume that $k$ is algebraically closed. Now see [Spr98, Proposition 2.4.12] (which applies only to smooth algebraic groups over an algebraically closed field).

Warning 5.4.9. Condition (iv) does not necessarily imply the others if $G$ is not smooth. For example, suppose that $G$ is $\mathbb{Q}_p$ over a field $k$ of characteristic $p > 0$. Then $G(\bar{k}) = \{1\}$, so (iv) holds. But $G$ is a group scheme of prime order, so $G$ is simple, and therefore $G$ violates (iii).

Proposition 5.4.10. If $\text{char } k = 0$ and $G$ is a commutative unipotent group over $k$, then $G \simeq G_a^n$ for some $n \geq 0$.  

118
**Sketch of proof.** First of all, $G$ must be connected, since otherwise it would have a nontrivial finite quotient embedding in some $\text{GL}_n$, and the elements of the image over $\overline{k}$ would not be unipotent.

Let $\text{Lie} G$ be the power of $G_a$ corresponding to the tangent space of $G$ at the origin. For a unipotent group $G \leq U_n$, the “exponential map” gives an isomorphism $\text{Lie} G \to G$ of varieties, the inverse being given by

$$1 + u \mapsto \log(1 + u) := u - \frac{u^2}{2} + \frac{u^3}{3} - \cdots,$$

which is a finite series for any nilpotent matrix $u$. If $G$ is also commutative, then the exponential map and its inverse are also homomorphisms of group schemes. □

**Warning 5.4.11.** The hypothesis “commutative” in Proposition 5.4.10 is necessary: consider $U_3$.

**Warning 5.4.12.** The hypothesis “$\text{char } k = 0$” in Proposition 5.4.10 is necessary too. For example, the constant group scheme $\mathbb{Z}/p\mathbb{Z}$ over $\mathbb{F}_p$ is a counterexample: it embeds in $G_a \cong U_2$, so it is unipotent. One can also give a connected counterexample: the underlying variety of the Witt group scheme $W_n$ is $\mathbb{A}^n$, but if $n \geq 2$, then $W_n$ is not isomorphic to $G_a^n$ since the group $W_n(\mathbb{F}_p) \cong \mathbb{Z}/p^n\mathbb{Z}$ is not killed by $p$.

Trying to classify all unipotent groups up to isomorphism is like trying to classify finite $p$-groups: hopeless.

### 5.5. Tori

(Reference: [Spr98, §3.2])

#### 5.5.1. Homomorphisms between powers of the multiplicative group.

**Lemma 5.5.1.** Consider the multiplicative group scheme $G_m = \text{Spec } k[t, t^{-1}]$ over a field $k$. We have

$$\text{End } G_m \cong \mathbb{Z}, \quad \text{Hom}(G_m^n, G_m^p) \cong M_{p \times n}(\mathbb{Z}), \quad \text{Aut } G_m^n \cong \text{GL}_n(\mathbb{Z}),$$

computed in the category of $k$-group schemes.

**Proof.** An endomorphism of $G_m$ is given by $t \mapsto f(t)$ where $f \in k[t, t^{-1}]^\times$ satisfies $f(tu) = f(t)f(u)$ in $k[t, t^{-1}, u, u^{-1}]$ (respecting the comultiplications amounts to this identity). Elements of $k[t, t^{-1}]^\times$ are monomials, and the only ones satisfying $f(tu) = f(t)f(u)$ are $f(t) = t^n$ for some $n \in \mathbb{Z}$. Thus $\text{End } G_m \cong \mathbb{Z}$. The other two claims follow from this: in particular, the unit group of $M_n(\mathbb{Z})$ is $\text{GL}_n(\mathbb{Z})$. □
5.5.2. Tori.

**Definition 5.5.2.** Let $k$ be a field. A torus over $k$ is a twist of $\mathbb{G}_m^n$ (as a group scheme) for some $n \in \mathbb{N}$. It is called a split torus if it is actually isomorphic to $\mathbb{G}_m^n$.

**Example 5.5.3.** Let $T$ be the affine variety $x^2 + 2y^2 = 1$ in $\mathbb{A}_\mathbb{Q}^2$. We secretly think of a point $(x, y)$ on $T$ as representing $x + y\sqrt{-2}$ and hence define

$$m : T \times T \to T$$

$$(x_1, y_1), (x_2, y_2) \mapsto (x_1x_2 - 2y_1y_2, x_1y_2 + y_1x_2).$$

Then one can show that $T$ is a non-split 1-dimensional torus over $\mathbb{Q}$.

**Example 5.5.4.** If $L/k$ is a finite separable extension of fields and $T$ is a torus over $L$, then the restriction of scalars $\text{Res}_{L/k} T$ is a torus over $k$.

**Example 5.5.5.** If $L/k$ is a finite separable extension of fields, then the norm homomorphism $L^\times \to k^\times$ is the map on $k$-points of a homomorphism of tori $\text{Res}_{L/k} \mathbb{G}_m \to \mathbb{G}_m$. The kernel of $N$ is a torus $\text{Res}^1_{L/k} \mathbb{G}_m$ of dimension $[L : k] - 1$ over $k$. For example, $\text{Res}^1_{\mathbb{Q}(\sqrt{-2})/\mathbb{Q}} \mathbb{G}_m$ is the torus $T$ in Example 5.5.3.

5.5.3. Character groups.

**Definition 5.5.6.** The character group of a $k$-torus $T$ is the $\mathbb{G}_k$-module $X(T) := \text{Hom}_{k_s}\text{-group schemes}(T_{k_s}, \mathbb{G}_m^{k_s})$.

If $T$ is an $n$-dimensional torus, then Lemma 5.5.1 implies that $X(T)$ stripped of its $\mathbb{G}_k$-action is a free abelian group of rank $n$.

5.5.4. Classification of tori.

**Theorem 5.5.7.** The functor

$$\{\text{tori}/k\} \leftrightarrow \{\mathcal{G}_k\text{-modules that are free of finite rank over } \mathbb{Z}\}^{\text{opp}}$$

$T \mapsto X(T)$

is an equivalence of categories.

**Proof.** If $k = k_s$, so that the $\mathcal{G}_k$-action is irrelevant, then the result follows from Lemma 5.5.1. For arbitrary $k$, equipping a finite-rank free $\mathbb{Z}$-module with a $\mathcal{G}_k$-action corresponds to equipping a corresponding torus over $k$ with a descent datum as in Proposition 4.4.4(i), since $\mathcal{G}_k$ acts trivially on $\text{Aut} \mathbb{G}_m^{k_s} \simeq \text{GL}_n(\mathbb{Z})$, so the result for $k$ follows from the result from $k_s$. (Strictly speaking, Proposition 4.4.4(i) is for a finite Galois extension, so it would better to proceed as in the proof of Theorem 4.5.2 by showing that $k$-tori that
split over a fixed finite Galois extension $k'$ are classified by $\text{Gal}(k'/k)$-modules that are free of finite rank, and then taking a direct limit.

\[
\square
\]

REMARK 5.5.8. Here is another way of thinking about Theorem 5.5.7. Theorem 4.5.2 gives a bijection

\[
\{\text{n-dimensional tori over } k\} = \{\text{twists of } \mathbb{G}_m^n\}
\]

\[
= H^1(\mathfrak{G}_k, \text{Aut } \mathbb{G}_m^n \otimes_k)
\]

\[
= H^1(\mathfrak{G}_k, \text{GL}_n(\mathbb{Z})) \quad \text{(where } \mathfrak{G}_k \text{ acts trivially on } \text{GL}_n(\mathbb{Z}))
\]

\[
= \text{Hom}_{\text{conts}}(\mathfrak{G}_k, \text{GL}_n(\mathbb{Z}))/\text{conjugacy}
\]

\[
= \{\mathfrak{G}_k\text{-modules that are free of rank } n \text{ over } \mathbb{Z}\},
\]

where each set is really a set of isomorphism classes.

5.5.5. Rationality. Whether a given $n$-dimensional torus $T$ is $k$-rational (i.e., birational to projective space over $k$) is a subtle question. By enumerating the possibilities for the action of $\mathfrak{G}_k$ on the character group, Voskresenskii proved that if $n \leq 2$, then $T$ is $k$-rational [Vos67]. On the other hand, Chevalley showed that there is a 3-dimensional torus over $\mathbb{Q}_p$ that is not $\mathbb{Q}_p$-rational, namely $\text{Res}^{1}_{K/\mathbb{Q}_p} \mathbb{G}_m$ for any Galois extension $K/\mathbb{Q}_p$ with $\text{Gal}(K/\mathbb{Q}_p) \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ [Che54, §5].

5.5.6. Groups of multiplicative type. The additive category of tori is not an abelian category because, for instance, the squaring homomorphism $\mathbb{G}_m \to \mathbb{G}_m$ is an epimorphism that is not a cokernel of any homomorphism $T \to \mathbb{G}_m$. This motivates enlarging the category slightly.

Definition 5.5.9. A group of multiplicative type over $k$ is an algebraic group $G$ that after base extension to $k_s$ is isomorphic to a product of groups each isomorphic to either $\mathbb{G}_m$ or $\mu_n$ for some $n$. (Some authors extend the notion also to group schemes that are not of finite type.)

Groups of multiplicative type do form an abelian category; see [SGA 3 II] IX, Corollaire 2.8 for a generalization. Moreover, one can define the character group $X(G)$ as for tori, and there is a generalization of the classification theorem (Theorem 5.5.7):

Theorem 5.5.10. The functor

\[
\text{\{groups of multiplicative type over } k\} \leftrightarrow \{\mathfrak{G}_k\text{-modules that are finitely generated as } \mathbb{Z}\text{-modules}\}^{\text{opp}}
\]

\[
G \quad \mapsto \quad X(G)
\]

is an equivalence of abelian categories.

Proof. See [SGA 3 II] X, Proposition 1.4].
Corollary 5.5.11. Each group \( G \) of multiplicative type contains a unique maximal torus \( T \) of the same dimension.

Proof. Theorem 5.5.10 translates this into a statement about character groups. The torus \( T \) is the one for which \( X(T) = X(G)/X(G)_{\text{tors}} \).

Over a separably closed field, groups of multiplicative type are exactly the algebraic groups that for some \( n \) embed into the torus in \( \text{GL}_n \) consisting of diagonal matrices.

5.5.7. Maximal tori. Every algebraic group \( G \) contains a maximal torus \( T \) (usually not normal in \( G \)); moreover, any such \( T \) remains maximal after base field extension. Call \( G \) split if \( G \) contains a split maximal torus.

5.6. Semisimple and reductive algebraic groups

(Reference: \[Kne67\])

5.6.1. Radical and unipotent radical.

Definition 5.6.1. The commutator subgroup \([G, G]\) of an algebraic group is the intersection of all algebraic subgroups containing the (scheme-theoretic) image of the morphism \( G \times G \to G \) sending \( g, h \in G(T) \) to \( ghg^{-1}h^{-1} \in G(T) \) for each \( k \)-scheme \( T \).

Definition 5.6.2. Let \( G \) be a smooth affine algebraic group. The derived series of \( G \) is the sequence of algebraic subgroups

\[
G = G^0 \triangleright G^1 \triangleright G^2 \triangleright \cdots ,
\]
each normal in the preceding one, defined by \( G^0 := G \) and \( G^{i+1} := [G^i, G^i] \) for \( i \geq 0 \). Call \( G \) solvable if \( G^n \) is trivial for some \( n \). (It turns out that this condition is equivalent to solvability of the abstract group \( G(K) \) for any algebraically closed field \( K \) containing \( k \) \[SGA 3\] VI, B 8.3(i)⇔(iii)].)

Let \( G \) be a smooth affine algebraic group. One can show that \( G \) contains a unique maximal smooth connected solvable normal subgroup \( \mathcal{R}(G) \), called the radical of \( G \). Also, \( G \) contains a unique maximal smooth connected unipotent normal subgroup \( \mathcal{R}_u(G) \), called the unipotent radical of \( G \).

Remark 5.6.3 (Radicals under field extension). For any field extension \( L \supseteq k \), by definition \( \mathcal{R}(G)_L \subseteq \mathcal{R}(G_L) \). If \( L \) is a separable algebraic extension of \( k \), then descent theory shows that equality holds. On the other hand, equality sometimes fails if \( L \) is inseparable over \( k \). Analogous statements hold for the unipotent radical \( \mathcal{R}_u(G) \).
5.6.2. Semisimple and reductive groups.

**Definition 5.6.4.** Let $G$ be a smooth affine algebraic group over a field $k$. Call $G$ semisimple if $\mathcal{R}(G_k) = \{1\}$. Call $G$ reductive if $\mathcal{R}_u(G_k) = \{1\}$.

**Warning 5.6.5.** Many authors also require a semisimple or reductive group to be connected.

**Warning 5.6.6.** Definition 5.6.4 uses the geometric radicals, i.e., the radical or unipotent radical of $G_k$ instead of $G$. Remark 5.6.3 shows that this makes no difference if $k$ is perfect. But if $k$ is imperfect, it matters: see Section 5.9.3.

By Theorem 5.4.8, smooth connected unipotent groups are solvable, so the unipotent radical is contained in the radical. In particular, semisimple groups are reductive.

**Example 5.6.7.** The algebraic group $\text{SL}_n$ is semisimple.

**Example 5.6.8.** The algebraic group $\text{GL}_n$ is reductive but not semisimple. Its radical is a copy of $\mathbb{G}_m$, consisting of the scalar multiples of the identity.

**Remark 5.6.9.** Although $\text{GL}_n$ contains nontrivial smooth connected unipotent subgroups (e.g., $U_n$), they are not normal. Similarly, $\text{SL}_n$ contains nontrivial smooth connected solvable subgroups (e.g., the torus consisting of diagonal matrices of determinant 1), but they are not normal.

5.6.3. Center of a reductive group.

**Theorem 5.6.10.** The center of a connected reductive group is a group of multiplicative type.

**Sketch of proof.** Let $G$ be a connected reductive group over $k$. For any maximal torus $T \leq G$, we have $C_G(T) = T$ [SGA 3 III, XIX, 2.8]. The center $Z$ of $G$ is a closed subgroup of $C_G(T) = T$, so $Z$ is of multiplicative type. □

**Corollary 5.6.11.** The center of a connected semisimple group is a finite group of multiplicative type.

**Proof.** Let $G$ be a connected semisimple group. Let $Z$ be its center. By Theorem 5.6.10, $Z$ is a group of multiplicative type. Let $T$ be the maximal torus in $Z$ given by Corollary 5.5.11. Since $T \subseteq Z$, the group $T$ is normal in $G$, so $T \subseteq \mathcal{R}(G) = \{1\}$, since $G$ is semisimple. Hence $T = \{1\}$. Now $\dim Z = \dim T = 0$, so $Z$ is finite. □

**Example 5.6.12.** The center of the reductive group $\text{GL}_n$ is $\mathbb{G}_m$.

**Example 5.6.13.** The center of the semisimple group $\text{SL}_n$ is $\mu_n$. 

123
5.6.4. **Isogenies.** An isogeny between connected algebraic groups is a surjective homomorphism $G \to H$ whose kernel is finite. If the kernel of an isogeny is (scheme-theoretically) contained in the center of $G$, then it is called a central isogeny, and $G$ is called a central cover of $H$.

**Example 5.6.14.** Let $n \geq 1$. The inclusion $SL_n \hookrightarrow GL_n$ is not surjective, so it is not an isogeny. The projection $GL_n \to PGL_n$ has a kernel that is not finite, so it is not an isogeny. But their composition $SL_n \to PGL_n$ is a central isogeny with kernel $\mu_n$.

**Proposition 5.6.15.** Every isogeny whose kernel is étale is central. In particular, every isogeny over a field of characteristic 0 is central.

**Proof.** Let $f: G \to H$ be an isogeny with étale kernel $K$. We may assume that $k$ is algebraically closed, so $K$ consists of a finite disjoint union of points (Proposition [3.5.35](#)). The conjugation action of $G$ on $K$ defines a homomorphism from $G$ to a finite group $\text{Aut} K$, but $G$ is connected, so this homomorphism must be trivial. In other words, $K$ is contained in the center of $G$.

**Example 5.6.16.** If $G$ is a smooth connected algebraic group over a field $k$ of positive characteristic $p$, then the relative Frobenius morphism $F_{G/k}: G \to G^{(p)}$ is an isogeny, but not necessarily a central isogeny.

5.6.5. **Simply connected and adjoint groups.** Call a central cover $G' \xrightarrow{f} G$ trivial if $f$ is an isomorphism.

**Definition 5.6.17.** A connected semisimple group $G$ is called simply connected if $G$ has no nontrivial central cover.

**Warning 5.6.18.** Let $G$ be a connected semisimple group over a separably closed field $k$. If $\text{char } k = 0$, then $G$ is simply connected in the sense of Definition [5.6.17](#) if and only if $G$ is algebraically simply connected in the sense of Definition [3.5.45](#). But if $\text{char } k = p > 0$, the notion of simply connected is more restrictive; for example, $\text{PGL}_p$ is algebraically simply connected but not simply connected: it has no nontrivial finite étale cover, but $\text{SL}_p \to \text{PGL}_p$ is a nontrivial central cover with kernel $\mu_p$.

**Proposition 5.6.19.** Let $G$ be a connected semisimple group. Then the following are equivalent:

(i) The group $G$ is not a nontrivial central cover of any other group $G'$.

(ii) The center $Z$ of $G$ is trivial.

**Proof.** If $G \xrightarrow{f} G'$ is a nontrivial central cover, then $\{1\} \neq \ker f \subseteq Z$, so $Z$ is nontrivial. Conversely, if $Z$ is nontrivial, then $G \to G/Z$ is a nontrivial central cover. □
**Definition 5.6.20.** A connected semisimple group $G$ is called **adjoint** if it satisfies the conditions of Proposition 5.6.19.

**Proposition 5.6.21.** Let $G$ be a connected semisimple group.

(a) Among all connected semisimple groups that centrally cover $G$, there is a maximal one $\tilde{G}$ that centrally covers all others. This $\tilde{G}$ is unique up to isomorphism (as a group equipped with a central isogeny to $G$), and is simply connected.

(b) Among all connected semisimple groups that $G$ centrally covers, there is a minimal one $G^{\text{ad}}$ that is centrally covered by all others. This $G^{\text{ad}}$ is unique up to isomorphism (as a group equipped with a central isogeny from $G$ to it), and is adjoint. If $Z$ is the center of $G$, then $G^{\text{ad}} \simeq G/Z$.

The formation of $\tilde{G}$ and $G^{\text{ad}}$ commutes with base field extension.

**Proof.**

(a) See [CGP10, Corollary A.4.11].

(b) By Corollary 5.6.11, $Z$ is a finite group of multiplicative type, so the connected semisimple groups centrally covered by $G$ are the quotients $G/Z'$ for $Z' \leq Z$. In particular, $G/Z$ is the minimal such quotient. By [SGA 3, III, XXII, Proposition 4.3.5], the center of $G/Z$ is trivial. □

**Example 5.6.22.** The connected semisimple group $SL_n$ is simply connected. Its center is $\mu_n$, and the quotient $(SL_n)^{\text{ad}} = SL_n / \mu_n$ is isomorphic to the adjoint group $PGL_n$.

**Corollary 5.6.23.** For a connected semisimple group, the properties of being simply connected or adjoint are unchanged by base field extension.

**Remark 5.6.24.** Here we explain how the use of the word “adjoint” here relates to other uses of the word. Each $g \in G(k)$ induces an automorphism $x \mapsto gxg^{-1}$ of $G$, which in turn induces an automorphism of its Lie algebra $\mathfrak{g}$. This construction works with $S$-valued points as well as $k$-valued points, so we get a homomorphism of algebraic groups $\text{Ad}: G \to \text{GL}(\mathfrak{g})$, called the **adjoint homomorphism**. The kernel of $\text{Ad}$ turns out to be the center $Z$ of $G$, so the image $G^{\text{ad}}$ of $\text{Ad}$ is isomorphic to $G/Z$.  

125
Because of Proposition 5.6.21[a], to classify all connected semisimple groups, it suffices to classify the simply connected semisimple groups $G$; then for each such $G$ compute the center $Z$, compute the finitely many subgroup schemes $Z' \subseteq Z$, and consider the quotients $G/Z'$.

5.6.6. Almost simple groups. A simple algebraic group is a connected semisimple group $G$ that has exactly two normal subgroup schemes, $\{1\}$ and $G$. If $k$ is an algebraically closed field of characteristic 0, then an algebraic group $G$ is simple if and only if the abstract group $G(k)$ is simple.

It is not true that every connected semisimple group is a product of simple groups. For example, if $n \geq 2$, then $\text{SL}_n$ is not simple (it has $\mu_n$ as a normal subgroup scheme), but it is not a nontrivial product either. Therefore we define a less restrictive concept: an almost simple algebraic group is a connected semisimple group $G$ such that the quotient $G/Z$ of $G$ by its center $Z$ is simple. (Recall that $Z$ is finite: see Corollary 5.6.11.)

Remark 5.6.25. What we call “simple” is what other authors might call “$k$-simple”: the notion is relative to the ground field, and might be lost if the base field is extended. The same applies to “almost simple”.

Theorem 5.6.26 (Classification of almost simple groups). Fix a separably closed field $k$. Almost simple groups over $k$ up to the equivalence relation generated by central isogenies are in bijection with connected Dynkin diagrams. In particular, for each connected Dynkin diagram $D$, there is one simply connected group and one adjoint group of type $D$.

Call $G$ geometrically almost simple (or absolutely almost simple) if $G_{k_s}$ is almost simple. For each field $k$, let $\mathcal{S}(k)$ be the set of isomorphism classes of split geometrically almost simple simply connected groups over $k$.

Theorem 5.6.27. For any field extension $L \supseteq k$, the map $\mathcal{S}(k) \to \mathcal{S}(L)$ is a bijection.

Thus among geometrically almost simple simply connected groups over $k$ of a given type $D$, there is exactly one that is split, and all others are twists of that one.

5.6.7. Decomposition of a semisimple group.

Theorem 5.6.28. Every simply connected semisimple group is uniquely expressible as a product of almost simple groups.

By taking the quotients by the centers, we find that every adjoint semisimple group is uniquely expressible as a product of adjoint simple groups.

Example 5.6.29. For $n > 1$, embed $\mu_n$ diagonally in $\text{SL}_n \times \text{SL}_n$, and let $G = (\text{SL}_n \times \text{SL}_n)/\mu_n$. Then $G$ is not a product of almost simple groups, but $\widetilde{G} = \text{SL}_n \times \text{SL}_n$, and $G^{\text{ad}} = \text{PGL}_n \times \text{PGL}_n$. 

126
Decompositions over $k$ and over $k_s$ are related, as we now explain. Let $G$ be a simply connected semisimple group over $k$. Write $G_{k_s} = \prod_{i \in I} G_i$ for some almost simple groups $G_i$ over $k_s$. The Galois group $\mathfrak{G}_k$ acts on $G_{k_s}$ and hence also on $I$. For each $i \in I$, the stabilizer of $i$ is $G_{L_i} \leq \mathfrak{G}_k$ for some finite separable extension $L_i \supseteq k$ contained in $k_s$, and $G_i$ descends to an algebraic group $H_i$ over $L_i$. For each $\mathfrak{G}_k$-orbit $J \subseteq I$, the product $\prod_{i \in J} G_i$ descends to an almost simple group $G_J$ over $k$. Thus the decomposition of $G$ over $k$ corresponds to the decomposition of $I$ into $\mathfrak{G}_k$-orbits. Finally, if $i \in J$, then $G_J \simeq \text{Res}_{L_i/k} H_i$. Thus the classification of simply connected groups reduces to the classification of geometrically almost simple simply connected groups over finite separable extensions.

**5.6.8. Decomposition of a reductive group.** The following theorem says that a reductive group is almost a direct product of a semisimple group and a torus.

**Theorem 5.6.30.** Let $G$ be a connected reductive group. Let $T$ be the maximal torus in the center of $G$ (see Corollary 5.5.11). Let $G' = [G, G]$ be the commutator subgroup. Then $G'$ is semisimple, and the multiplication map $G' \times T \to G$ is surjective with finite kernel isomorphic to $G' \cap T$.

**Proof.** We may assume that $k$ is algebraically closed. In this case, the result is contained in [PR94, Theorem 2.4].

Let us summarize how to build all reductive groups over a field $k$.

1. Given a Dynkin diagram $\mathcal{D}$ and a finite separable extension $L \supseteq k$, construct the unique split geometrically almost simple simply connected group over $L$ of type $\mathcal{D}$.
2. Use Galois cohomology to classify its twists over $L$; these are all geometrically almost simple connected groups over $L$ of type $\mathcal{D}$.
3. Apply $\text{Res}_{L/k}$ to these twists (for all $\mathcal{D}$ and $L$) to obtain the almost simple simply connected groups over $k$.
4. Take a finite product to obtain the simply connected groups over $k$.
5. Divide by a subgroup scheme of the center to obtain the connected semisimple groups over $k$.
6. Take the product with a torus, and divide again by a subgroup scheme of the center to obtain the connected reductive groups over $k$.

**Remark 5.6.31.** Semisimple and reductive groups can also be understood in terms of reduced root data.

### 5.7. Abelian varieties

(Reference: [Mum70, §3.2])
Definition 5.7.1. An algebraic group over a field \( k \) is called an abelian variety if it is smooth, proper, and connected.

Example 5.7.2. A 0-dimensional abelian variety is the same thing as the trivial algebraic group. A 1-dimensional abelian variety is the same thing as an elliptic curve.

Proposition 5.7.3. Abelian varieties are nice.

Proof. Let \( A \) be an abelian variety. By Theorem 5.2.20, \( A \) is quasi-projective. Quasi-projective and proper imply projective. Since \( A \) has a \( k \)-point (the identity), connected implies geometrically connected (Proposition 2.3.24). Smooth and geometrically connected imply geometrically integral (Proposition 3.5.66).

□

Abelian varieties are also commutative: see [Mum70, pp. 41–44] for two proofs.

Proposition 5.7.4. Let \( A \) be an abelian variety over a field \( k \), and let \( m \) be an integer such that \((\text{char } k) \nmid m\). Then the multiplication-by-\( m \) map \( A \to A \) is étale.

Sketch of proof. Because of Theorem 4.3.7(ii), we may assume that \( k \) is algebraically closed. The set of points where the map is étale is open, so it suffices to check that it is étale at each \( a \in A(k) \). By translating, it suffices to check that it is étale at \( a = 0 \). One can show that its derivative at 0 equals multiplication-by-\( m \) as an endomorphism of the tangent space of \( A \) at 0. If \((\text{char } k) \nmid m\), then this linear map is invertible.

□

Definition 5.7.5. A semiabelian variety is an extension \( G \) of an abelian variety \( A \) by a torus \( T \):

\[
0 \to T \to G \to A \to 0.
\]

5.7.1. Jacobian varieties.

(References: [Mil86b], [BLR90], Chapters 8 and 9, [Kle05])

Let \( X \) be a nice \( k \)-curve. Recall that there is a homomorphism \( \text{deg}: \text{Pic} X \to \mathbb{Z} \), and that \( \text{Pic}^0 X \) is defined as its kernel.

Theorem 5.7.6. Let \( X \) be a nice \( k \)-curve of genus \( g \). Assume that \( X \) has a \( k \)-point. Then there is a \( g \)-dimensional abelian variety \( J = \text{Jac} X \), called the Jacobian of \( X \), such that \( J(k) \simeq \text{Pic}^0 X \) as groups, and more generally \( J(L) \simeq \text{Pic}^0 X_L \) for every field extension \( L \supseteq k \), functorially in \( L \).

Proof. See [Mil86b].

□

Remark 5.7.7. In fact, [Mil86b] contains a stronger version of Theorem 5.7.6 that specifies not only \( J(L) \) for field extensions \( L \supseteq k \), but also \( J(T) \) for every \( k \)-scheme \( T \), i.e., the entire functor of points. This is needed if one wants to determine the group scheme \( J \).
uniquely up to isomorphism. Under the hypotheses of Theorem 5.7.6, if \( \pi: X \times_k T \to T \) denotes the second projection, and \( X_t := \pi^{-1}(t) \) for each \( t \in T \), then

\[
J(T) \cong \left\{ \mathcal{L} \in \text{Pic}(X \times_k T) : \text{for every } t \in T, \text{the restriction } \mathcal{L}_t \in \text{Pic} X_t \text{ is of degree } 0 \right\}.
\]

Elements of \( J(T) \) can be thought of as families of degree 0 line bundles on \( X \) parametrized by the points of \( T \); the pullback of a line bundle on \( T \) restricts to the trivial line bundle on each fiber since the map from a fiber to \( T \) factors through a point.

**Remark 5.7.9.** In both Theorem 5.7.6 and Remark 5.7.7, the assumption that \( X \) has a \( k \)-point can be weakened to the assumption that \( X \) has a degree 1 divisor, or equivalently \( X \) has closed points of degrees whose gcd is 1.

**Warning 5.7.10.** If \( X \) does not have a degree 1 divisor, then the conclusions of Theorem 5.7.6 and Remark 5.7.7 can sometimes fail. The problem is that for any \( k \)-scheme \( J \) and for any Galois field extension \( L \supseteq k \), there is a bijection \( J(k) \to J(L)^{\text{Gal}(L/k)} \), but in general \( \text{Pic}^0 X \to (\text{Pic}^0 X_L)^{\text{Gal}(L/k)} \) is only injective: see Corollary 6.7.8 for a related fact, and see Exercise 2.12 for an example. In general, the Jacobian \( J \) still exists, but the correct description of its points over a field \( L \supseteq k \) is \( J(L) \cong (\text{Pic}^0 X_L)^{\text{Gal}(L_s/L)} \), functorially in \( L \).

The correct generalization of this to \( T \)-valued points for an arbitrary \( k \)-scheme \( T \) is that the functor of points of \( J \) is the \( \text{fppf-sheafification} \) (see Section 6.3.4) of the functor on the right side of (5.7.8).

**Remark 5.7.11.** The functor has a variant using \( \text{Pic} \) instead of \( \text{Pic}^0 \). It is represented by the Picard scheme \( \text{Pic}_{X/k} \), a group scheme that is only \( \text{locally} \) of finite type over \( k \). It has countably many connected components \( \text{Pic}^n_{X/k} \), indexed by \( n \in \mathbb{Z} \), and each \( \text{Pic}^n_{X/k} \) is a nice \( k \)-variety. Moreover, \( \text{Pic}^0_{X/k} \) is isomorphic to the Jacobian \( J \), and there is an exact sequence

\[
0 \to J \to \text{Pic}^0_{X/k} \to \mathbb{Z} \to 0,
\]

where the \( \mathbb{Z} \) on the right denotes a constant group scheme over \( k \).

**Remark 5.7.12.** Even more generally, given an \( S \)-scheme \( X \), the relative Picard functor \( \text{Pic}_{X/S} \) is defined as the fppf-sheafification of the functor

\[
T \mapsto \text{Pic}(X \times_S T)
\]

on \( S \)-schemes \( T \). (The sheafification process automatically trivializes pullbacks of line bundles on \( T \), so it is not necessary to take the quotient as in (5.7.8).) Here are two criteria for representability of \( \text{Pic}_{X/S} \):

- If \( X \to S \) is flat, projective, and finitely presented with geometrically reduced fibers, then \( \text{Pic}_{X/S} \) is represented by a scheme that is locally of finite presentation over \( S \).
• If $X$ is a proper $k$-scheme, then $\text{Pic}_{X/k}$ is represented by a scheme that is locally of finite type over $k$.

5.7.2. Albanese varieties.

(References: [Ser60, Wit10] Section 2 and Appendix A)

The notion of Jacobian of a curve generalizes in two different ways to higher-dimensional varieties, as we discuss in this section and the next.

Let $X$ be a geometrically integral variety over a field $k$. Is there a morphism to an abelian variety, $f: X \to A$, such that every other such morphism $f': X \to A'$ factors uniquely as $f$ followed by a homomorphism $A \to A'$? Not quite: for instance, if $x \in X(k)$ is such that $f(x) = 0$, and $f'$ is $f$ followed by a nonzero translation, then $f'(x) \neq 0$, but any homomorphism $A \to A'$ must map 0 to 0.

If a point $x \in X(k)$ is fixed, however, and we restrict attention to morphisms that send $x$ to 0, then the answer becomes yes. This can be reformulated as follows:

**Theorem 5.7.13 (Existence of Albanese varieties).** Let $\mathcal{C}_{X,x}$ be the category of pairs $(A,f)$, where $A$ is an abelian variety over $k$, and $f: X \to A$ is a morphism such that $f(x) = 0$; a morphism from $(A,f)$ to $(A',f')$ is a homomorphism $\alpha: A \to A'$ making the triangle

$$
\begin{array}{ccc}
X & \xrightarrow{f} & A \\
\downarrow{f'} & & \downarrow{\alpha} \\
A' & & 
\end{array}
$$

commute. Then $\mathcal{C}_{X,x}$ has an initial object $(\text{Alb}_{X/k}, \iota)$.

**Proof.** See [Ser60] Théorème 5] for the case where $k$ is algebraically closed, and [Wit10] Appendix A] for the general case.

**Definition 5.7.14.** The abelian variety $\text{Alb}_{X/k}$ is called the **Albanese variety** of $X$.

**Remark 5.7.15.** For a variant that does not require a $k$-point $x$, see Example 5.12.11. It will follow from Exercise 5.16 that $\text{Alb}_{X/k}$ is independent of $x$.

**Remark 5.7.16.** There is also a variant using semiabelian varieties instead of only abelian varieties: see [Ser60 Théorème 7] and [Wit08 Appendix A].

5.7.3. Picard varieties.

(References: [Gro95b, Kle05])

Let $X$ be a nice $k$-variety. The group scheme $\text{Pic}^0_{X/k}$ is proper over $k$ [Gro95b Théorème 2.1(ii)], but in general it may happen that it is not reduced, and hence not an abelian variety. The **Picard variety** of $X$ is the associated reduced subscheme $\text{Pic}^0_{X/k,\text{red}}$. 

130
Theorem 5.7.17 ([Gro95b, Corollaire 3.2]). The scheme $\text{Pic}^0_{X/k, \text{red}}$ is a subgroup scheme of $\text{Pic}^0_{X/k}$, and it is an abelian variety.

**Sketch of proof.** In general, for an algebraic group $G$ over a field $k$ of characteristic $p > 0$, it can happen that $G_{\text{red}}$ is not a subgroup scheme: see Exercise 5.11. But if $G$ is commutative, proper, and connected, then Proposition 5.2.19 and its proof imply that $G$ is an extension of an abelian variety $A$ by a finite commutative connected group scheme $F$ of order $p^n$ for some $n$; then it turns out that $p^nF = 0$, so $p^nG$ (the scheme-theoretic image of multiplication-by-$p^n$) is isomorphic to $p^nA = A$, so $p^nG$ is a closed subgroup of $G$ whose underlying scheme is $G_{\text{red}}$. Apply this to $G := \text{Pic}^0_{X/k}$. □

**Remark 5.7.18.** The group scheme $\text{Pic}^0_{X/k}$ is an abelian variety even before passing to the reduced subscheme if any of the following hold:

- char $k = 0$;
- $X$ is a curve; or
- $X$ is an abelian variety.

But there exist nice varieties $X$ of dimension $\geq 2$ over an algebraically closed field $k$ of characteristic $p$ such that $\text{Pic}^0_{X/k}$ is not reduced; see Example 5.7.22 for an example, and [Kle05, Remark 9.5.15] for discussion.

**Definition 5.7.19.** If $X$ is an abelian variety, then $\text{Pic}^0_{X/k}$ is called the dual abelian variety.

**Theorem 5.7.20** (Albanese–Picard duality). Let $X$ be a nice $k$-variety. Then $\text{Pic}^0_{X/k, \text{red}}$ is the dual abelian variety of $\text{Alb}_{X/k}$.

**Proof.** See [Gro95b, Théorème 3.3(iii)]. □

**Remark 5.7.21.** Let $X$ be a nice $k$-variety. Let $0$ be the identity point of $\text{Pic}^0_{X/k}$, and let $T_0\text{Pic}^0_{X/k}$ be the tangent space there. Then it turns out that $T_0\text{Pic}^0_{X/k} \simeq H^1(X, \mathcal{O}_X)$. In particular, if $\dim \text{Pic}^0_{X/k} < \dim H^1(X, \mathcal{O}_X)$, then $\text{Pic}^0_{X/k}$ is not smooth at 0, and hence not reduced (see Theorem 5.2.16).

**Example 5.7.22** ([Igu55]). Let $k$ be a field of characteristic 2. Let $E$ and $E'$ be elliptic curves over $k$ such that $E$ has a $k$-point $e$ of order 2. Let $\iota$ be the order 2 automorphism of $E \times E'$ given by $(x, y) \mapsto (x + e, -y)$. Then $\iota$ has no fixed points, so the quotient variety $X := (E \times E')/\iota$ is a nice surface. One can show that $\text{Alb}_{X/k}$ is the quotient of $E$ by the subgroup generated by $e$; in particular, $\dim \text{Pic}^0_{X/k} = \dim \text{Alb}_{X/k} = 1$. On the other hand, it turns out that $\dim H^1(X, \mathcal{O}_X) = 2$. Thus, by Remark 5.7.21, $\text{Pic}^0_{X/k}$ is not reduced. (For other examples, see [Ser58, Section 20].)
5.7.4. Abelian schemes.

(Reference: [Mil86a, §20])

Definition 5.7.23. A group scheme $A \to S$ is an abelian scheme if it is smooth and proper and has connected fibers.

An abelian scheme over $S$ may be thought of as a family of abelian varieties parametrized by the points of $S$.

Remark 5.7.24. Let $R$ be a discrete valuation ring, and let $K = \text{Frac } R$. Let $A$ be an abelian variety over $K$. If $A$ has good reduction in the sense of Section 3.5.14, so there exists a smooth proper $R$-model $\mathcal{A}$, then it turns out that $A \to \text{Spec } R$ is automatically an abelian scheme. Thus $A$ has good reduction if and only if it is the generic fiber of an abelian scheme over $\text{Spec } R$.

5.7.5. Néron models of abelian varieties.

(Reference: [BLR90])

Recall from Section 3.5.16 the notion of Néron model.

Theorem 5.7.25 (Néron). Let $R$ be a discrete valuation ring. Let $K = \text{Frac } R$. Let $A$ be an abelian variety over $K$. Then $A$ has a Néron model $\mathcal{N}$, and $\mathcal{N}$ is of finite type over $R$.

Proof. See [Art86a, Theorem 1.2] or [BLR90, §1.3, Corollary 2]. ☐

Proposition 5.7.26. Let $R,K,A,\mathcal{N}$ be as in Theorem 5.7.25. Let $T$ be a smooth $R$-scheme. Then any $K$-rational map $T_K \dashrightarrow A$ extends to an $R$-morphism $T \to \mathcal{N}$.

Proof. According to [Wei48b, §2, No. 15, Théorème 6], any $K$-rational map $T_K \dashrightarrow A$ is a $K$-morphism. Next, the Néron property says that any $K$-morphism $T_K \to A$ extends to an $R$-morphism $T \to \mathcal{N}$. ☐

Remark 5.7.27. Theorem 5.7.25 extends to the case where $R$ is replaced by an integral Dedekind scheme, and $K$ is its function field. See [BLR90, §1.4, Theorem 3]. For example, an abelian variety over $\mathbb{Q}$ has a Néron model over $\mathbb{Z}$.

Remark 5.7.28. Theorem 5.7.25 can be extended also in a different direction, to the case where $A$ is a semiabelian variety over a discrete valuation ring. See [Art86a, Theorem 1.9] or [BLR90, §10.2, Theorem 2]. But these Néron models are generally no longer of finite type. For example, if $A = \mathbb{G}_{m,K}$ and $\pi \in R$ is a uniformizer, then $A(K) = K^\times = R^\times \times \pi\mathbb{Z}$, and the Néron model $\mathcal{N}$ can be constructed by glueing copies of $\mathbb{G}_{m,R}$ indexed by $n \in \mathbb{Z}$ along their generic fibers, with the $n$th generic fiber glued to the $0$th by multiplication-by-$\pi^n$ on $\mathbb{G}_{m,K}$: see [BLR90, §10.1, Example 5].

It is not yet known if Remarks 5.7.27 and 5.7.28 can be combined: see [BLR90, §10.3].
5.7.6. Néron models of elliptic curves.

(References: [BLR90, Section 1.5], [Liu02, Section 10.2], [Con15])

Here we describe in more explicit terms the Néron model of an elliptic curve \( E \), and relate it to Weierstrass equations. Let \( R \) be a discrete valuation ring, and let \( K = \text{Frac} \, R \). Let \( v: K \to \mathbb{Z} \cup \{ \infty \} \) be the discrete valuation.

Start with an elliptic curve \( E \) over \( K \). If \( \text{char} \, K \) is not 2 or 3, then \( E \) is the closure in \( \mathbb{P}^2_K \) of an affine plane curve \( y^2 = x^3 + Ax + B \) with \( A, B \in K \) such that \( 4A^3 + 27B^2 \neq 0 \). Without restriction on the characteristic, \( E \) is the curve in \( \mathbb{P}^2_K \) defined by a Weierstrass equation

\[
y^2z + a_1xyz + a_3yz^2 = x^3 + a_2x^2z + a_4xz^2 + a_6z^3
\]

such that a certain polynomial \( \Delta \) in \( a_1, a_2, a_3, a_4, a_6 \) is nonzero [Sil09, Section III.1]. A Weierstrass model of \( E \) is a closed subscheme of \( \mathbb{P}^2_R \) cut out by an equation (5.7.29) with \( a_1, a_2, a_3, a_4, a_6 \in R \) whose generic fiber over \( K \) is isomorphic to \( E \). Among all such models, any one that minimizes \( v(\Delta) \) is called a minimal Weierstrass model: cf. [Sil09, Chapter VII].

Let \( W \) be a minimal Weierstrass model, so \( W \) is a proper \( R \)-scheme. If \( v(\Delta) = 0 \), then \( W \) is an abelian scheme over \( R \); this is the case in which \( E \) has good reduction. If \( v(\Delta) > 0 \), then the special fiber \( W_k \) has a nonsmooth point, so \( W \to \text{Spec} \, R \) is not smooth, but \( W \) might be regular. In any case, one can iteratively blow up nonregular points until one reaches a regular proper model \( \mathcal{E} \), which in fact is the minimal regular proper model in the sense of Section 9.3.1.6 (usually constructing the minimal regular proper model requires normalizations as well as blow-ups, and requires blowing down some exceptional curves, but this turns out to be unnecessary for elliptic curves: see the end of [Con15]). Although \( \mathcal{E} \) is regular, it need not be smooth over \( R \). Removing from \( \mathcal{E} \) all nonsmooth points of the special fiber \( \mathcal{E}_k \) (which may include removing entire irreducible components of \( \mathcal{E}_k \) if they are of multiplicity > 1) yields the smooth locus \( \mathcal{E}^{\text{smooth}} \). Similarly, removing from \( W \) the nonsmooth point of the special fiber \( W_k \) (if there is one) yields the smooth locus \( W^{\text{smooth}} \).

**Theorem 5.7.30.** Let \( R \) be a discrete valuation ring. Let \( K = \text{Frac} \, R \). Let \( E \) be an elliptic curve over \( K \). Let \( W, \mathcal{E}, \) and \( \mathcal{N} \) be, respectively, a minimal Weierstrass model, the minimal regular proper model, and the Néron model. Let \( \mathcal{N}^0 \) be the open subscheme of \( \mathcal{N} \) obtained by removing the non-identity components of the special fiber of \( \mathcal{N} \). Then \( \mathcal{E}^{\text{smooth}} \to \mathcal{N} \) and \( W^{\text{smooth}} \to \mathcal{N}^0 \).

**Proof.** See [Con15, Theorems 5.4 and 5.5]. The morphisms come from the Néron property: for example, the identity \( E \to E \) extends to \( \mathcal{E}^{\text{smooth}} \to \mathcal{N} \).

The first conclusion in Theorem 5.7.30 generalizes to higher genus: see Theorem 3.5.82

5.7.7. Arithmetic of abelian varieties.
Theorem 5.7.31 (Mordell–Weil theorem). Let $A$ be an abelian variety over a global field $k$. Then the abelian group $A(k)$ is finitely generated.

Sketch of proof. Fix $m \in \mathbb{Z}_{\geq 2}$ not divisible by char $k$. Theorem 5.7.31 implies the “weak Mordell–Weil theorem” that $A(k)/mA(k)$ is finite, but in fact, all known proofs of Theorem 5.7.31 involve proving the weak Mordell–Weil theorem (or some variant) first. For a proof of the weak Mordell–Weil theorem, see Theorem 8.4.9. Combining this with the theory of height functions completes the proof: see [Ser97, 4.3]. □

Let $A$ be an abelian variety over a global field $k$. To $A$ one can attach two objects that are conjecturally related to $A(k)$:

- The Shafarevich–Tate group of $A$ is
  \[ \text{III}(A) := \ker(H^1(k, A) \to \prod_{v \in \Omega_k} H^1(k_v, A)). \]
  Because $\text{III}(A)$ is a subgroup of a Galois cohomology group, it is a torsion abelian group.
- The $L$-function of $A$ is
  \[ L(A, s) := \prod_{\text{finite } v} \det (1 - q_v^{-s} \text{Frob}_v |(V_\ell A)^{I_v})^{-1}, \]
  where $q_v$ is the order of the residue field, $\text{Frob}_v \in \mathfrak{S}_k$ is a Frobenius element, $V_\ell A$ is as in Example 7.5.5, and $I_v \leq \mathfrak{S}_k$ is an inertia group. It turns out that the product converges for $\text{Re } s > 3/2$, and conjecturally it has an analytic continuation to all of $\mathbb{C}$ [Tat95a, p. 216].

Conjecture 5.7.32 (Shafarevich–Tate conjecture [Tat63, Conjecture 4.1]). For every abelian variety $A$ over a global field $k$, the group $\text{III}(A)$ is finite.

Conjecture 5.7.32 is open even for elliptic curves $A$ over $\mathbb{Q}$: this case has been proved only under the additional hypothesis that the order of vanishing of its $L$-function at $s = 1$ is at most 1.

Conjecture 5.7.33 (Birch and Swinnerton-Dyer conjecture, rank part). Let $A$ be an abelian variety over a global field $k$. Then $\text{ord}_{s=1} L(A, s) = \text{rk } A(k)$.

Remark 5.7.34. The full Birch and Swinnerton-Dyer conjecture predicts that the leading coefficient in the Taylor series of $L(A, s)$ at $s = 1$ equals a product of certain arithmetic invariants of $A$, including $\# \text{III}(A)$; it may be considered an analogue of the Dirichlet analytic class number formula. The conjecture was formulated for elliptic curves over $\mathbb{Q}$ by Birch and Tate.\footnote{Or should we say Tate-Shafarevich group? In the Cyrillic alphabet, the first letter III of Shafarevich comes after T.}
Swinnerton-Dyer [BSD65, SD67], and generalized to abelian varieties over global fields by Tate [Tat95a].

Conjecture 5.7.33 is known for elliptic curves $A$ over $\mathbb{Q}$ such that $\operatorname{ord}_{s=1} L(A, s) \leq 1$.

5.8. Finite étale group schemes

A smooth algebraic group of dimension 0 over $k$ is the same thing as a finite étale group scheme over $k$.

A $\mathfrak{G}_k$-group is a discrete group equipped with a continuous action of $\mathfrak{G}_k$. A $\mathfrak{G}_k$-module is a discrete abelian group equipped with a continuous action of $\mathfrak{G}_k$. A $\mathfrak{G}_k$-group or $\mathfrak{G}_k$-module is finite if it is finite as a set. The following gives a concrete way to study finite étale group schemes over $k$:

**Theorem 5.8.1.** The functors

$$
\{\text{finite étale group schemes over } k\} \leftrightarrow \{\text{finite } \mathfrak{G}_k\text{-groups}\}
$$

$$
G \mapsto G(k_s)
$$

$$
\text{Spec} \operatorname{Hom}_{\text{sets}}(A, k_s)_{\mathfrak{G}_k} \leftrightarrow A
$$

are inverse equivalences of categories, and the first restricts to an equivalence of categories

$$
\{\text{commutative finite étale group schemes over } k\} \leftrightarrow \{\text{finite } \mathfrak{G}_k\text{-modules}\}.
$$

**Proof.** The first equivalence arises from taking the group objects on both sides of Theorem 1.3.2 and using the anti-equivalence between affine $k$-schemes and $k$-algebras. Then imposing commutativity on both sides yields the second equivalence. \qed

5.9. Classification of smooth algebraic groups

(Reference: [Kne67])

5.9.1. Classification over perfect fields. Let $G$ be a smooth algebraic group over a perfect field $k$. We will define a chain of smooth algebraic subgroups in $G$, each normal in $G$.

The connected component $G_{\text{conn}} = G^0$ of $G$ is a closed and open normal subgroup of $G$ (Proposition 5.2.4), and $G/G_{\text{conn}}$ is a finite étale group scheme, called the component group of $G$ (this holds even if $k$ is not necessarily perfect and $G$ is not necessarily smooth). Next, “Chevalley’s theorem” states that there is a unique exact sequence of smooth connected algebraic groups

$$
(5.9.1) \quad 0 \to G_{\text{affine}} \to G_{\text{conn}} \to A \to 0,
$$

where $G_{\text{affine}}$ is affine and $A$ is an abelian variety; in fact, $G_{\text{affine}}$ is the unique maximal smooth connected affine algebraic subgroup of $G_{\text{conn}}$ (or of $G$). As mentioned in Section 5.6, the
radical $G_{\text{solv}} := \mathcal{R}(G_{\text{affine}})$ is the unique maximal smooth connected solvable normal subgroup of $G_{\text{affine}}$; the quotient $G_{\text{affine}}/G_{\text{solv}}$ is semisimple. As mentioned in Section 5.6, the unipotent radical $G_{\text{unip}} := \mathcal{R}_u(G_{\text{affine}}) = \mathcal{R}_u(G_{\text{solv}})$ is the unique maximal smooth connected unipotent normal subgroup of $G_{\text{affine}}$; then $G_{\text{solv}}/G_{\text{unip}}$ is a torus.

To summarize, we have the following chain of normal algebraic subgroups of $G$:

$$
\begin{array}{c}
\mathcal{R}(	ext{finite étale}) \\
G_{\text{conn}} \quad \text{proper} \\
\mathcal{R}(	ext{abelian variety}) \\
G_{\text{affine}} \quad \text{semisimple} \\
G_{\text{solv}} \quad \text{reductive} \\
G_{\text{unip}} \quad \text{torus} \\
\mathcal{R}(	ext{unipotent}) \\
\{1\}
\end{array}
$$

Each label between groups indicates the type of group that arises as the quotient.

### 5.9.2. Functorial properties.

**Proposition 5.9.2.** If $L \supseteq k$ is an extension of perfect fields, then the chain for $G_L$ is obtained by base-extending each group in the chain for $G$.

**Proof.** For $G_{\text{conn}}$ it follows since $G_{\text{conn}}$ is geometrically connected (Proposition 5.2.4). For $G_{\text{affine}}$ it follows from the uniqueness of (5.9.1), since base-extending (5.9.1) yields a sequence with the same properties over $L$. For $G_{\text{solv}}$, this has been mentioned already in Remark 5.6.3. For $G_{\text{unip}}$ see [CGP10, Proposition 1.1.9(1)].

**Proposition 5.9.3.** Let $f : G \to H$ be a homomorphism of smooth algebraic groups. Then

(a) $f$ restricts to a homomorphism $G_{\text{conn}} \to H_{\text{conn}}$, and

(b) $f$ restricts to a homomorphism $G_{\text{affine}} \to H_{\text{affine}}$.

**Proof.**

(a) The image of $G_{\text{conn}}$ is connected and contains the identity point 1 of $H$.

(b) Let $I$ be the image of the induced homomorphism $G_{\text{affine}} \to H_{\text{conn}}/H_{\text{affine}}$. By Theorem 5.2.9, $I$ is both a quotient of the smooth affine connected group $G_{\text{affine}}$, and a closed
subgroup of the abelian variety $H_{\text{conn}}/H_{\text{affine}}$. The former shows that $I$ is smooth, affine, and connected (Proposition 5.2.7(a)), and the latter shows that $I$ is proper. Thus $I$ is trivial.

\(\square\)

\(\hat{\ast}\) Warning 5.9.4. A homomorphism $f: G \to H$ of smooth algebraic groups does not necessarily restrict to $G_{\text{solv}} \to H_{\text{solv}}$ and $G_{\text{unip}} \to H_{\text{unip}}$. (For a counterexample, let $f$ be the embedding $U_n \hookrightarrow \text{SL}_n$ for some $n \geq 2$.)

5.9.3. Imperfect fields.

(Reference: [CGP10])

A few aspects of the classification fail over imperfect fields $k$. Let $G$ be a smooth connected affine algebraic group.

- As in Remark 5.6.3 if $k$ is not perfect, the unipotent radical of $G_\bar{k}$ need not descend to an algebraic group over $k$; thus $\mathcal{R}_u(G_\bar{k})$ can be strictly larger than $\mathcal{R}_u(G)_\bar{k}$. In fact, it can happen that $\mathcal{R}_u(G_\bar{k}) \neq \{1\}$ while $\mathcal{R}_u(G) = \{1\}$: see Exercise 5.13. Call $G$ pseudo-reductive if $\mathcal{R}_u(G) = \{1\}$ [CGP10, Definition 1.1.1]; this is weaker than being reductive.
- There are similar issues with the radical $\mathcal{R}(G)$. Moreover, it turns out that semisimplicity condition $\mathcal{R}(G_\bar{k}) = \{1\}$ implies $[G, G] = G$, but the weaker condition $\mathcal{R}(G) = \{1\}$ does not, so it is natural to require $[G, G] = G$ separately. Therefore call $G$ pseudo-semisimple if $\mathcal{R}(G) = \{1\}$ and $[G, G] = G$ [CGP10, Definition 11.2.2].
- Chevalley’s theorem above must be modified as follows: a connected algebraic group $G$ contains a smallest connected affine normal subgroup scheme $G_{\text{affine}}$ such that $G/G_{\text{affine}}$ is an abelian variety. But $G_{\text{affine}}$ need not be smooth: see [BLR90, 9.2, Theorem 1]. In particular, the formation of $G_{\text{affine}}$ does not commute with inseparable base extension.

There is an alternative to Chevalley’s theorem that works over any field, but is backwards in that the affine group is the quotient instead of the subgroup. Call an algebraic group $A$ anti-affine if $\mathcal{O}(A) = k$. Anti-affine algebraic groups are smooth, connected, and commutative; see [Bri09] and the references listed there for these and more properties of these groups.

Theorem 5.9.5. A smooth connected algebraic group $G$ over a field $k$ fits in an exact sequence of smooth connected algebraic groups

$$0 \to A \to G \to L \to 0$$

in which $A$ is anti-affine and $L$ is affine.

Sketch of proof. Let $L = \text{Spec} \mathcal{O}(G)$, and use the group structure on $G$ to define a group structure on $L$. See [DG70, III, §3, no. 8] for the rest of the proof. \(\square\)
For cohomological purposes, Theorem 5.9.5 is superior to the original Chevalley theorem in that the commutative group is on the left.

5.10. Approximation theorems

(References: PR94 Chapter 7 and Rap14)

Recall from Section 2.6.4.5 the notions of weak and strong approximation for varieties over a global field.

5.10.1. Weak approximation. Recall from Section 2.6.2 that for any variety \(X\) over \(\mathbb{R}\) (or a subfield), the set \(X(\mathbb{R})\) can be equipped with the analytic topology.

THEOREM 5.10.1 (Real approximation theorem). Let \(G\) be a connected affine algebraic group over \(\mathbb{Q}\). Then \(G(\mathbb{Q})\) is dense in \(G(\mathbb{R})\).

Theorem 5.10.1 is implied by the case \(k = \mathbb{Q}\) of Theorem 5.10.4(a) below.

\(\square\) WARNING 5.10.2. The conclusion of Theorem 5.10.1 can fail if \(G\) is not connected: see Exercise 5.14. It can fail also if \(G\) is not affine: consider a rank 0 elliptic curve over \(\mathbb{Q}\).

\(\square\) WARNING 5.10.3. There exists a connected semisimple algebraic group \(G\) over \(\mathbb{Q}\) such that \(G(\mathbb{Q})\) is not dense in \(G(\mathbb{Q}_2)\) [San81 Exemple 5.8].

THEOREM 5.10.4 (Weak approximation theorem). Let \(G\) be a connected affine algebraic group over a number field \(k\).

(a) There exists a finite set of finite places \(T\) of \(k\) such that \(G(k)\) is dense in \(\prod_{v \in T} G(k_v)\).

(b) The closure of \(G(k)\) in \(\prod_{v \in \Omega_k} G(k_v)\) is an open normal subgroup, and the quotient is a finite abelian group.

(c) If \(G\) is a simply connected or adjoint group, then \(G\) satisfies weak approximation.

PROOF.

(a) Let \(L \supseteq k\) is a finite Galois extension such that \(G_L\) is split. Let \(T\) be the set of \(v \in \Omega_k\) for which a decomposition group of \(v\) in \(\text{Gal}(L/k)\) is not cyclic. Thus \(T\) is a subset of the set of ramified finite primes in the extension \(L \supseteq k\). It turns out that \(T\) satisfies the conclusion [San81 Corollaire 3.5(ii)]. The proof reduces to the case of tori, which is attributed to Serre. (In general, a variety over a global field that satisfies weak approximation away from finitely many places is said to satisfy weak weak approximation!)

(b) See [San81 Corollaire 3.5(i)]. The quotient is called the defect of weak approximation.

(c) See PR94 Theorem 7.8. \(\square\)

REMARK 5.10.5. If instead \(k\) is a global function field, (c) still holds [Har67 Satz 2.2.4], but (a) and (b) can fail. For example, if \(p\) is odd, \(k = \mathbb{F}_p(t)\), and \(G \leq \mathbb{G}_a^2\) is defined by
\[ y^p = tx^p + x \text{ over } k, \text{ then } G(k) \text{ is finite by } \text{Vol91, Theorem 3], but } G(k_v) \text{ is infinite for every } v \text{ by Proposition 3.5.74.} \]

For more on weak approximation in algebraic groups, see [PR94, Section 7.3].

### 5.10.2. Strong approximation.

**Theorem 5.10.6** (Strong approximation theorem; Kneser, Platonov, Prasad, Margulis). Let \( G \) be a connected semisimple algebraic group over a global field \( k \). Let \( S \) be a finite set of places of \( k \). Then \( G(k) \) is dense in \( G(\mathbf{A}^S) \) if and only if \( G \) is simply connected and for each almost simple factor \( G_i \) of \( G \), there exists \( v \in S \) such that \( G_i(k_v) \) is noncompact.

**Proof.** See the original sources [Kne66, Pla69, Pra77, Mar77], or see [PR94, Section 7.4]. □

See Theorem 8.4.10 for the reason for the simply connected hypothesis.

**Remark 5.10.7.** If \( k \) is a number field, there is a more general statement, applicable to any algebraic group \( G \) over \( k \). Namely, \( G \) satisfies strong approximation if and only if \( G \) is connected and affine, the torus \( G_{\text{sol/v}} / \text{unip} \) is trivial, and the semisimple quotient \( G / G_{\text{sol}} \) satisfies the criterion of Theorem 5.10.6.

### 5.11. Inner twists

Let \( G \) be a smooth algebraic group over \( k \). The action of \( G \) on itself by inner automorphisms defines a homomorphism

\[ G(k_s) \to \text{Aut } G_{k_s}. \]

This induces a map of pointed sets

\[ H^1(k, G) \to H^1(k, \text{Aut } G_{k_s}). \] (5.11.1)

The image of an element \( \tau \in H^1(k, G) \) under (5.11.1) (or, more precisely, a cocycle representing this image) defines a twist \( G^\tau \) of the algebraic group \( G \), called an **inner twist**. It is another smooth algebraic group over \( k \).

### 5.12. Torsors

(Reference: Section 6.4 of [BLR90], Chapter 2 of [Sko01])

**5.12.1. Warmup: torsors of groups.** Let \( G \) be a group.

**Definition 5.12.1.** A (right) \( G \)-torsor (also called torsor under \( G \) or principal homogeneous space of \( G \)) is a right \( G \)-set isomorphic to \( G \) with the right action of \( G \) by translation.
In other words, a $G$-torsor is a set $X$ with a simply transitive $G$-action (simply transitive means that $X$ is nonempty and that for every $x, x' \in X$ there exists a unique $g \in G$ such that $xg = x'$).

If $X$ is a $G$-torsor, then a choice of $x \in X$ determines an isomorphism of $G$-sets

$$G \longrightarrow X$$

$$g \longmapsto xg.$$ 

**Example 5.12.2.** If $G$ is a subspace of a vector space $V$, and $X$ is a translate of $G$, then $X$ is a $G$-torsor. Here $X$ is not canonically isomorphic to $G$, but a choice of $x \in X$ determines a translation isomorphism $G \to X$ sending $0$ to $x$.

**5.12.2. Torsors under algebraic groups.** Let $k$ be a field. Let $G$ be a smooth algebraic group over $k$. The trivial $G$-torsor over $k$, which for convenience we denote by $G$, is the underlying variety of $G$ equipped with the right action of $G$ by translation.

**Definition 5.12.3.** A $G$-torsor over $k$ (also called **torsor under $G$** or **principal homogeneous space of $G$**) is a $k$-variety $X$ equipped with a right action of $G$ such that $X_{ks}$ equipped with its right $G_{ks}$-action is isomorphic to $G_{ks}$ (the isomorphism is required to respect the right actions of $G_{ks}$). A **morphism of $G$-torsors** is a $G$-equivariant morphism of $k$-schemes.

**Remark 5.12.4.** The definition can be generalized to non-smooth $G$, but then one should use $\overline{k}$ instead of $k$. We restrict to smooth $G$ for now so that Galois cohomology suffices in Section 5.12.4. For a generalization, see Section 6.5.

**Remark 5.12.5.** If $X$ is a $G$-torsor over $k$, then $X(k_s)$ is a $G(k_s)$-torsor in the sense of Section 5.12.1.

**Warning 5.12.6.** A $k$-variety $X$ equipped with a right $G$-action making $X(k_s)$ a $G(k_s)$-torsor is not necessarily a $G$-torsor. For example, if $G$ is a smooth algebraic group over $\mathbb{F}_p$, then $X$ could be $G$ with the action

$$X \times G \longrightarrow X$$

$$(x, g) \longmapsto x \cdot F(g),$$

where $F: G \to G$ is the Frobenius endomorphism; this $X$ is not a $G$-torsor if $\dim G > 0$.

**Remark 5.12.7.** The notion of torsor can be generalized to the notion of homogeneous space. First suppose that $G$ is a group. A right $G$-set $X$ decomposes as a disjoint union of $G$-orbits. If $X$ consists of exactly one $G$-orbit, then $X$ is called a **homogeneous space of $G$**. If $H$ is a subgroup of $G$, then $H \backslash G$ is a homogeneous space; conversely, if $X$ is a homogeneous space, and $H$ is the stabilizer of some $x \in X$, then $X \simeq H \backslash G$ as homogeneous spaces.
Now suppose that $G$ is a smooth algebraic group. A $k$-variety $X$ equipped with a right $G$-action is called a **homogeneous space** if there exists $x \in X(k_s)$ such that

$$G_k \longrightarrow X_k$$

$$g \longmapsto xg$$

is surjective, or equivalently if there exists a closed subgroup $H \leq G_k$ such that $X_k \simeq H \backslash G_k$ as $k_s$-varieties equipped with right $G_k$-action.

### 5.12.3. Examples.

#### Example 5.12.8

Let $T$ be the torus $x^2 + 2y^2 = 1$ of Example 5.5.3. Then the affine variety $X$ defined by $x^2 + 2y^2 = -3$ in $\mathbb{A}^2_\mathbb{Q}$ can be viewed as a $T$-torsor over $\mathbb{Q}$. It is a nontrivial torsor, since $X(\mathbb{Q}) = \emptyset$.

#### Example 5.12.9

Let $L/k$ be a finite Galois extension of fields. Let $G$ be the constant group scheme over $k$ associated to $\text{Gal}(L/k)$. (See Section 5.1.) Then the obvious right action of $G$ on $\text{Spec} L$ makes $\text{Spec} L$ a $G$-torsor over $k$.

#### Example 5.12.10

Let $A$ be a smooth closed subgroup of a smooth algebraic group $B$. Let $\phi: B \rightarrow C := B/A$ be the natural surjective morphism to the quotient (which in general is only a $k$-variety, since we did not assume that $A$ was normal). Let $c \in C(k)$. Then the closed subscheme $\phi^{-1}(c) \subseteq B$ is an $A$-torsor over $k$.

#### Example 5.12.11 (Albanese torsor)

Let $X$ be a geometrically integral variety over a field $k$. Let $\mathcal{C}_X$ be the category of triples $(A, T, f)$, where $A$ is an abelian variety over $k$, and $T$ is an $A$-torsor, and $f: X \rightarrow T$ is a morphism; a morphism from $(A, T, f)$ to $(A', T', f')$ consists of a homomorphism $\alpha: A \rightarrow A'$, and a morphism of varieties $\tau: T \rightarrow T'$ such that the diagrams

$$\begin{align*}
T \times A & \longrightarrow T \\
\downarrow (a, \tau) & \downarrow \tau \\
T' \times A' & \longrightarrow T'
\end{align*}$$

$$\begin{align*}
X & \longrightarrow T \\
\downarrow f & \downarrow \tau \\
X & \longrightarrow T'
\end{align*}$$

commute. Then $\mathcal{C}_X$ has an initial object $(\text{Alb}_{X/k}, \text{Alb}^1_{X/k}, \iota)$; see [Wit08, Appendix A].

The abelian variety $\text{Alb}_{X/k}$ is called the **Albanese variety** of $X$, and its torsor $\text{Alb}^1_{X/k}$ is called the **Albanese torsor** of $X$. In the case that $X$ has a $k$-point $x$, the abelian variety $\text{Alb}_{X/k}$ defined using $\mathcal{C}_{X,x}$ in Theorem 5.7.13 coincides with the abelian variety $\text{Alb}_{X/k}$ defined using $\mathcal{C}_X$: see Exercise 5.16.

As in Remark 5.7.16 there is a semiabelian variant: see [Wit08, Appendix A].

#### Example 5.12.12

Let $X$ be a nice genus 1 curve, so $\text{Alb}_{X/k}$, the Jacobian of $X$, is a 1-dimensional abelian variety, an elliptic curve. One can show that the morphism $X \rightarrow \text{Alb}^1_{X/k}$ is an isomorphism, so $X$ is a torsor under the elliptic curve $\text{Alb}_{X/k}$. 

141
5.12.4. Classification of torsors. For any fixed smooth algebraic group $G$ over $k$, we have bijections

$$\{G\text{-torsors over } k\} = \{\text{twists of } G\} \quad (\text{these should really be sets of } k\text{-isomorphism classes})$$

$$\leftrightarrow H^1(k, \text{Aut } G_{k_s}) \quad (\text{by Theorems } 4.5.2 \text{ and } 5.2.20)$$

$$= H^1(k, G(k_s)) \quad (\text{see Exercise } 5.15)$$

$$=: H^1(k, G).$$

Given a $G$-torsor $X$, let $[X] \in H^1(k, G)$ be its class.

Remark 5.12.13. The cohomology class of a torsor can also be constructed explicitly. Given a $G$-torsor $X$, choose $x \in X(k_s)$, and define $g_\sigma \in G(k_s)$ by $\sigma x = x \cdot g_\sigma$; then $\sigma \mapsto g_\sigma$ is a $1$-cocycle representing the class of $X$ in $H^1(k, G)$.

A $G$-torsor is analogous to a coset of a group $G$ in some larger group, or to a translate of a subspace $G$ in some larger vector space. To trivialize a torsor $T$, one must choose a point in $T$ to be translated back to the identity of $G$, but such a point might not exist over the ground field. With this intuition, the following should not be a surprise:

Proposition 5.12.14 (Trivial torsors). Let $G$ be a smooth algebraic group over a field $k$. Let $X$ be a $G$-torsor over $k$. The following are equivalent:

(i) $X$ is isomorphic to the trivial torsor $G$.

(ii) $X(k) \neq \emptyset$.

(iii) $[X] \in H^1(k, G)$ is the neutral element.

Proof. (i)$\iff$(iii): This is a general fact about twists.

(i)$\Rightarrow$(ii): The set $G(k)$ contains the identity.

(ii)$\Rightarrow$(iii): This follows from the explicit construction of a cocycle above. \qed

Exercise 5.22 gives another way of thinking about torsors when $G$ is commutative.

5.12.5. Geometric operations on torsors. Throughout this section, $G$ is a smooth algebraic group over $k$. When $G$ is commutative, $H^1(k, G)$ is an abelian group. The group operations can be expressed in purely geometric terms, as we now explain. In fact, some versions of the operations make sense even when $G$ is not commutative.

5.12.5.1. Inverse torsors. Let $G$ be the trivial right $G$-torsor. It also has a left action of $G := G$, so one says that $G$ is a $G$-$G$-bitorsor:

$$G \circlearrowright G \circlearrowleft G$$

The automorphism group scheme of the right $G$-torsor $G$ is $G$ acting on the left.
Now let $\tau \in H^1(k, G)$. The left action of $\mathcal{G}$ on $G$ does not commute with the left action of other elements of $\mathcal{G}$ so if we twist $G$ by (a cocycle representing) $\tau$ to get the corresponding right $G$-torsor $T$, then the left action of $\mathcal{G}$ must be twisted too. The result is that $T$ is a $\mathcal{G}^\tau$-$G$-bitorsor, where $\mathcal{G}^\tau$ is the inner twist (see Section 5.11):

$\mathcal{G}^\tau \circ T \circ G$.

The same $k$-scheme $T$ has a left action of $G$ defined by $g \cdot t := tg^{-1}$, and similarly a right action of $\mathcal{G}^\tau$. The resulting $G$-$\mathcal{G}^\tau$-bitorsor is denoted $T^{-1}$, and is called the inverse torsor:

$G \circ T^{-1} \circ \mathcal{G}^\tau$.

**Example 5.12.15.** If $G$ is commutative, then $\mathcal{G}^\tau = G$ and $[T^{-1}] = -[T]$ in the abelian group $H^1(k, G)$.

**5.12.5.2. Contracted products.** Let $T$ be a right $G$-torsor; let $\tau \in H^1(k, G)$ be its class. Let $X$ be a quasi-projective $k$-variety equipped with a left $G$-action. This action defines a homomorphism $G(k_s) \to \text{Aut} X_{k_s}$ and hence a map $H^1(k, G) \to H^1(k, \text{Aut} X_{k_s})$. The image of (a cocycle representing) $\tau$ under this map corresponds to a twist of $X$, called the **contracted product** $T^G \times X$. Geometrically, it is the quotient of $T \times_k X$ by the $G$-action in which $g \in G$ acts by $(t, x) \mapsto (tg^{-1}, gx)$.

In a similar way, if $T$ is a left $G$-torsor and $Z$ is a quasi-projective variety with a right $G$-action, then we can construct the contracted product $Z^G \times T$.

**Example 5.12.16.** If $G$ is commutative and $Z$ also is a $G$-torsor, then $Z^G \times T$ is another $G$-torsor, and $[Z \times T] = [Z] + [T]$ in the abelian group $H^1(k, G)$.

**Example 5.12.17.** If $Z$ is a right $G$-torsor, and $T$ is a $G$-$H$-bitorsor, then $Z^G \times T$ is a right $H$-torsor.

**5.12.5.3. Subtraction of torsors.** Let $Z$ and $T$ be two right $G$-torsors; let $\zeta, \tau \in H^1(k, G)$ be their classes. As in Section 5.12.5.1, $T^{-1}$ is a $G$-$G^\tau$-bitorsor. By Example 5.12.17, $Z^G \times T^{-1}$ is then a right $G^\tau$-torsor. If we fix $T$, then the “subtraction-of-$\tau$” map

$$H^1(k, G) \xrightarrow{-\tau} H^1(k, G^\tau)$$

$$[Z] \mapsto [Z^G \times T^{-1}],$$

is a bijection, the inverse bijection being subtraction-of-$[T^{-1}]$.

**Example 5.12.18.** If $G$ is commutative, then $G^\tau = G$ and the class of the right $G$-torsor $Z^G \times T^{-1}$ is $\zeta - \tau$ by Examples 5.12.15 and 5.12.16.
5.12.6. **Torsors over fields of dimension** \( \leq 1 \). The following theorem shows that certain algebraic groups over certain fields have no nontrivial torsors:

**Theorem 5.12.19.**

(a) (Lang) Let \( k \) be a finite field, and let \( G \) be a smooth connected algebraic group over \( k \). Then \( H^1(k, G) = 0 \).

(b) (Steinberg) Let \( k \) be a perfect field. Then

\[
\dim k \leq 1 \iff H^1(k, G) = 0 \text{ for all smooth connected affine algebraic groups } G \text{ over } k.
\]

**Proof.**

(a) We follow the original proof of [Lan56]. An element of \( H^1(k, G) \) corresponds to a \( G \)-torsor \( X \). By Proposition 5.12.14, it suffices to show that \( X \) has a \( k \)-point.

Fix \( x \in X(\overline{k}) \). Then every other point of \( X(\overline{k}) \) is \( xg \) for some \( g \in G(\overline{k}) \), and to say that \( xg \) is a \( k \)-point is to say that it is fixed by the Frobenius automorphism \( \sigma \in \text{Gal}(\overline{k}/k) \).

Thus we must find \( g \in G(\overline{k}) \) such that \( \sigma(xg) = xg \), or equivalently \( \sigma x g g^{-1} = x \). Since \( X \) is a torsor, there exists \( b \in G(\overline{k}) \) such that \( \sigma x b = x \), so it suffices to show the following:

\[
(5.12.20) \quad \text{Every } b \in G(\overline{k}) \text{ is of the form } \sigma g g^{-1}.
\]

(Alternatively, we could have reduced to proving (5.12.20) by using the definition of non-abelian \( H^1 \).)

Let \( q = \# k \). Let \( F: G \to G \) be the \( q \)-power Frobenius endomorphism; it acts on \( \overline{k} \)-points in the same way as \( \sigma \). There is a left action of \( G \) on \( T := G \) in which \( g \) acts as \( t \mapsto F(g) t g^{-1} \). Then (5.12.20) is equivalent to \( b \) being in the \( G(\overline{k}) \)-orbit of \( 1 \).

Fix \( t \in T(\overline{k}) \) and define a morphism

\[
\phi: G\overline{k} \to T\overline{k},
\]

\[
g \mapsto F(g) t g^{-1}.
\]

The derivative of \( F \) is everywhere 0, so the derivative of \( \phi \) at \( g = 1 \) equals the derivative of the invertible morphism \( g \mapsto tg^{-1} \) at \( g = 1 \); thus the derivative of \( \phi \) at \( g = 1 \) is invertible. If a morphism between smooth varieties \( V \to W \) of the same dimension has invertible derivative somewhere, its image contains a nonempty Zariski open subset of \( W \). Applying this to \( \phi: G\overline{k} \to T\overline{k} \) shows that an arbitrary \( G(\overline{k}) \)-orbit in \( T(\overline{k}) \) contains a nonempty Zariski open subset of \( G(\overline{k}) \). Since also \( G \) is connected, and hence geometrically connected, any two orbits will intersect. But orbits are disjoint, so there can be only one. In particular, \( b \) is in the \( G(\overline{k}) \)-orbit of \( 1 \), as required.

(b) See [Ste65] Theorem 1.9], or the reproduction in Theorem 1’ of III.§2 and III.Appendix 1 of [Ser02].

\[\square\]
Remark 5.12.21. The same proof shows that Theorem 5.12.19(a) remains true if the smoothness hypothesis is dropped and one interprets \(H^1(k, G)\) as the Čech fppf cohomology set defined in Section 6.4.4.

**Corollary 5.12.22.** A nice genus 1 curve \(X\) over a finite field \(k\) has a \(k\)-point.

**Proof.** Let \(E\) be the Jacobian of \(X\). As discussed in Example 5.12.12, \(X\) is an \(E\)-torsor. By Theorem 5.12.19(a), \(H^1(k, E) = 0\), so \(X\) is a trivial torsor. By Proposition 5.12.14(i) \(\Rightarrow\)(ii), \(X\) has a \(k\)-point. \(\square\)

**Remark 5.12.23.** The first proof of Corollary 5.12.22 used the Riemann–Roch theorem: see [Sch31, Satz 20]. Corollary 5.12.22 can also be viewed as a consequence of the Hasse–Weil bound: see Corollary 7.2.1.

### 5.12.7. Torsors over local fields.

**Theorem 5.12.24.** Let \(k\) be a local field.

(a) (Borel–Serre) Let \(G\) be an affine algebraic group over \(k\). If \(\text{char } k = 0\) or \(G\) is connected and reductive, then \(H^1(k, G)\) is finite.

(b) (Kneser, Bruhat–Tits) If \(k \not\cong \mathbb{R}\), and \(G\) is a simply connected semisimple algebraic group over \(k\), then \(H^1(k, G) = 0\).

(c) (Tate) If \(A\) is an abelian variety over \(k\), then \(H^1(k, A) \simeq \text{Hom}_{\text{conts}}(A(k), \mathbb{Q}/\mathbb{Z})\).

**Proof.**

(a) See [BS64, Théorème 6.1] and [Ser02, III.§4.3, Remark 2].

(b) This was proved in [Kne65a, Kne65b] using the classification of such groups when \(k\) is a finite extension of \(\mathbb{Q}_p\), and was extended to local fields of characteristic \(p\) in [BT87], which gave a classification-free proof.

(c) See [Tat95b]. \(\square\)

**Warning 5.12.25.** With regard to Theorem 5.12.24(a), it is not true that \(H^1(k, G)\) is finite for every affine algebraic group \(G\) over a local field \(k\) of characteristic \(p\), even if \(k\) is commutative and smooth. For example, \(H^1(k, \mathbb{Z}/p\mathbb{Z})\) is infinite in this case, since if \(t \in k\) is a uniformizer, then each positive integer \(n\) not divisible by \(p\) gives rise to a \(\mathbb{Z}/p\mathbb{Z}\)-extension \(k[y]/(y^p - y - t^{-n})\) of \(k\), and these are distinct because their discriminants are distinct. For a connected pseudo-reductive example, see [CGP10, Example 11.3.3].

**Warning 5.12.26.** Theorem 5.12.24(a) can fail if the affineness assumption is dropped. For example, if \(A\) is a nonzero abelian variety, then Theorem 5.12.24(c) implies that \(H^1(k, A)\) is infinite.
Warning 5.12.27. Theorem 5.12.24(b) is false for $k = \mathbb{R}$. For example, $\#H^1(\mathbb{R}, \text{Spin}_n) \to \infty$ as $n \to \infty$, as can be deduced from the fact that the number of isomorphism types of rank $n$ quadratic forms over $\mathbb{R}$ grows with $n$. Nevertheless, the group $H^1(\mathbb{R}, G)$ can be described explicitly for every simply connected group over $\mathbb{R}$ [Bor88].

For more results along the lines of Theorems 5.12.19 and 5.12.24, see [Ser02, Chapter III].

5.12.8. Local-global principle for torsors. Let $G$ be an algebraic group over a global field $k$. Let $X$ be a right $G$-torsor, and let $[X]$ denote its class in $H^1(k, G)$ (throughout this section, if $\text{char } k = p$ and $G$ is not smooth, then interpret $H^1(k, G)$ as the Čech fppf cohomology set defined in Section 6.4.4). By Proposition 5.12.14, $X$ has a $k$-point if and only if $[X]$ is the neutral element $0$. Similarly, $X$ has a $k_v$-point if and only if the image $[X_{k_v}]$ of $[X]$ under $H^1(k, G) \to H^1(k_v, G)$ is $0$. Thus the statement that $X$ satisfies the local-global principle is the statement

“If $[X]$ maps to $0$ in $H^1(k_v, G)$ for every $v$, then $[X] = 0$ in $H^1(k, G)$.”

Hence the statement that all right $G$-torsors satisfy the local-global principle is the statement that the kernel

$$\text{III}^1(k, G) := \ker(H^1(k, G) \to \prod_v H^1(k_v, G))$$

is trivial.

If $G$ is noncommutative, then a stronger statement is that the map

$$H^1(k, G) \longrightarrow \prod_v H^1(k_v, G) \tag{5.12.28}$$

is injective. For each $\tau \in H^1(k, G)$, we have an inner twist $G^\tau$ of $G$, and the subtraction-of-$\tau$ bijection $H^1(k, G) \to H^1(k, G^\tau)$ of Section 5.12.5.3 identifies the fiber of (5.12.28) containing $\tau$ with $\text{III}^1(k, G^\tau)$. Thus injectivity of (5.12.28) is equivalent to the statement that $\text{III}^1(k, G^\tau) = 0$ for every inner twist $G^\tau$ of $G$. There are also variants in which $v$ ranges not over all places of $k$, but only over places outside a fixed finite subset $S$; one defines

$$\text{III}^1_S(k, G) := \ker(H^1(k, G) \to \prod_{v \not\in S} H^1(k_v, G)).$$

None of the injectivity statements are true in general, but the following weaker result holds:

**Theorem 5.12.29.** Let $k$ be a global field. Let $S$ be a finite set of places of $k$. Let $G$ be an affine algebraic group over $k$. Then $H^1(k, G) \to \prod_{v \not\in S} H^1(k_v, G)$ has finite fibers.

**Proof.** The number field case was proved by Borel and Serre [BS64, Theorem 7.1]. For the global function field case, see [Nis79, BP90, Section 4], [Oes84, IV, 2.6, Proposition(a)], and [Con12b, Theorem 1.3.3(i)].

146
Remark 5.12.30. The analogue of Theorem 5.12.29 for abelian varieties is a conjecture: see Conjecture 5.7.32.

Theorem 5.12.31 (Kneser, Harder, Chernousov). Let $G$ be a simply connected semisimple group over a global field $k$. Then the map

$$H^1(k, G) \rightarrow \prod_v H^1(k_v, G) \simeq \prod_{\text{real } v} H^1(k_v, G)$$

is a bijection. In particular, if $k$ is a totally imaginary number field or a global function field, then $H^1(k, G) = 0$.

Proof. By Theorem 5.12.24(b), $H^1(k_v, G)$ is trivial for each nonreal place $v$. For the number field case, see [PR94, Theorem 6.6]. The statement $H^1(k, G) = 0$ for a global function field is proved in [Har75]. □

Theorem 5.12.32 (Voskresenskii). Let $T$ be a torus of dimension at most 2 over a global field $k$. Then $\text{III}^1(k, T) = 0$.

Sketch of proof. One classifies all finite subgroups of $\text{GL}_d(\mathbb{Z})$ for $d \leq 2$ to classify all possibilities for $T$, and one checks the result in each case: see [Vos65] for the details. □

Exercises

5.1. (Center of a group scheme vs. center of its group of points) Over a field $k$, let $\{\pm 1\}$ denote the constant group scheme associated to a two-element group (view 1 and $-1$ as symbols that are distinct even if $\text{char } k = 2$). Let $\{\pm 1\}$ act on $\mathbb{G}_m$ so that $-1$ acts as $x \mapsto x^{-1}$. Let $G$ be the semidirect product $\mathbb{G}_m \rtimes \{\pm 1\}$ over $k$. Let $Z$ be the center of $G$.

(a) Prove that $Z \simeq \mu_2$.

(b) Show that if $k = \mathbb{F}_2$, then $Z(k)$ is strictly smaller than the center of $G(k)$.

5.2. Let $S$ be a scheme.

(a) Prove that the group schemes $U_{n,S}$ and $\mathbb{G}^{n(n-1)/2}_{a,S}$ over $S$ have the same underlying $S$-scheme.

(b) Prove that if $S$ is nonempty and $n \geq 3$, they are not isomorphic as group schemes.

5.3. (Group schemes of order $p$) Let $k$ be a field of characteristic $p$. Show that $\mu_p$, $\alpha_p$, and the constant group scheme $\mathbb{Z}/p\mathbb{Z}$ over $k$ are pairwise nonisomorphic as group schemes over $k$.

5.4. ("Inseparable twist" of $\mathbb{G}_a$) Let $k$ be a field of characteristic $p$, and suppose that $t \in k - k^p$. (So in particular, $k$ is not perfect.) Let $G$ be the $k$-subvariety of $\mathbb{G}_a^2$ defined by the equation $y^p = tx^p + x$. Prove that

(a) $G$ is a subgroup scheme of $\mathbb{G}_a^2$.

(b) $G_{\overline{k}} \simeq \mathbb{G}_{a,\overline{k}}$ as $\overline{k}$-group schemes.

(c) $G$ is not isomorphic to the $k$-group scheme $\mathbb{G}_a$. 
(d) $G$ as a $k$-variety (without group structure) is not isomorphic to $\mathbb{A}^1$.

(e) $G$ is birational to $\mathbb{A}^1$ over $k$ if and only if $p = 2$.

5.5. (Coordinate-free variant of $GL_n$) Let $k$ be a field, and let $V$ be a finite-dimensional $k$-vector space. For each $k$-algebra $A$, define $GL_V(A)$ to be the group of $A$-module automorphisms of $V \otimes_k A$. Prove that the functor $GL_V$ is represented by an algebraic group.

5.6. (Representations of $G_m$) Let $G$ be an algebraic group over a field $k$. A (finite-dimensional) representation of $G$ is a homomorphism $G \to GL_V$ of algebraic groups for some finite-dimensional $k$-vector space $V$. Prove that giving a representation of $G_m$ on a vector space $V$ is equivalent to giving a direct sum decomposition $V = \bigoplus_{n \in \mathbb{Z}} V_n$ into subspaces indexed by $\mathbb{Z}$. (Hint: Given a decomposition, define an action of $G_m$ on $V$ such that each $a \in k$ act as multiplication-by-$a^n$ on $V_n$ and likewise for elements of $k$-algebras.)

5.7. (Hodge structures [Del71, 2.1])

(a) Define the Deligne torus $S := \text{Res}_{\mathbb{C}/\mathbb{R}} G_m$. Prove that there is a unique isomorphism $S_{\mathbb{C}} \cong G_m \times G_m$ of algebraic groups over $\mathbb{C}$ such that the induced homomorphism $S_{\mathbb{C}}(\mathbb{R}) \hookrightarrow S(\mathbb{C}) \to (G_m \times G_m)(\mathbb{C}) = \mathbb{C}^\times \times \mathbb{C}^\times$ is $z \mapsto (z, \bar{z})$.

(b) Let $V$ be an $\mathbb{R}$-vector space. Complex conjugation acts on $V_{\mathbb{C}} := V \otimes_{\mathbb{R}} \mathbb{C}$ through the second factor. Let $W$ be a $\mathbb{C}$-subspace of $V_{\mathbb{C}}$. Let $\overline{W}$ be the image of $W$ under complex conjugation. Prove that $\overline{W}$ is another $\mathbb{C}$-subspace of $V_{\mathbb{C}}$.

(c) A Hodge structure over $\mathbb{R}$ is a finite-dimensional representation of $S$. Prove that giving a Hodge structure is the same as giving a finite-dimensional $\mathbb{R}$-vector space $V$ equipped with a direct sum decomposition $V_{\mathbb{C}} = \bigoplus_{(p, q) \in \mathbb{Z}^2} V^{pq}$ into $\mathbb{C}$-subspaces $V^{pq}$ such that $V^{qp} = \overline{V^{pq}}$ for all $(p, q) \in \mathbb{Z}^2$.

5.8. The cocharacter group of a $k$-torus $T$ is the $G_k$-module $Y(T) := \text{Hom}_{k_{\text{alg}}} (G_m, T)$. 

(a) Describe the abelian group $Y(T)$ stripped of its $G_k$-action.

(b) Define a bilinear $G_k$-equivariant pairing

$$X(T) \times Y(T) \to \mathbb{Z}$$

and show that it identifies each of $X(T)$ and $Y(T)$ with the $\mathbb{Z}$-dual of the other.

(c) Restate Theorem 5.5.7 using $Y(T)$ instead of $X(T)$.

(Remark: One advantage of $X(T)$ over $Y(T)$ is that it can be used also in the generalization given in Theorem 5.5.10.)

5.9. Compute $\text{Hom}(\mu_n, G_m)$ in the category of algebraic groups over a field $k$. 

148
5.10. Let $T$ be a group of multiplicative type over a field $k$. Prove that $T$ is smooth if and only if either $\text{char } k = 0$, or $\text{char } k = p$ and $X(T)$ has no nontrivial elements of order $p$.

5.11. Let $k = \mathbb{F}_2(t)$. Let $f: \mathbb{G}_a \to \mathbb{G}_a$ be the homomorphism $x \mapsto x^4 - tx^2$. Let $G = \ker f$.
   (a) Prove that $G^0 \simeq \alpha_2$.
   (b) Prove that $G_{\text{red}}$ is not a subgroup scheme of $G$.

5.12. Let $k$ be a field. Let $n \geq 1$. Let $A = k[\epsilon]/(\epsilon^n)$. Let $G = \text{Res}_{A/k} \mathbb{G}_m$. Prove that there exists a unipotent group $U$ of dimension $n - 1$ and an exact sequence
   \[ 1 \to U \to G \to \mathbb{G}_m \to 1 \]
   of smooth algebraic groups.

5.13. (Example of a pseudo-reductive group) Let $k$ be a separably closed field of characteristic $p$ having a field extension $L$ of degree $p$. Let $G = \text{Res}_{L/k} \mathbb{G}_m$.
   (a) Prove that $\dim R_u(G_k) = p - 1$.
   (b) Prove that $G(k)$ has no nontrivial elements of order $p$.
   (c) Prove that $\mathscr{R}_u(G) = \{1\}$.
   (d) Deduce that $G$ is pseudo-reductive but not reductive. (Cf. [CGP10, Example 1.1.3].)

5.14. (Failure of real approximation) Let $T$ be the torus $x^2 + 2y^2 = 1$ of Example 5.5.3. Let $G$ be the kernel of the cubing map $T \to T$. Prove that $G(\mathbb{Q})$ is not dense in $G(\mathbb{R})$.

5.15. Let $G$ be a smooth algebraic group over a field $k$. Let $G$ be the trivial right $G$-torsor. Prove that there is an isomorphism $G(k) \simeq \text{Aut } G$.

5.16. Let $X$ be a geometrically integral $k$-variety with a $k$-point $x$. Prove that the category $\mathcal{C}_{X,x}$ of Section 5.7.2 is equivalent to the category $\mathcal{C}_X$ of Example 5.12.11 and that the two definitions of $\text{Alb}_{X/k}$ are compatible.

5.17. Let $k$ be a field. (Assume char $k \neq 2$ if you want to make the problem easier.)
   (a) Find explicit equations for all 1-dimensional tori $T$ over $k$.
   (b) For each $T$, find explicit equations for all $T$-torsors over $k$.

5.18. Prove that any smooth connected algebraic group $G$ over a field $k$ is geometrically integral.

5.19. Use Theorem 5.12.19(a) to give another proof of Wedderburn’s theorem that every finite division ring is commutative, or equivalently, that the Brauer group of a finite field is trivial.

5.20. In [Lan56], Lang proved a stronger form of Theorem 5.12.19(a). Specifically, he proved that any homogeneous space $X$ of a smooth connected algebraic group $G$ over a finite field $k$ has a $k$-point. Prove this.

5.21. Let $k$ be a finite field. Let $G$ be an algebraic group over $k$.
   (a) Prove that $H^1(k, G)$ is finite.
      (Hint: To handle the noncommutative case, use [Ser02] I.§5.5, Corollary 2].)
   (b) Give an example to show that $H^1(k, G)$ can have more than one element.
5.22. (Extensions and torsors) Let $G$ be a smooth commutative algebraic group over a field $k$, with group law written additively. An extension of the constant group scheme $\mathbb{Z}$ by $G$ (in the category of commutative $k$-group schemes) is a commutative $k$-group scheme $E$ fitting in an exact sequence

$$0 \rightarrow G \rightarrow E \rightarrow \mathbb{Z} \rightarrow 0.$$ 

A morphism of extensions is a commutative diagram

$$
\begin{array}{c}
0 \longrightarrow G \longrightarrow E \longrightarrow \mathbb{Z} \longrightarrow 0 \\
\downarrow \quad \quad \quad \quad \quad \quad \downarrow \\
0 \longrightarrow G \longrightarrow E' \longrightarrow \mathbb{Z} \longrightarrow 0.
\end{array}
$$

Given an extension, write $E = \coprod_{n \in \mathbb{Z}} E_n$, where $E_n$ is the inverse image under $E \rightarrow \mathbb{Z}$ of the point corresponding to the integer $n$.

(a) Prove that each $E_n$ is a $G$-torsor.

(b) Prove that

$$
\{ \text{extensions of } \mathbb{Z} \text{ by } G \} \rightarrow \{ \text{$G$-torsors over } k \}
$$

$$
(0 \rightarrow G \rightarrow E \rightarrow \mathbb{Z} \rightarrow 0) \mapsto E_1
$$

defines an equivalence of categories, and hence that the set of isomorphism classes of extensions is in bijection with $H^1(k, G)$.

(c) Prove that any extension induces an exact sequence of $\mathfrak{g}_k$-modules

$$0 \rightarrow G(k_\text{s}) \rightarrow E(k_\text{s}) \rightarrow \mathbb{Z} \rightarrow 0$$

and that the image of $n$ under the coboundary homomorphism $\mathbb{Z} = H^0(\mathfrak{g}_k, \mathbb{Z}) \rightarrow H^1(k, G)$ is $[E_n]$.

(Remark: Similarly, a 2-extension

$$0 \rightarrow G \rightarrow E_1 \rightarrow E_0 \rightarrow \mathbb{Z} \rightarrow 0$$

gives rise to a class in $H^2(k, G)$, and so on; this is related to the notion of gerbe.)
CHAPTER 6

Étale and fppf cohomology

(References: [SGA 4\textsuperscript{1}/2], [Mil80], [FK88], [Tam94])

Étale cohomology was developed by M. Artin and Grothendieck for reasons to be discussed in Section 6.1. To set up the foundations of étale cohomology properly would require a whole book. In fact, there are several books about this, cited above. We will only introduce some of the key concepts and definitions, and cite many results without proof.

In this chapter, schemes are assumed to be separated and locally noetherian.

6.1. The reasons for étale cohomology

6.1.1. Generalization of Galois cohomology. Étale cohomology over Spec \( k \) is the same as Galois cohomology, so étale cohomology over more general schemes can be thought of as a generalization of Galois cohomology. More precisely, it will turn out that any abelian sheaf \( \mathcal{F} \) for the étale topology on Spec \( k \) gives rise to a continuous \( G_k \)-module called \( \mathcal{F}(k_\text{sep}) \) (and vice versa), and the étale cohomology group \( H^i_{\text{ét}}(\text{Spec } k, \mathcal{F}) \) equals the Galois cohomology group \( H^i(G_k, \mathcal{F}(k_\text{sep})) \). See Theorem 6.4.6.

For instance, in Section 5.12 we saw that torsors under a smooth algebraic group \( A \) over \( k \) could be classified by the Galois cohomology set \( H^1(G_k, A(k_\text{sep})) \). To classify torsors under group schemes over a more general scheme \( S \) we need étale cohomology.

One can also generalize the cohomological description of the Brauer group of a field, to define the Brauer group of an arbitrary scheme.

6.1.2. Comparison with classical cohomology theories. Given a compact complex manifold \( X \), one can define singular cohomology groups \( H^i(X, \mathbb{Z}) \), \( H^i(X, \mathbb{Z}/n\mathbb{Z}) \), and so on. One can also define cohomology of coherent analytic sheaves; this can be useful in proving the existence of global meromorphic functions on compact complex manifolds, for instance. These cohomology theories use the analytic topology on \( X \).

It would be nice if these cohomology theories worked for varieties over other fields. But one does not usually have an analytic topology on such a variety, so one needs to find substitutes. To measure the success of a cohomology theory, we check whether for proper \( \mathbb{C} \)-varieties it gives the same answers as the classical topological cohomology theories such as singular cohomology.
It turns out that the Zariski topology on a proper variety gives the right answers for cohomology of coherent sheaves; see [Ser55] or [Har77] Appendix B, 2.1. But the Zariski topology is not fine enough to give the right answers for constant coefficients. For instance, if $X$ is a nice $\mathbb{C}$-curve of genus $g$, then the singular cohomology group $H^1(X(\mathbb{C}), \mathbb{Z})$ and the sheaf cohomology group $H^1(X^{an}, \mathbb{Z})$ for the analytic topology both give $\mathbb{Z}^{2g}$, which should be considered the right answer; but if we use the Zariski topology on $X$, and let $\mathbb{Z}$ be the constant sheaf $\mathbb{Z}$ on $X$, then $H^1(X, \mathbb{Z}) = 0$ since $\mathbb{Z}$ is flasque [Har77, III.2.5]. Again, the problem is that the Zariski topology has too few open subsets in comparison with the analytic topology.

To obtain a sufficiently fine topology on a scheme, one must be open-minded about what a topology is, and in particular about what open subsets and open coverings are: see Section 6.2. The “topologies” that follow are not topologies in the usual sense.

The étale “topology” on $X$, which is finer than the Zariski topology, is a substitute for the analytic topology, and has an associated cohomology theory. Étale cohomology does not give the right answer for $H^1(X, \mathbb{Z})$, but it does give the right answers for cohomology with a finite abelian group as coefficients, at least when the order of the group is not divisible by the characteristic. For instance, if $X$ is a nice curve of genus $g$ over an algebraically closed field $k$, and $n$ is an integer not divisible by $\text{char} \ k$, then we get the right answer $H^1_{\text{et}}(X, \mathbb{Z}/n\mathbb{Z}) \simeq (\mathbb{Z}/n\mathbb{Z})^{2g}$. One can also define an even finer “topology”, the fppf topology, which lets one remove the restriction on the characteristic.

Étale cohomology with coefficients in some rings of characteristic zero can be defined by taking an inverse limit. For instance, $H^1_{\text{et}}(X, \mathbb{Z}_\ell) := \varprojlim_n H^1_{\text{et}}(X, \mathbb{Z}/\ell^n\mathbb{Z})$. This is important for an application to the Weil conjectures: see Chapter 7. Other applications of étale and fppf cohomology, to torsors and to Brauer groups of schemes, are given towards the end of Chapter 6.

6.2. Grothendieck topologies

(Reference: [Vis05] §2.3)

Before the notion of a topology on a set was invented, people studied metric spaces. Then people noticed that many properties of metric spaces could be defined without reference to the metric: for many purposes, just knowing which subsets were open was enough. This led to the definition of a topology on a set, in which an arbitrary collection of subsets could be decreed to be the open sets, provided that the collection satisfied some axioms modeled after the theorems about open sets in metric spaces. (See [Moo08] for the history.)

Grothendieck took this one step further by observing that sometimes one does not even need to know the open subsets: for many purposes (for instance, the concept of a sheaf), it suffices to have a notion of open covering. This led to the notion of a Grothendieck topology,
which is usually not a topology in the standard sense. Just as an open set in a topological
space need not be open relative to any metric, an open covering in a Grothendieck topology
need not consist of actual open subsets!

This relaxation of the notion of open covering is necessary to obtain a sufficiently fine
topology on a scheme.

**Remark 6.2.1.** This point of view was used already in Chapter 4.

**Definition 6.2.2.** Let \( C \) be a category. (Our set-theoretic conventions are such that the
collection of objects in each category is a set: see Section A.4.) We consider all families of
morphisms \( \{ U_i \to U \}_{i \in I} \) in \( C \) having a common target. A Grothendieck (pre)topology on \( C \)
is a set \( T \) whose elements are some of these families (the families that do belong to \( T \) are
called the open coverings), satisfying the following axioms:

(i) Isomorphisms are open coverings: If \( U' \to U \) is an isomorphism, then the one-element
family \( \{ U' \to U \} \) belongs to \( T \).

(ii) An open covering of an open covering is an open covering: If \( \{ U_i \to U \} \) belongs to \( T \),
and \( \{ V_{ij} \to U_i \} \) belongs to \( T \) for each \( i \), then \( \{ V_{ij} \to U \} \) belongs to \( T \).

(iii) A base extension of an open covering is an open covering: If \( \{ U_i \to U \} \) belongs to \( T \),
and \( V \to U \) is a morphism, then the fiber products \( V \times_U U_i \) exist and \( \{ V \times_U U_i \to V \} \)
belongs to \( T \).

**Remark 6.2.3.** There is another approach, using sieves, which has advantages and
disadvantages, one disadvantage being that it is farther from geometric intuition. The SGA 4
definition of Grothendieck topology is in terms of sieves [SGA 4, II.1.1]. A Grothendieck
pretopology gives rise to a Grothendieck topology, and all the Grothendieck topologies we
will use arise this way. From now on, we will abuse terminology and call a pretopology a
topology, as is commonly done.

**Definition 6.2.4.** A pair \(( C, T )\) consisting of a category \( C \) and a Grothendieck topology
\( T \) on \( C \) is called a site.

**6.2.1. The Zariski site.** Let \( X \) be a topological space. Let \( C \) be the category whose
objects are the open sets in \( X \), and such that for any \( U, V \in C \),

\[
\text{Hom}(U, V) = \begin{cases} 
\{ i \}, & \text{if } U \subseteq V, \text{ and } i: U \to V \text{ is the inclusion,} \\
\emptyset, & \text{otherwise.}
\end{cases}
\]

Let \( T \) be the collection of families \( \{ U_i \to U \} \) such that \( \bigcup_i U_i = U \). Then \( T \) is a Grothendieck
topology on \( C \), called the classical Grothendieck topology.

Let \( X \) be a scheme. The (small) Zariski site \( X_{\text{Zar}} \) is the site associated to the underlying
topological space sp(\( X \)).
6.2.2. The (small) étale site. Fix a scheme $X$. Take $\mathcal{C}$ to be the category $\text{Et}_X$ of schemes $U$ equipped with an étale morphism $U \to X$, and in which morphisms are $X$-morphisms. (These morphisms will automatically be étale \cite{SP, Tag 02GW}.) Call a family $\{\phi_i : U_i \to U\}$ of morphisms in $\mathcal{C}$ an open covering if $\bigcup_i \phi_i(U_i) = U$ as topological spaces. This defines the (small) étale site $X_{\text{et}}$.

Remark 6.2.5. For the big étale site, one would take $\mathcal{C} = \text{Schemes}_X$. Open coverings are defined as families of étale morphisms $\{\phi_i : U_i \to U\}$ such that $\bigcup U_i \to U$ is étale. The definitions of sheaves and cohomology (see Sections 6.3.2 and 6.4.1) make sense for both the small and the big étale sites. But the cohomology of a big étale sheaf equals the cohomology of its restriction to the small étale site \cite{SP, Tag 03YX}, and the small étale site is easier to work with, so the small étale site is generally preferred.

6.2.3. The (big) fppf and fpqc sites. Fix a scheme $X$. Take $\mathcal{C} = \text{Schemes}_X$. An open covering is a family $\{\phi_i : U_i \to U\}$ of $X$-morphisms such that $\bigcup U_i \to U$ is fppf (respectively, fpqc). This defines the (big) fppf site $X_{\text{fppf}}$ (respectively, the (big) fpqc site $X_{\text{fpqc}}$).

Remark 6.2.6. By the étale site, we will always mean the small étale site. By the fppf or fpqc site, we will always mean the big site. (One reason for this: As mentioned in Section 6.2.2, for the small étale site, morphisms between objects in $\mathcal{C}$ are automatically étale \cite{SP, Tag 02GW}. But if one considered the small fppf site, by taking $\mathcal{C}$ to be the category of fppf $X$-schemes with $X$-morphisms, it would not be automatic that $X$-morphisms between objects in $\mathcal{C}$ were fppf — for example, all $k$-varieties are fppf over $\text{Spec} \ k$, but a $k$-morphism between two $k$-varieties need not be flat. The same problem arises with fpqc.)

6.2.4. Continuous maps of sites.

Definition 6.2.7. A continuous map of sites $(\mathcal{C}', \mathcal{T}') \to (\mathcal{C}, \mathcal{T})$ is a functor in the opposite direction $F : \mathcal{C} \to \mathcal{C}'$ respecting open coverings, in the following sense:

1. for every open covering $\{U_i \to U\}$ in $\mathcal{T}$, collection $\{FU_i \to FU\}$ is an open covering in $\mathcal{T}'$, and
2. for every open covering $\{U_i \to U\}$ in $\mathcal{T}$ and $\mathcal{C}$-morphism $V \to U$, the $\mathcal{C}'$-morphism $F(V \times_U U_i) \to FV \times_{FU} FU_i$ is an isomorphism.

The reversal of direction makes the definition compatible with maps of topological spaces:

Example 6.2.8. Let $f : X' \to X$ be a continuous map of topological spaces. Equip the categories of open subsets of $X$ and $X'$ with the classical Grothendieck topologies to obtain sites $(\mathcal{C}, \mathcal{T})$ and $(\mathcal{C}', \mathcal{T}')$. Then $f$ induces a continuous map of sites $(\mathcal{C}', \mathcal{T}') \to (\mathcal{C}, \mathcal{T})$: the functor $\mathcal{C} \to \mathcal{C}'$ takes an open subset $U$ of $X$ to the open subset $f^{-1}U$ of $X'$.
If a set $X$ is equipped with topologies $\mathcal{T}'$ and $\mathcal{T}$ (in the usual sense), and $\mathcal{T}'$ is finer (more open sets) than $\mathcal{T}$, then the identity map $(X, \mathcal{T}') \to (X, \mathcal{T})$ is a continuous map of topological spaces. Similarly:

**Example 6.2.9.** For any scheme $X$, Proposition 3.8.2 yields continuous maps

$$X_{\text{fppf}} \to X_{\text{et}} \to X_{\text{Zar}}.$$ 

**Remark 6.2.10.** There is a more restrictive notion, called a **morphism of sites**: this is a continuous map of sites for which the inverse image functor on the categories of sheaves is exact: see [SP, Tag OOX1]. The maps in Example 6.2.9 are morphisms of sites.

### 6.3. Presheaves and sheaves

#### 6.3.1. Presheaves.

**Definition 6.3.1.** A **presheaf of abelian groups** (or **abelian presheaf**) $\mathcal{F}$ on a category $\mathcal{C}$ is a functor

$$\mathcal{C}^{\text{opp}} \to \text{Ab}$$

$$U \mapsto \mathcal{F}(U).$$

An element of $\mathcal{F}(U)$ is called a **section** of $\mathcal{F}$ over $U$. A **morphism of presheaves** is a morphism of functors.

**Remark 6.3.2.** Similarly, one may define a **presheaf of sets**, or a **presheaf of groups** (also called **group presheaf**), and so on.

**Example 6.3.3.** If $\mathcal{C}$ is the category of open subsets of a topological space (Section 6.2.1), then we get the same notion of presheaf as in [Har77 II.1]. (The condition there that $\mathcal{F}(\emptyset) = 0$ is unnatural and should be deleted.) For this reason, for arbitrary $\mathcal{C}$, the homomorphism $\mathcal{F}(U) \to \mathcal{F}(V)$ induced by a morphism $V \to U$ of $\mathcal{C}$ is called the **restriction** from $U$ to $V$ and denoted $s \mapsto s|_V$, even though $V$ might not be an actual subset of $U$.

**Example 6.3.4.** Let $A$ be an abelian group. The **constant presheaf** $A$ on a category $\mathcal{C}$ is the functor $\mathcal{F}$ such that $\mathcal{F}(U) = A$ for all $U \in \mathcal{C}$, and such that $\mathcal{F}$ takes each morphism in $\mathcal{C}$ to the identity $A \to A$.

#### 6.3.2. Sheaves.

**Definition 6.3.5.** Let $A, B, C$ be sets, and let $f: A \to B$, $g: B \to C$, and $h: B \to C$ be functions. Then

$$A \xrightarrow{f} B \xrightarrow{g} C$$

is called **exact** if
(i) $f$ is injective, and
(ii) $f(A)$ equals the equalizer $\{b \in B : g(b) = h(b)\}$ of $g$ and $h$.

**Example 6.3.6.** If $A, B, C$ are abelian groups, and $f, g, h$ are homomorphisms, then
$$A \xrightarrow{f} B \xrightarrow{g} C$$
is exact if and only if the sequence of abelian groups
$$0 \to A \xrightarrow{f} B \xrightarrow{g-h} C$$
is exact.

**Definition 6.3.7.** Let $\mathcal{F}$ be a presheaf on a site $(\mathcal{C}, \mathcal{T})$. Then $\mathcal{F}$ is a sheaf if and only if
\[(6.3.8) \quad \mathcal{F}(U) \to \prod_i \mathcal{F}(U_i) \Rightarrow \prod_{i,j} \mathcal{F}(U_i \times_U U_j)\]
is exact for all open coverings $\{U_i \to U\}$ in $\mathcal{T}$. (Here the two arrows on the right correspond to the two projections, from $U_i \times_U U_j$ to $U_i$ and to $U_j$.) A morphism of sheaves $\mathcal{F} \to \mathcal{G}$ is simply a morphism of presheaves.

**Example 6.3.9.** If $\mathcal{T}$ is the classical Grothendieck topology on a topological space, then the sheaf condition says
(i) an element $s \in \mathcal{F}(U)$ is determined by its restriction to an open covering, and
(ii) given elements $s_i \in \mathcal{F}(U_i)$ for an open covering $\{U_i \to U\}$ that are compatible (they agree on pairwise intersections), one can glue to obtain an element $s \in \mathcal{F}(U)$ whose restriction to $U_i$ is $s_i$ for each $i$.

**Remark 6.3.10.** Suppose that $\{U_i \to U\}$ is an open covering in one of the sites $X_{et}$, $X_{fppf}$, or $X_{fpqc}$. Let $U' = \coprod U_i$ and $U'' = U' \times_U U'$. If a presheaf $\mathcal{F}$ already satisfies $\mathcal{F}(U') = \prod \mathcal{F}(U_i)$, then exactness of $(6.3.8)$ is equivalent to exactness for the open covering consisting of the single morphism $U' \to U$, the exactness of
\[(6.3.11) \quad \mathcal{F}(U) \to \mathcal{F}(U') \Rightarrow \mathcal{F}(U'')\].

**Definition 6.3.12.** An abelian sheaf is a sheaf of abelian groups. A group sheaf is a sheaf of groups.

**6.3.3. Examples of sheaves.** Here we show that some presheaves arising commonly in algebraic geometry are fpqc sheaves. The sheaf property in each case turns out to be a consequence of fpqc descent.

**Definition 6.3.13.** Let $X$ be a scheme. Let $\mathcal{C}$ be a subcategory of $\textbf{Schemes}_X$. Let $\mathcal{F}$ be a quasi-coherent $\mathcal{O}_X$-module, so in particular, $\mathcal{F}$ is a sheaf on $X_{Zar}$. Define a presheaf $\mathcal{F}_C$.
on \( C \) by
\[
\mathcal{F}_C(U) := (p^* \mathcal{F})(U) = \text{Hom}(p^* \mathcal{O}_X, p^* \mathcal{F})
\]
for each object \( U \overset{\varphi}{\to} X \) of \( C \).

**Example 6.3.14.** Take \( C \) to be the underlying category of \( X_{\text{fpqc}} \); then Definition 6.3.13 extends a quasi-coherent \( \mathcal{O}_X \)-module \( \mathcal{F} \) to a presheaf \( \mathcal{F}_{\text{fpqc}} \) on \( X_{\text{fpqc}} \).

**Proposition 6.3.15.** Let \( \mathcal{F} \) be a quasi-coherent \( \mathcal{O}_X \)-module on a scheme \( X \). Then the presheaf \( \mathcal{F}_{\text{fpqc}} \) on \( X_{\text{fpqc}} \) in Example 6.3.14 is an abelian sheaf. (And hence the same is true on \( X_{\text{Zar}}, X_{\text{et}}, \) and \( X_{\text{fppf}} \). Of course, this is trivial for \( X_{\text{Zar}} \), on which \( \mathcal{F}_{\text{Zar}} = \mathcal{F} \).)

**Proof.** By Remark 6.3.10, it suffices to check exactness of (6.3.11) for each fpqc morphism \( p: S' \to S \) of \( X \)-schemes. For this, we may replace \( \mathcal{F} \) by its restriction to \( S \), which we now rename \( \mathcal{F} \). Let \( S'' = S' \times_S S' \), and let \( q: S'' \to S \) be the projection. Then (6.3.11) for \( \mathcal{F}_{\text{fpqc}} \) is
\[
\text{Hom}(\mathcal{O}_S, \mathcal{F}) \to \text{Hom}(p^* \mathcal{O}_S, p^* \mathcal{F}) \to \text{Hom}(q^* \mathcal{O}_S, q^* \mathcal{F}).
\]
This is exact, because Theorem 4.2.3 implies that the functor from quasi-coherent \( S \)-modules to quasi-coherent \( S' \)-modules with descent data is fully faithful. \( \square \)

**Proposition 6.3.16.** Let \( S \) be a scheme, and let \( X \) and \( Y \) be \( S \)-schemes. The functor \( U \mapsto \text{Hom}_U(X_U, Y_U) \) is a sheaf of sets on \( S_{\text{fpqc}} \), denoted \( \text{Hom}(X,Y) \).

**Proof.** Remark 6.3.10 lets us reduce to showing that for each fpqc morphism \( p: U' \to U \) of \( S \)-schemes, if \( U'' := U' \times_U U' \), then
\[(6.3.17) \quad \text{Hom}_U(X_U, Y_U) \to \text{Hom}_{U'}(X_{U'}, Y_{U'}) \to \text{Hom}_{U''}(X_{U''}, Y_{U''})
\]
is exact. The map from \( \text{Hom}_U(X_U, Y_U) \) to the equalizer sends an \( U \)-morphism \( X_U \to Y_U \) to the morphism between the associated \( U' \)-schemes with descent data; this map is a bijection by Theorem 4.3.5(i). Thus (6.3.17) is exact. \( \square \)

**Corollary 6.3.18.** Let \( S \) be a scheme, and let \( X \) be an \( S \)-scheme. The functor \( U \mapsto \text{Aut}_U(X_U) \) is a group sheaf on \( S_{\text{fpqc}} \).

**Proof.** By Proposition 6.3.16, the monoid presheaf \( \text{Hom}(X,X) \) is a sheaf; take the subgroup of invertible elements in each monoid. \( \square \)

Recall from Definition 2.3.3 that if \( X \) is a scheme, and \( Y \) is an \( X \)-scheme, then the functor of points \( h_Y: \text{Schemes}_X^{\text{opp}} \to \text{Sets} \) is defined by \( h_Y(U) := \text{Hom}_X(U,Y) \).

**Proposition 6.3.19.** Let \( S \) be a scheme, and let \( X \) be an \( S \)-scheme. Then the functor of points \( h_X \), viewed as a presheaf on the fpqc site \( S_{\text{fpqc}} \), is a sheaf (and hence the same is true for the Zariski, étale, fppf sites).

157
Proof. Remark 6.3.10 lets us reduce to showing that for each fpqc morphism $p: U' \to U$ of $S$-schemes, if $U'' := U' \times_U U'$, then

$$\text{Hom}_S(U, X) \to \text{Hom}_S(U', X) \Rightarrow \text{Hom}_S(U'', X)$$

is exact. Applying Proposition 2.3.15 to each term rewrites this as

$$\text{Hom}_{U}(U, X_U) \to \text{Hom}_{U'}(U', X_{U'}) \Rightarrow \text{Hom}_{U''}(U'', X_{U''}),$$

which, as a special case of (6.3.17), is exact. □

Remark 6.3.20. If $G$ is a group scheme over $X$, then $h_G$ is a group sheaf. We sometimes write $G$ when we mean the associated sheaf. For instance, the abelian sheaf $G_a$ on $X_{\text{Zar}}$ is the same as $\mathcal{O}_X$, and the abelian sheaf $G_a$ on $X_{\text{fpqc}}$ is the same as $(\mathcal{O}_X)_{\text{fpqc}}$. Another example: the abelian sheaf $G_m$ on $X_{\text{fpqc}}$ sends each $U$ to $\mathcal{O}_U(U)^\times$.

6.3.4. Sheafification.

Definition 6.3.21. A sheafification of a presheaf $\mathcal{F}$ is a sheaf $\mathcal{F}^+$ equipped a morphism $i: \mathcal{F} \to \mathcal{F}^+$ such that every presheaf morphism from $\mathcal{F}$ to a sheaf factors uniquely through $i$.

The definition implies that a sheafification is unique if it exists.

Proposition 6.3.22. (cf. [Har77, II.1.2]) Let $\mathcal{F}$ be a presheaf on a site. Then the sheafification of $\mathcal{F}$ exists.

Sketch of proof. Let $\mathcal{F}$ be a presheaf. Call two sections $s, t \in \mathcal{F}(U)$ equivalent if there exists an open covering $\{U_i \to U\}$ such $s|_{U_i} = t|_{U_i}$ for all $i$. This defines an equivalence relation. Let $\mathcal{F}_1(U)$ be the set of equivalence classes. Then $\mathcal{F}_1$ is another presheaf.

Loosely speaking, a section of $\mathcal{F}^+$ is something that is locally (for some open covering in the Grothendieck topology) a section of $\mathcal{F}_1$. More precisely, one should define $\mathcal{F}^+(U) := \check{H}^0(U, \mathcal{F}_1)$, using the notation of Section 6.4.4. □

Remark 6.3.23. The Zariski, étale, and fppf topologies are independent of the choice of universe in the sense that

(1) any open covering can be refined to one in which all the morphisms $U_i \to U$ are open immersions, étale morphisms of finite presentation, or flat morphisms of finite presentation, respectively, and

(2) for any $U$, the isomorphism classes of such morphisms form a set that does not grow as one enlarges the universe.

The same is not true for fpqc morphisms: for instance over $\text{Spec} k$, one has the fpqc morphism $\text{Spec} L \to \text{Spec} k$, where $L$ is the purely transcendental extension $k(\{t_i : i \in I\})$ for a set $I$ of arbitrary cardinality, bounded only by the size of the universe. In the fpqc topology, even the sheafification of a presheaf can depend on the choice of universe [Wat75, Theorem 5.5, 158]
Remark (c)]. Because of this, in situations requiring sheafification, the fppf topology is preferred over the fpqc topology.

**Definition 6.3.24.** The constant presheaf $A$ (on a Zariski, étale, fppf, or fpqc site) is usually not a sheaf, so we define the constant sheaf to be the sheafification of the constant presheaf.

**6.3.5. Exact sequences.**

**Definition 6.3.25.** Let $\alpha : \mathcal{G} \to \mathcal{H}$ be a morphism of abelian sheaves on a site. Then the kernel $\ker(\alpha)$ is defined as the presheaf $U \mapsto \ker(\mathcal{G}(U) \to \mathcal{H}(U))$. It turns out to be a sheaf.

**Definition 6.3.26.** A sequence of abelian sheaves

$$\mathcal{F} \xrightarrow{\alpha} \mathcal{G} \xrightarrow{\beta} \mathcal{H}$$

on a site $(\mathcal{C}, \mathcal{T})$ with $\beta \circ \alpha = 0$ is called exact (at $\mathcal{G}$) if $\ker(\beta)$ is a sheafification of the presheaf image of $\alpha$ defined by $U \mapsto \text{im}(\mathcal{F}(U) \to \mathcal{G}(U))$ (for the natural morphism from this presheaf image to $\ker(\beta)$). In other words, the sequence is exact if for each $U \in \mathcal{C}$ and for each $g \in \mathcal{G}(U)$, we have

$$\beta(g) = 0 \iff \exists \text{ open covering } \{U_i \to U\} \text{ and } f_i \in \mathcal{F}(U_i) \text{ with } \alpha(f_i) = g|_{U_i}.$$ 

**Remark 6.3.27.** Let $A, B, C$ be fppf group schemes over a scheme $S$. A sequence

$$A \to B \to C$$

of homomorphisms of group schemes over $S$ is exact in the sense of Definition [5.1.18] if and only if the associated sequence of sheaves on $S_{\text{fppf}}$ is exact. (One can make sense of this even if $A, B$, and $C$ are noncommutative.)

**6.4. Cohomology**

**6.4.1. The derived functor definition.** In this section we fix a scheme $X$, and an element $\bullet$ of $\{\text{Zar, et, fppf}\}$, so that $X_{\bullet}$ is one of the sites we have defined. It turns out that the category of abelian sheaves on $X_{\bullet}$ has enough injectives.

**Definition 6.4.1.** (cf. [Har77, III.1]) For $q \in \mathbb{N}$, define the functor

$$\{\text{abelian sheaves on } X_{\bullet}\} \to \text{Ab}$$

$$\mathcal{F} \mapsto H^q(X, \mathcal{F})$$
as the $q^{th}$ right derived functor of the (left exact) global sections functor

\[ \{ \text{abelian sheaves on } X_\bullet \} \rightarrow \text{Ab} \]

\[ \mathcal{F} \mapsto \mathcal{F}(X). \]

If $\mathcal{F}$ is an abelian sheaf on $X_\bullet$, then the abelian group $H^q_\bullet(X, \mathcal{F})$ is called the $q^{th}$ cohomology group of $\mathcal{F}$.

In particular, for any exact sequence of abelian sheaves on $X_\bullet$

\[ 0 \rightarrow \mathcal{F} \rightarrow \mathcal{G} \rightarrow \mathcal{H} \rightarrow 0 \]

we get a long exact sequence

\[ 0 \rightarrow H^0_\bullet(X, \mathcal{F}) \rightarrow H^0_\bullet(X, \mathcal{G}) \rightarrow H^0_\bullet(X, \mathcal{H}) \rightarrow \]

\[ H^1_\bullet(X, \mathcal{F}) \rightarrow H^1_\bullet(X, \mathcal{G}) \rightarrow H^1_\bullet(X, \mathcal{H}) \rightarrow \cdots \]

**Remark 6.4.2.** For each abelian sheaf $\mathcal{F}$ on $X_\bullet = (\mathcal{C}, \mathcal{T})$ and for each “open subset” $U \in \mathcal{C}$, one can define $H^q_\bullet(U, \mathcal{F})$ by taking the derived functors of $\Gamma(U, -)$. There is a canonical “pullback” homomorphism $H^q_\bullet(X, \mathcal{F}) \rightarrow H^q_\bullet(U, \mathcal{F})$. In fact,

\[ \mathcal{C}^{\text{opp}} \rightarrow \text{Ab} \]

\[ U \mapsto H^q_\bullet(U, \mathcal{F}) \]

defines a presheaf called $H^q(U, \mathcal{F})$.

Alternatively, one can restrict $\mathcal{F}$ to the site $U_\bullet$ and take $H^q_\bullet(U, \mathcal{F}|_U)$. There is a canonical isomorphism

\[ H^q_\bullet(U, \mathcal{F}) \simeq H^q_\bullet(U, \mathcal{F}|_U), \]

because one can show that the functor $\mathcal{F} \mapsto \mathcal{F}|_U$ takes injective sheaves on $X_\bullet$ to injective sheaves on $U_\bullet$: see [Mi80] III.1.10 and III.1.11].

**6.4.2. Étale cohomology and limits.** Exercise 1.17 stated that for a direct limit of fields $K = \lim K_\alpha$, we have $\text{Br } K = \lim \text{Br } K_\alpha$. There are various versions of this for schemes and étale cohomology, discussed in [SGA 4\text{II}] VII, §5]. Here is one:

**Theorem 6.4.3.** Let $(X_i)_{i \in I}$ be a filtered inverse system of schemes. Suppose that the $X_i$ are quasi-compact and quasi-separated, and that the morphisms in the system are affine.

(a) The limit $X := \varprojlim X_i$ exists in the category of schemes.
(b) Suppose that $0 \in I$, and $G_0$ is a commutative group scheme of finite presentation over $X_0$. For $i \geq 0$, let $G_i = G_0 \times_{X_0} X_i$. Let $G = G_0 \times_{X_0} X$. For each $q \in \mathbb{N}$, the natural homomorphism
\[
\lim_{\rightarrow} H^q_{\text{et}}(X_i, G_i) \longrightarrow H^q_{\text{et}}(X, G)
\]
is an isomorphism.

**Proof.** See [SGA 4II, VII, Corollaire 5.9]. □

### 6.4.3. Étale cohomology and Galois cohomology.

For this section, we fix a field $k$ and a separable closure $k_s$. By Proposition 3.5.35, the only field extensions $L$ of $k$ for which $\text{Spec} L \rightarrow \text{Spec} k$ is étale are the finite separable extensions.

**Definition 6.4.4.** If $\mathcal{F}$ is a sheaf on $(\text{Spec} k)_{\text{et}}$, define $\mathcal{F}(k_s) := \varprojlim \mathcal{F}(L)$, where the direct limit is over all finite separable extensions $L/k$ contained in $k_s$, and $\mathcal{F}(L)$ means $\mathcal{F}(\text{Spec} L)$.

**Remark 6.4.5.** We get the same direct limit if we take only finite Galois extensions $L/k$. Then $\mathcal{G}_k$ acts continuously on each $L$, hence on each $\mathcal{F}(L)$. Thus $\mathcal{F}(k_s)$ is naturally a $\mathcal{G}_k$-set.

**Theorem 6.4.6 (Étale cohomology over a field).**

(i) The functor
\[
\{ \text{sheaves of sets on } (\text{Spec} k)_{\text{et}} \} \longrightarrow \{ \mathcal{G}_k\text{-sets} \}
\]
\[\mathcal{F} \longmapsto \mathcal{F}(k_s)\]
is an equivalence of categories. The global section functor $\mathcal{F} \mapsto \mathcal{F}(k)$ corresponds to the functor that takes a $\mathcal{G}_k$-set $M$ to the set of invariants $M^{\mathcal{G}_k}$.

(ii) The equivalence in part (i) restricts to an equivalence
\[
\{ \text{abelian sheaves on } (\text{Spec} k)_{\text{et}} \} \longrightarrow \{ \mathcal{G}_k\text{-modules} \}
\]

(iii) There are natural isomorphisms
\[
H^q_{\text{et}}(\text{Spec} k, \mathcal{F}) \simeq H^q(\mathcal{G}_k, \mathcal{F}(k_s))
\]
for all $q \in \mathbb{N}$.

**Proof.**

(i) We describe an inverse functor. Let $S$ be a $\mathcal{G}_k$-set. For each finite separable extension $L/k$ contained in $k_s$, define $\mathcal{F}(L) = S^{\text{Gal}(k_s/L)}$. By Proposition 3.5.35, every étale $k$-scheme $U$ is a disjoint union of $k$-schemes of the form $\text{Spec} L$, and we define $\mathcal{F}(U)$ as
the corresponding product of the sets \( \mathcal{F}(L) \). The restriction morphisms are products of inclusion morphisms

\[
\mathcal{F}(L) = S^{\text{Gal}(k_s/L)} \hookrightarrow S^{\text{Gal}(k_s/M)} = \mathcal{F}(M)
\]

for finite separable extensions \( L/M \) of finite separable extensions of \( k \) contained in \( k_s \).

The rest of the proof of (i) is easy.

(ii) This is obvious from (i).

(iii) Under (ii), the global sections functor corresponds to the \( \mathfrak{S}_k \)-invariants functor. Take derived functors on both sides. \( \square \)

### 6.4.4. Čech cohomology.

Let \( \mathcal{U} = \{ U_i \to U \}_{i \in I} \) be an open covering on some site \( \mathcal{S} \). For \( (i_0, \ldots, i_p) \in I^{p+1} \), define

\[
U_{i_0 \ldots i_p} := U_{i_0} \times U_{i_1} \times \cdots \times U_p
\]

If \( (i_0, \ldots, i_p) \in I^{p+1} \) and \( j \in \{0, \ldots, p\} \), then forgetting the \( j \)th factor gives a projection

\[
U_{i_0 \ldots i_p} \to U_{i_0 \ldots \hat{i}_j \ldots i_p},
\]

where the \( \hat{\cdot} \) means that that index is omitted. We obtain

\[
\prod_{i_0} U_{i_0} \leftarrow \prod_{i_0 i_1} U_{i_0 i_1} \leftarrow \prod_{i_0 i_1 i_2} U_{i_0 i_1 i_2} \leftarrow \cdots.
\]

Let \( \mathcal{F} \) be an abelian presheaf on \( \mathcal{S} \). Then we obtain

\[
\prod_{i_0} \mathcal{F}(U_{i_0}) \leftarrow \prod_{i_0 i_1} \mathcal{F}(U_{i_0 i_1}) \leftarrow \prod_{i_0 i_1 i_2} \mathcal{F}(U_{i_0 i_1 i_2}) \leftarrow \cdots.
\]

Relabel these products as \( C^0, C^1, \) and so on, and combine each stack of arrows by taking their alternating sum to obtain homomorphisms \( d^q \):

\[
C^0 \xrightarrow{d^0} C^1 \xrightarrow{d^1} C^2 \xrightarrow{d^2} \cdots.
\]

**Definition 6.4.7.** The elements of \( C^q, \ker(d^q), \text{im}(d^q-1) \), respectively, are called Čech \( q \)-cochains, Čech \( q \)-cocycles, and Čech \( q \)-coboundaries.

One can check that the composition \( d^q \circ d^{q-1} \) of any two successive homomorphisms is zero, so we have a complex. Take the cohomology groups of this complex, and denote them

\[
\check{H}^q(\mathcal{U}, \mathcal{F}) = \frac{\ker d^q}{\text{im} d^{q-1}}.
\]

where we interpret \( \text{im} d^{q-1} \) as 0 if \( q = 0 \).

**Warning 6.4.8.** In the case of the Zariski site, one obtains the same group \( \check{H}^q(\mathcal{U}, \mathcal{F}) \) if one fixes a well ordering on \( I \) and takes products only over \( (p + 1) \)-tuples satisfying \( i_0 < i_1 < \cdots < i_p \), as in [Har77, III.§4]. But for the étale site and other sites, this approach gives the wrong cohomology groups because the fiber products contain new information even when some of the indices are equal.
**Definition 6.4.9.** Let $U = \{U_i \to U\}_{i \in I}$ and $V = \{V_j \to U\}_{j \in J}$ be open coverings with respect to some site $(\mathcal{C}, T)$. Then $U$ is called a refinement of $V$ if there exists a map $\pi : I \to J$ and a morphism $U_i \to V_{\pi(i)}$ for each $i \in I$.

If $U$ is a refinement of $V$, then there is an induced morphism $\check{\mathcal{H}}^q(V, \mathcal{F}) \to \check{\mathcal{H}}^q(U, \mathcal{F})$ for each $q \geq 0$.

**Definition 6.4.10.** Let $\mathcal{F}$ be an abelian presheaf on a site $(\mathcal{C}, T)$, let $U \in \mathcal{C}$, and let $q \in \mathbb{N}$. The $q^{th}$ Čech cohomology group of $U$ with coefficients in $\mathcal{F}$ is

$$\check{\mathcal{H}}^q(U, \mathcal{F}) := \lim\limits_{\rightarrow} \check{\mathcal{H}}^q(U, \mathcal{F}),$$

where the direct limit is taken over all open coverings of $U$, ordered by refinement.

**Warning 6.4.11.** The abelian groups $\check{\mathcal{H}}^q(U, \mathcal{F})$ and $H^q(U, \mathcal{F})$ need not be isomorphic.

**Proposition 6.4.12.** If $\mathcal{F}$ is an abelian sheaf on a site $(\mathcal{C}, T)$, and $U \in \mathcal{C}$, then we have

$$\check{\mathcal{H}}^0(U, \mathcal{F}) \cong H^0(U, \mathcal{F}) = \mathcal{F}(U),$$

$$\check{\mathcal{H}}^1(U, \mathcal{F}) \cong H^1(U, \mathcal{F}),$$

$$\check{\mathcal{H}}^2(U, \mathcal{F}) \hookrightarrow H^2(U, \mathcal{F}).$$

**Sketch of proof.** The first line is immediate from the definition of $\check{\mathcal{H}}^0(U, \mathcal{F})$ and the sheaf property of $\mathcal{F}$. For the second and third lines, let $\mathcal{H}(\mathcal{F})$ be the presheaf of Remark 6.4.2 and use Proposition 6.7.1 for the spectral sequence of Čech cohomology $E_2^{pq} := \check{\mathcal{H}}^p(U, \mathcal{H}^q(\mathcal{F})) \Rightarrow H^{p+q}(U, \mathcal{F})$, and use the fact $\check{\mathcal{H}}^0(U, \mathcal{H}^q(\mathcal{F})) = 0$; see [Sha72, pp. 200–201].

**Theorem 6.4.13 (M. Artin).** Let $X$ be a quasi-compact scheme such that every finite subset of $X$ is contained in an affine open subset. (This is automatic if $X$ is quasi-projective over an affine scheme.) Let $\mathcal{F}$ be an abelian sheaf on $X_{et}$. Then there are canonical isomorphisms $\check{H}^q_{et}(X, \mathcal{F}) \cong H^q_{et}(X, \mathcal{F})$ for all $q \in \mathbb{N}$.

**Proof.** See the original reference [Art71], or see [Mil80, III.2.17].

**Important Remark 6.4.14.** In group cohomology, one can define $H^0(G, A)$ and $H^1(G, A)$ even when the group $A$ is nonabelian. Similarly, one can define $\check{H}^0(X, \mathcal{F})$ and $\check{H}^1(X, \mathcal{F})$ for a presheaf $\mathcal{F}$ of possibly nonabelian groups: see [Mil80, p. 122].

### 6.5. Torsors over an arbitrary base

(Reference: [Mil80, III.§4])

Torsors under a group scheme $G$ over a general base scheme can be thought of as families of torsors. (In differential geometry, such objects are sometimes called principal $G$-bundles.)
6.5.1. Definition of torsors.

**Definition 6.5.1.** Let \( G \to S \) be an fppf group scheme. An \( G \)-torsor over \( S \) (or simply \( G \)-torsor) is an fppf \( S \)-scheme \( X \) equipped with a right \( G \)-action

\[
X \times_S G \to X
\]
such that one of the following equivalent conditions holds:

(i) There exists an fppf base change \( S' \to S \) such that

\[
X_{S'} \text{ with its right } G_{S'} \text{-action}
\]
is isomorphic over \( S' \) to

\[
G_{S'} \text{ with the right translation } G_{S'} \text{-action}.
\]

(ii) The morphism

\[
X \times_S G \to X \times_S X
\]

\[
(x, g) \mapsto (x, xg)
\]
is an isomorphism.

**Proof of equivalence.**

\(\Rightarrow\) Take \( S' = X \). Then \(\Rightarrow\) backwards says that \( S' \times_S X \simeq S' \times_S G \). In other words, \( X_{S'} \simeq G_{S'} \). Moreover, the right \( G \)-actions correspond: this is simply the formula \((xg)h = x(gh)\) coming from the definition of right \( G \)-action on \( X \).

\(\Rightarrow\) Let \( \phi \) be the morphism

\[
X \times_S G \to X \times_S X
\]

\[
(x, g) \mapsto (x, xg).
\]

Base extend \( \phi \) by \( S' \to S \) and use \(\Rightarrow\) to replace \( X_{S'} \) by \( G_{S'} \): this gives

\[
\phi_{S'} : G_{S'} \times_{S'} G_{S'} \to G_{S'} \times_{S'} G_{S'}
\]

\[
(x, g) \mapsto (x, xg)
\]

Since \( G \) is a group scheme, \( \phi_{S'} \) is an isomorphism. But \( S' \to S \) is fppf, hence fpqc, so fpqc descent (Theorem 4.3.7(ii)) implies that \( \phi \) was an isomorphism to begin with.

**Remark 6.5.2.** Let \( X \) be an \( G \)-torsor over \( S \). By fpqc descent (Theorem 4.3.7(ii)), many properties of \( G \) are inherited by \( X \). For instance, if \( G \) is smooth over \( S \), then \( X \) is smooth over \( S \).

6.5.2. Trivial torsors. We have the following analogue of Proposition 5.12.14.
Proposition 6.5.3. Let $G \to S$ be an fppf group scheme. Let $X$ be an $G$-torsor over $S$. The following are equivalent:

(i) $X$ is isomorphic to the trivial torsor ($G$ with right translation action).
(ii) $X(S) \neq \emptyset$; i.e., $X \to S$ admits a section.
(iii) $X$ corresponds to the neutral element of $\tilde{H}^1_{fppf}(S, G)$ (see Section 6.5.5).

Proof. 

(i) $\Rightarrow$ (ii): This is because $G \to S$ has the identity section.

(ii) $\Rightarrow$ (i): The second definition of torsor gives us an isomorphism $X_X \simeq G_X$ of $G_X$-torsors over $X$. If we have a section $S \to X$, we can further base extend by this to get $X_S \simeq G_S$; in other words, $X \simeq G$ as $G$-torsors over $S$.

(i) $\Leftrightarrow$ (iii): This is by definition of the correspondence given in Section 6.5.5. $\square$

6.5.3. Examples. Generalizing Example 5.12.9, we have:

Example 6.5.4. Let $G$ be a finite group. A Galois covering $S' \to S$ with Galois group $G$ in the sense of Remark 4.4.7 is the same thing as an torsor under the constant $S$-group scheme corresponding to $G$.

Example 6.5.5. Let $\mathcal{L}$ be an invertible sheaf on a scheme $S$. Let $L \to S$ be the corresponding line bundle, i.e., $L := \text{Spec} \text{Sym}(\mathcal{L})$ (some authors use $\mathcal{L}^{-1}$ instead). Thus there exists a finite cover of $S$ by open subsets $U$ such that $L_U \to U$ is isomorphic to $U \times \mathbb{A}^1 \to U$. Let $Z$ be the zero section of the line bundle, viewed as a closed subscheme of $L$. Then the open subscheme $X := L - Z$ of $L$ is an $\mathbb{G}_{m, S}$-torsor over $S$. This torsor is trivial if and only if $L \simeq \mathcal{O}_S$.

Example 6.5.6. The same construction as in Example 6.5.5 associates to any locally free rank $n$ sheaf a $GL_n$-torsor.

6.5.4. Torsor sheaves. Recall that a scheme gives rise to its functor of points, which is a sheaf of sets. Thus sheaves of sets can be viewed as a generalization of schemes. Similarly group sheaves can be viewed as a generalization of group schemes.

Definition 6.5.7. Let $G$ be a group sheaf on a site with final object $S$ (e.g., the étale site on a scheme $S$). A $G$-torsor sheaf $T$ is a sheaf of sets equipped with a right action $T(U) \times G(U) \to T(U)$ for each $U \in \mathcal{C}$, functorially in $U$, such that there exists an open covering $\{U_i \to S\}$ and an isomorphism $T|_{U_i} \to G|_{U_i}$ identifying the right $G|_{U_i}$-action on $T|_{U_i}$ with the right action of $G|_{U_i}$ on itself by translations.

Definition 6.5.8. Say that an open covering $\{V_i \to S\}$ trivializes a torsor sheaf $T$ if there exist isomorphisms $T|_{V_i} \simeq G|_{V_i}$ respecting the right $G$-actions for all $i$. 

165
6.5.5. **Torsors and $H^1$**. Section 5.12 used Galois descent to show that (scheme) torsors under a smooth algebraic group $G$ over $k$ are classified by $H^1(k,G)$. The generalization to base schemes $S$ other than Spec $k$ breaks up into two steps:

1. Relate $\check{H}^1(S, G)$ to torsor sheaves. By definition, giving a sheaf locally is the same as giving a sheaf, so the question of descent does not come up.
2. Ask whether torsor sheaves are represented by (scheme) torsors. This is the delicate part, because it involves descent of schemes, which is not always effective.

The following handles the first step:

**Proposition 6.5.9.** Let $G$ be a group sheaf on a site with final object $S$. Then there is an isomorphism of pointed sets

$$\{\text{G-torsor sheaves}\} \cong \check{H}^1(S, G).$$

**Proof.** The construction is similar to the construction of a 1-cocycle from a twist in Remark 4.5.4 as we now demonstrate.

Let $T$ be a $G$-torsor sheaf. Choose an open covering $U := \{U_i \to S\}$ and isomorphisms $f_i: G|_{U_i} \cong T|_{U_i}$. Then on the overlaps $U_{i,j} = U_i \times_S U_j$ the transition maps $f_i^{-1}f_j: G|_{U_{i,j}} \cong G|_{U_{i,j}}$ are given by left multiplication by some $g_{i,j} \in G(U_{i,j})$. The $g_{i,j}$ form a Čech 1-cocycle. Changing the isomorphisms $f_i$ corresponds to replacing the 1-cocycle by a cohomologous one. In this way, we get an isomorphism of pointed sets

$$\{\text{G-torsor sheaves trivialized by } U\} \cong \check{H}^1(U, \mathcal{F}).$$

Taking the direct limit over all open coverings gives the desired isomorphism. \hfill $\square$

Fortunately, it is often true that torsor sheaves are represented by torsor schemes:

**Theorem 6.5.10.** Let $G$ be an fppf group scheme over a locally noetherian scheme $S$. Then we have

$$\{\text{G-torsors}\} \cong \{\text{G-torsor sheaves}\} \cong \check{H}^1_{\text{fppf}}(S, G) \cong H^1_{\text{fppf}}(S, G),$$

where the last term and the last isomorphism should be included only if $G$ is commutative (since otherwise $H^1_{\text{fppf}}(S, G)$ is not defined). Moreover, the first injection is a bijection in any of the following cases:

(i) $G \to S$ is an affine morphism.
(ii) $G$ is of finite presentation and separated over $S$, and $\dim S \leq 1$.
(iii) $G \to S$ is an abelian scheme, and $G$ is locally factorial.

**Proof.** For the last isomorphism, see [Mi80, III.4.7]. Case (i) follows from Theorem 4.3.5. Case (ii) follows from [Ray70b, Théorème XI.3.1(1)] in the smooth case, and
Ana73 Théorème 4.D] in general. Case (iii) is a special case of Ray70b Théorème XI.3.1(2). In Ray70b XI and XIII one can find other hypotheses that guarantee that the injection is a bijection. On the other hand, Ray70b XII contains some counterexamples. □

Remark 6.5.11. To avoid the delicate issue of representability by a scheme, one can enlarge the category of schemes to the category of algebraic spaces. Under the hypotheses of Theorem 6.5.10 (or the weaker hypothesis that $G \to S$ is a group algebraic space over an algebraic space), a $G$-torsor sheaf for the fppf topology on $S$ is always represented by a $G$-torsor algebraic space, because the definition of algebraic space is fppf local: see LMB00 10.4.2 and SP Tag 04SK.

To simplify notation, we write $H^1(S,G)$ for $\check{H}^1_{fppf}(S,G)$ from now on.

6.5.6. Geometric operations on torsors over schemes. The notions of inner twist, inverse torsors, contracted product, and subtraction of torsors in Sections 5.11 and 5.12.5 can be generalized to base schemes $S$ other than $\text{Spec} k$. The idea in each case is that the construction are easy in the case where the torsor $T \to S$ involved is trivial, so we do the construction after fppf base change, and then descend the result to $S$. We will only state the results here: see Sko01 pp. 20–21 for more details.

Let $G$ be an fppf group scheme over a scheme $S$. Assume that $G$ is affine over $S$: this is to ensure that descent is effective, so that we can work with torsors as schemes instead of only as sheaves.

6.5.6.1. Inner twists. Given $\tau \in H^1(S,G)$ (perhaps the class of a $G$-torsor $T \to S$), one obtains another fppf group scheme $G^\tau$ affine over $S$.

6.5.6.2. Inverse torsors. Let $T \to S$ be a right $G$-torsor, and let $\tau$ be its class in $H^1(S,G)$. Then $T$ may be viewed as a $G^\tau$-$G$-bitorsor, and the same $S$-scheme may be viewed as a $G$-$G^\tau$-bitorsor $T^{-1}$.

6.5.6.3. Contracted products. Let $G \to S$ be an fppf group scheme. Let $X$ be an $S$-scheme that is affine over $S$ and equipped with a right $G$-action (but $X$ is not necessarily a torsor). Let $T$ be a left $G$-torsor over $S$. The contracted product $X \times^G T$ is the quotient of $X \times_S T$ by the $G$-action in which $g \in G$ acts by $(x,t) \mapsto (xg, g^{-1}t)$. The result is an $S$-scheme that is affine over $S$.

6.5.6.4. Subtraction of torsors. Let $Z$ and $T$ be two right $G$-torsors over $S$. Let $\tau = [T] \in H^1(S,G)$ be their classes. Then $Z \times^G T^{-1}$ is a right $G^\tau$-torsor over $S$.

Example 6.5.12 (Twisted torsor). Let $k$ be a field. Let $S$ be a $k$-scheme. Let $G$ be an affine algebraic group over $k$. Then $G_S$ is an fppf group scheme over $S$ that is affine over $S$. Suppose that $f : Z \to S$ is a right $G_S$-torsor, but $T \to \text{Spec} k$ is a right $G$-torsor. Define

$$Z^\tau := Z \times^G_{S} T_S = Z \times_k T$$
and let \( f^r : Z^r \to S \) be its structure morphism. Then \( Z^r \) is a right \( G^r \)-torsor over \( S \) (i.e., a right \( (G^r)_S \)-torsor).

### 6.5.7. Unramified torsors

This section will be essential for the finiteness of Selmer sets in Section 8.4.4. Let \( k \) be a global field. Let \( S \) be a finite nonempty set of places of \( k \) containing all the archimedean places. Let \( \mathcal{O}_{k,S} \) be the ring of \( S \)-integers in \( k \). For \( v \not\in S \), let \( \mathcal{O}_{k,v} \) be the local ring of \( \mathcal{O}_{k,S} \) at \( v \), let \( \mathcal{O}_v \) be its completion, and let \( k_v = \text{Frac} \mathcal{O}_v \), so \( k_v \) is the completion of \( k \) at \( v \). Let \( \mathcal{G} \) be a smooth finite-type affine group scheme over \( \mathcal{O}_{k,S} \). Affineness guarantees that every element of \( H^1 \) is actually represented by a torsor scheme (Theorem 6.5.10(i)). Let \( G = \mathcal{G} \times_{\mathcal{O}_{k,S}} k \).

Let \( \tau \in H^1(k, G) \) and \( v \not\in S \). Let \( \tau_v \) be the image of \( \tau \) in \( H^1(k_v, G) \). Call \( \tau \) unramified at \( v \) if \( \tau \) is in the image of \( H^1(\mathcal{O}_{k,v}, \mathcal{G}) \to H^1(k_v, G) \), or equivalently, if \( \tau_v \) is the image of \( H^1(\mathcal{O}_v, \mathcal{G}) \to H^1(k_v, G) \) (the equivalence follows from a fancy version of fpqc descent: see [BLR90, Section 6.2, Proposition D.4(b)]). Call \( \tau \) unramified outside \( S \) if \( \tau \) is unramified at every \( v \not\in S \); in this case, \( \tau \) comes from an element of \( H^1(\mathcal{O}_{k,S}, \mathcal{G}) \): first, the torsor corresponding to \( \tau \) spreads out over \( \mathcal{O}_{k,S'} \) for some finite \( S' \supseteq S \); then apply fpqc descent to \( \text{Spec} \mathcal{O}_{k,S'} \prod_{v \in S \setminus S'} \text{Spec} \mathcal{O}_{k,v} \to \text{Spec} \mathcal{O}_{k,S} \). Let \( H^1_S(k, \mathcal{G}) \) be the set of \( \tau \in H^1(k, G) \) that are unramified outside \( S \).

As in Section 6.5.1, we have an exact sequence of smooth algebraic groups over \( k \)

\[
1 \to G^0 \to G \to F \to 1
\]

where \( G^0 \) is the connected component of \( G \), and \( F \) is finite étale over \( k \). Enlarging \( S \) if necessary, we get an corresponding exact sequence of smooth finite-type separated group schemes over \( \mathcal{O}_{k,S} \)

\[
1 \to \mathcal{G}^0 \to \mathcal{G} \to \mathcal{F} \to 1
\]

in which \( \mathcal{G}^0 \) has connected fibers, and \( \mathcal{F} \) is finite étale of order \( n \). The map \( H^1(k, G) \to H^1(k, F) \) restricts to a map \( h : H^1_S(k, \mathcal{G}) \to H^1_S(k, \mathcal{F}) \).

**Theorem 6.5.13.** Under the hypotheses above,

(a) The maps \( H^1_S(k, \mathcal{G}) \to h^* H^1_S(k, \mathcal{F}) \to \prod_{v \in S} H^1(k_v, F) \) have finite fibers.

(b) If \( k \) is a number field, then \( H^1_S(k, \mathcal{G}) \) itself is finite.

**Proof.** Step 1: For each \( v \not\in S \), the kernel of \( H^1(\mathcal{O}_v, \mathcal{F}) \to H^1(k_v, F) \) is trivial.

If \( T \) is an \( \mathcal{F} \)-torsor over \( \mathcal{O}_v \), then \( T \) is finite over \( \mathcal{O}_v \) by Remark 6.5.2 and hence proper over \( \mathcal{O}_v \), so \( T(\mathcal{O}_v) = T(k_v) \) by the valuative criterion for properness. Thus \( T(\mathcal{O}_v) \neq \emptyset \) if and only if \( T(k_v) \neq \emptyset \). That is, \( T \) is trivial if and only if \( T_{k_v} \) is trivial.

**Step 2:** \( H^1(\mathcal{O}_v, \mathcal{G}^0) = 0 \).
Let $T \to \text{Spec} \mathcal{O}_v$ be a $G^0$-torsor. Its special fiber $T_{k(v)}$ over the residue field corresponds to an element of $H^1(k(v), G^0_{k(v)})$, which is trivial by Lang’s theorem (Theorem 5.12.19(a)). Thus $T_{k(v)}$ has a $k(v)$-point. Since $G^0$ is smooth over $\mathcal{O}_v$, so is $T$ (Remark 6.5.2), so Hensel’s lemma (Theorem 3.5.62(a)) implies that $T$ has an $\mathcal{O}_v$-point. Thus $T$ is a trivial torsor.

**Step 3: The kernel of $h$ is finite.**

For each $v \notin S$, we have the following commutative diagram in which the maps labelled “Step 1” and “Step 2” have trivial kernel:

$$
\begin{array}{ccc}
H^1(k, G) & \longrightarrow & H^1(k, F) \\
\downarrow & & \downarrow \\
H^1(k_v, G) & \longrightarrow & H^1(k_v, F) \\
\uparrow & & \uparrow \\
H^1(\mathcal{O}_v, G) & \longrightarrow & H^1(\mathcal{O}_v, F).
\end{array}
$$

Suppose $\tau \in \text{ker} \ h$. By definition of $H^1_S(k, G)$, for each $v \notin S$, the element $\tau_v$ comes from some $\tau_{\mathcal{O}_v} \in H^1(\mathcal{O}_v, G)$. The diagram shows that $\tau_{\mathcal{O}_v}$ maps to 0 in $H^1(k_v, F)$. Step 1 shows that $\tau_{\mathcal{O}_v}$ maps to 0 already in $H^1(\mathcal{O}_v, F)$. Step 2 shows that $\tau_{\mathcal{O}_v} = 0$. Thus $\tau_v = 0$.

Hence $\text{ker} \ h$ is contained in

$$
\mathop{\Pi}\limits_{v \in S} H^1(k, G) := \text{ker} \left( H^1(k, G) \to \prod_{v \in S} H^1(k_v, G) \right),
$$

which is finite by Theorem 5.12.29 since $G$ is affine.

**Step 4: Every fiber of $h$ is finite.**

Given a nonempty fiber $h^{-1}(\phi)$ with $\phi \in H^1_S(k, F)$, choose $\tau \in h^{-1}(\phi) \subseteq H^1_S(k, G)$. Then $\tau$ comes from an element of $H^1(\mathcal{O}_{k,S}, G)$. Call this element $\tau$ too.

If $G$ were commutative, then $h^{-1}(\phi)$ would be in bijection with $h^{-1}(0)$ via the subtraction-of-$\tau$ map. In the general case, subtraction-of-$\tau$ and subtraction-of-$\phi$ (see Section 5.12.5.3) identify the top row of

$$
\begin{array}{ccc}
H^1_S(k, G) & \overset{h}{\longrightarrow} & H^1_S(k, F) \\
\downarrow & & \downarrow \\
H^1_S(k, G^\tau) & \overset{h^\tau}{\longrightarrow} & H^1_S(k, F^\phi)
\end{array}
$$

with the bottom row, and $h^{-1}(\phi)$ is identified with $(h^\tau)^{-1}(0)$. By Step 3 applied to $G^\tau$, the latter is finite. Thus $h^{-1}(\phi)$ is finite.

**Step 5: The map $H^1_S(k, F) \to \prod_{v \in S} H^1(k_v, F)$ has finite fibers.**
Fix $\xi_v \in H^1(k_v, F)$ for each $v \in S$. Consider $\tau \in H^1_S(k, \mathcal{F})$ mapping to $\xi_v$ for all $v$. By Theorem 4.3.7(i), the torsor $T \to \text{Spec} \ k$ corresponding to $\tau$ is finite étale. By Proposition 3.5.35 $T$ as $k$-scheme is a disjoint union of $k$-schemes of the form $\text{Spec} \ R$, where each $R$ is the valuation ring of a finite unramified extension of $k_v$. This implies that each $L/k$ above is unramified outside $S$. For finite $v \notin S$, the class $\tau_v$ comes from $H^1(O_v, \mathcal{F})$, so the base extension $T_{k_v}$ comes from a finite étale $O_v$-scheme, which by Theorem 3.5.51 is a disjoint union of $O_v$-schemes $\text{Spec} \ R$, where each $R$ is the valuation ring of a finite unramified extension of $k_v$. This implies that each $L/k$ above is unramified outside $S$. For finite $v \notin S$, the $v$-adic valuation of the discriminant of each $L/K$ may be nonzero, but it is bounded given $\xi_v$. A variant of Hermite’s theorem [Ser97, 4.1] says that $k$ has only finitely many separable extensions of degree $\leq n$ and bounded discriminant.

Step 6: If $k$ is a number field, then $H^1_S(k, \mathcal{G})$ is finite.

If $k$ is a number field, then (an elementary case of) Theorem 5.12.24(a) shows that $H^1(k_v, F)$ is finite for each of the finitely many $v$ in $S$. Thus the conclusion follows from (a).

6.6. Brauer groups

(References: [Gro68b, Gro68c, Gro68d] and [Mil80 IV])

6.6.1. Cohomology of $\mathbb{G}_m$.

**Proposition 6.6.1.** Let $X$ be a scheme. Then

(i) $H^0_{\text{Zar}}(X, \mathbb{G}_m) \simeq H^0_{\text{et}}(X, \mathbb{G}_m) \simeq H^0_{\text{fppf}}(X, \mathbb{G}_m) \simeq \mathcal{O}_X(X)^\times$.

(ii) $H^1_{\text{Zar}}(X, \mathbb{G}_m) \simeq H^1_{\text{et}}(X, \mathbb{G}_m) \simeq H^1_{\text{fppf}}(X, \mathbb{G}_m) \simeq \text{Pic} X$ (generalization of Hilbert’s theorem 90).

**Proof.**

(i) This is true by definition.

(ii) For each Zariski open covering $\mathcal{U} = \{U_i \to X\}$, we have

$$\frac{\{\text{line bundles trivialized by } \mathcal{U}\}}{\text{isomorphism}} \simeq \check{H}^1_{\text{Zar}}(\mathcal{U}, \mathbb{G}_m),$$

because the transition maps needed to describe a line bundle are invertible functions on the pairwise intersections. Taking the direct limit over open coverings, we get the first
of the isomorphisms in 
\[
\text{Pic } X \simeq \tilde{H}^1_{\text{Zar}}(X, \mathbb{G}_m) \simeq H^1_{\text{Zar}}(X, \mathbb{G}_m),
\]
and the second isomorphism comes from Proposition 6.4.12.

If we repeat the argument using the étale topology instead of the Zariski topology, we get an isomorphism
\[
\text{Pic } X_{\text{et}} \simeq H^1_{\text{et}}(X, \mathbb{G}_m),
\]
where \(\text{Pic } X_{\text{et}}\) is the group of isomorphism classes of “étale line bundles”, that is, sheaves \(\mathcal{L}\) on \(X_{\text{et}}\) such that there exists an étale open covering \(\{U_i \to X\}\) such that \(\mathcal{L}|_{U_i} \simeq \mathcal{O}_{U_i}\) for all \(i\).

We claim that for any étale surjective morphism \(X' \to X\), the maps
\[
\begin{array}{c}
\{ \text{line bundles on } X \} \\
\text{trivialized by } X'
\end{array} \xrightarrow{\text{fpqc descent}} \begin{array}{c}
\{ \text{trivial line bundles on } X' \} \\
\text{with descent datum}
\end{array}
\]
\[
\begin{array}{c}
\{ \text{line bundles on } X_{\text{et}} \} \\
\text{trivialized by } X'_{\text{et}}
\end{array} \xrightarrow{\text{étale gluing}} \begin{array}{c}
\{ \text{trivial line bundles on } X'_{\text{et}} \} \\
\text{with descent datum},
\end{array}
\]
where each set denotes a set of isomorphism classes, are bijections. The top horizontal map is a bijection by Theorem 4.2.3 on fpqc descent of quasi-coherent sheaves: one can show that descending a line bundle yields a line bundle. The right vertical map is the functor of Definition 6.3.13; it gives a bijection, because the descent data are given by isomorphisms of trivial line bundles, and the automorphism groups of the trivial line bundle \(\mathcal{O}_X\) and \(\mathcal{O}_{X_{\text{et}}}\) are both equal to \(\mathcal{O}_X(X)^\times\) for every scheme \(X\). The bottom horizontal map is a bijection because an étale sheaf is uniquely determined by its restriction to an étale open cover with glueing data.

Finally, taking the limit of the bijection between the sets on the left over all \(X' \to X\) yields \(\text{Pic } X \simeq \text{Pic } X_{\text{et}}\), since every line bundle (on \(X\) or \(X_{\text{et}}\)) is trivialized by some \(X'\). Thus \(\text{Pic } X, \text{Pic } X_{\text{et}}, H^1_{\text{Zar}}(X, \mathbb{G}_m), H^1_{\text{et}}(X, \mathbb{G}_m)\) are all isomorphic.

The same proof shows that \(\text{Pic } X \simeq H^1_{\text{fppf}}(X, \mathbb{G}_m)\). □

**Remark 6.6.2.** Specializing part (ii) to the case \(X = \text{Spec } k\) with the étale topology gives \(H^1(\mathcal{G}_k, k^\times) = 0\), which is (Noether’s generalization of) Hilbert’s theorem 90.

**Remark 6.6.3.** More generally, if \(G\) is any smooth commutative group scheme over a scheme \(X\), then \(H^q_{\text{et}}(X, G) \simeq H^q_{\text{fppf}}(X, G)\) [Gro68d, Théorème 11.7]. The analogue for smooth noncommutative \(G\) holds too, as far as it makes sense: \(H^1_{\text{et}}(X, G) \simeq H^1_{\text{fppf}}(X, G)\) [Gro68d, Remarque 11.8(3)].
6.6.2. The cohomological Brauer group. For a field $k$, Theorems 1.5.12 and 6.4.6(iii) yield

\[ \text{Br}_k \cong H^2(\mathfrak{g}_k, k_s^\times) \cong H^2_{\text{et}}(\text{Spec } k, \mathbb{G}_m). \]

The right hand side makes sense when $\text{Spec } k$ is replaced by an arbitrary scheme, so we are led to the following definition:

**Definition 6.6.4.** For any scheme $X$, define the (cohomological) Brauer group as

\[ \text{Br} X := H^2_{\text{et}}(X, \mathbb{G}_m). \]

If $R$ is a commutative ring, define $\text{Br} R := \text{Br}(\text{Spec } R)$.

**Warning 6.6.5.** Some authors use $\text{Br} X$ instead to denote the Brauer group defined using Azumaya algebras as in Definition 6.6.14 and use $\text{Br}' X$ to denote the cohomological Brauer group. Some instead use $\text{Br}' X$ to denote the torsion subgroup of the cohomological Brauer group, because of Theorem 6.6.17(iii).

**Remark 6.6.6.** For any scheme $X$, we have $\text{Br} X \cong H^2_{\text{fppf}}(X, \mathbb{G}_m)$, by Remark 6.6.3.

If $X \to Y$ is a morphism of schemes, then there is an induced homomorphism $\text{Br} Y \to \text{Br} X$, and we obtain a functor

\[ \text{Schemes}^{\text{op}} \to \text{Ab} \]

\[ X \mapsto \text{Br} X. \]

**Proposition 6.6.7 (Brauer group of a regular integral noetherian scheme).** Let $X$ be a regular integral noetherian scheme. Then

(i) $\text{Br} X \to \text{Br} k(X)$ is injective.

(ii) $\text{Br} X$ is a torsion abelian group.

**Proof.**

(i) This is a special case of [Gro68c, Corollaire 1.10].

(ii) Since $\text{Br} k(X)$ is a Galois cohomology group, it is torsion. So (i) implies (ii). \[ \square \]

**Warning 6.6.8.** Without regularity, Proposition 6.6.7 can fail: Exercise 6.6 gives a counterexample to (i) from [AG60, p. 388]. Part (ii) can fail too: see Warning 6.6.18(i).

For an extension of Proposition 6.6.7(i), see Theorem 6.8.3.

**Corollary 6.6.9.** If $X \to Y$ is a birational morphism of regular integral noetherian schemes, then $\text{Br} Y \to \text{Br} X$ is injective.
Proof. Functoriality of $\text{Br}$ yields a commutative diagram

\[
\begin{array}{ccc}
\text{Br} X & \longrightarrow & \text{Br} \mathbb{k}(X) \\
\uparrow & & \uparrow \\
\text{Br} Y & \longrightarrow & \text{Br} \mathbb{k}(Y)
\end{array}
\]

and the horizontal homomorphisms are injective by Proposition 6.6.7(i). □

See Corollary 6.8.5 for a partial refinement of Corollary 6.6.9.

Proposition 6.6.10 (Brauer group of a limit). Let $(X_i)_{i \in I}$ be a filtered inverse system of schemes. Suppose that the $X_i$ are quasi-compact and quasi-separated, and that the morphisms in the system are affine. Let $X = \varprojlim X_i$. Then $\text{Br} X \simeq \varprojlim \text{Br} X_i$.

Proof. Take $G_0 = \mathbb{G}_m$ and $q = 2$ in Theorem 6.4.3. □

Proposition 6.6.10 is useful for spreading out Brauer group elements:

Corollary 6.6.11. Let $X$ be a variety over a global field $k$. Let $A \in \text{Br} X$. Then for some finite set $S$ of places of $k$, there exist a finite-type $\mathcal{O}_{k,S}$-scheme $\mathcal{X}$, an element $A \in \text{Br} \mathcal{X}$ and a morphism $X \hookrightarrow \mathcal{X}$ identifying $X$ with the generic fiber $\mathcal{X}_k$ such that $\text{Br} \mathcal{X} \rightarrow \text{Br} X$ maps $A$ to $A$.

Proof. Theorem 3.2.1 lets us spread out $X$ to a finite-type $\mathcal{O}_{k,S}$-scheme $\mathcal{X}$. The open subschemes $\mathcal{X}_{\mathcal{O}_{k,T}}$, as $T$ ranges over finite sets of places with $T \supseteq S$, form a filtered inverse system and $\varprojlim \mathcal{X}_{\mathcal{O}_{k,T}} \simeq X$. By Proposition 6.6.10 $\text{Br} X \simeq \varprojlim \text{Br} \mathcal{X}_{\mathcal{O}_{k,T}}$. Thus $A$ comes from an element of $\text{Br} \mathcal{X}_{\mathcal{O}_{k,T}}$ for some $T$. Rename $T$ as $S$, and rename $\mathcal{X}_{\mathcal{O}_{k,T}}$ as $\mathcal{X}$. □

6.6.3. Azumaya algebras. A matrix algebra over a field $k$ is $\text{End} V$ for some finite-dimensional vector space over $k$. The generalization of this over a scheme $X$ is the $\mathcal{O}_X$-algebra $\text{End}_{\mathcal{O}_X}(\mathcal{E}) := \text{Hom}_{\mathcal{O}_X}(\mathcal{E}, \mathcal{E})$ for some locally free $\mathcal{O}_X$-module $\mathcal{E}$.

An Azumaya algebra over $k$ is a $k$-algebra that becomes isomorphic to an $r \times r$ matrix algebra for some $r \in \mathbb{Z}_{>0}$ after finite separable base extension. The generalization of this is the following:

Definition 6.6.12. [Gro68b, Théorème 5.1] An Azumaya algebra on a scheme $X$ is an $\mathcal{O}_X$-algebra $\mathcal{A}$ that is coherent as an $\mathcal{O}_X$-module with $\mathcal{A}_x \neq 0$ for all $x \in X$, and that satisfies one of the following equivalent conditions:

(i) There is an open covering $\{U_i \rightarrow X\}$ in the étale topology such that for each $i$ there exists $r_i \in \mathbb{Z}_{>0}$ such that $\mathcal{A} \otimes_{\mathcal{O}_X} \mathcal{O}_{U_i} \simeq \mathbb{M}_{r_i}(\mathcal{O}_{U_i})$.

(ii) There is an open covering $\{U_i \rightarrow X\}$ in the fppf topology such that for each $i$ there exists $r_i \in \mathbb{Z}_{>0}$ such that $\mathcal{A} \otimes_{\mathcal{O}_X} \mathcal{O}_{U_i} \simeq \mathbb{M}_{r_i}(\mathcal{O}_{U_i})$. 

173
(iii) $\mathcal{A}$ is locally free as an $\mathcal{O}_X$-module, and the fiber $\mathcal{A}(x) := \mathcal{A} \otimes \mathcal{k}(x)$ is an Azumaya algebra over the residue field $\mathcal{k}(x)$ for each $x \in X$.

(iv) $\mathcal{A}$ is locally free as an $\mathcal{O}_X$-module, and the canonical homomorphism $\mathcal{A} \otimes \mathcal{A}^{opp} \to \text{End}_{\mathcal{O}_X}(\mathcal{A})$ is an isomorphism.

6.6.3.1. The Azumaya Brauer group.

Definition 6.6.13. Two Azumaya algebras $\mathcal{A}$ and $\mathcal{A}'$ on $X$ are similar (and we then write $\mathcal{A} \sim \mathcal{A}'$) if there exist locally free coherent $\mathcal{O}_X$-modules $\mathcal{E}$ and $\mathcal{E}'$ of positive rank at each $x \in X$ such that $\mathcal{A} \otimes \mathcal{O}_X \text{End}_{\mathcal{O}_X}(\mathcal{E}) \simeq \mathcal{A}' \otimes \mathcal{O}_X \text{End}_{\mathcal{O}_X}(\mathcal{E}')$.

Definition 6.6.14. Let $X$ be a scheme. The Azumaya Brauer group $\text{Br}_{\text{Az}} X$ is the set of similarity classes of Azumaya algebras on $X$. The multiplication is induced by $\mathcal{A}, \mathcal{B} \mapsto \mathcal{A} \otimes \mathcal{B}$, the inverse is induced by $\mathcal{A} \mapsto \mathcal{A}^{opp}$, and the identity is the class of $\mathcal{O}_X$.

Then $\text{Br}_{\text{Az}}$ is a functor from $\text{Schemes}^{opp}$ to $\text{Ab}$, just as $\text{Br}$ was.

6.6.3.2. Cyclic Azumaya algebras. The cyclic algebra constructions from Section 1.5.7 generalize in a straightforward way to an arbitrary base scheme $X$. Namely, suppose that $a \in \Gamma(X, \mathcal{O}_X^\times)$ is a global unit, and that $Y \to X$ is a $\mathbb{Z}/n\mathbb{Z}$-torsor. As in Section 1.5.7, we define a twisted polynomial algebra $\mathcal{O}_Y[x]_\sigma$, where $\sigma$ acts as the generator of $\mathbb{Z}/n\mathbb{Z}$, and $x\ell = (\sigma \ell) x$ for all sections $\ell$ of $\mathcal{O}_Y$. Then the $\mathcal{O}_X$-algebra $\mathcal{O}_Y[x]_\sigma/(x^n - a)$ turns out to be an Azumaya $\mathcal{O}_X$-algebra, split by the étale cover $Y \to X$.

There is a cohomological version of this construction. The exact sequence

$$1 \to \mu_n \to \mathbb{G}_m \to \mathbb{G}_m \to 1$$

lets us map $a$ to an element of $H^1(X, \mu_n)$. On the other hand, the torsor $Y \to X$ has a class in $H^1(X, \mathbb{Z}/n\mathbb{Z})$. The cup product yields an element of $H^2(X, \mu_n)$, which can be mapped to an element of $H^2(X, \mathbb{G}_m) =: \text{Br} X$.

The two constructions above are related: the homomorphism (6.6.16) defined in the next section maps the class of $\mathcal{O}_Y[x]_\sigma/(x^n - a)$ to the element of $\text{Br} X$.

Remark 6.6.15. Suppose that $X$ is a scheme over $\mathbb{Z}[1/n, \zeta_n]$, so $\mathbb{Z}/n\mathbb{Z}$ is isomorphic to $\mu_n$ over $X$. Then we may form a cyclic algebra from two units $a, b \in \Gamma(X, \mathcal{O}_X^\times)$, by reinterpreting the $\mu_n$-torsor $\text{Spec } \mathcal{O}_X[x]/(x^n - b) \to X$ as a $\mathbb{Z}/n\mathbb{Z}$-torsor and proceeding as before.

6.6.4. Comparison of the two definitions of the Brauer group. Just as Azumaya algebras of dimension $n^2$ over a field $k$ are classified up to isomorphism by $H^1(k, \text{PGL}_n)$, Azumaya algebras of rank $n^2$ over a scheme $X$ are classified by $H^1(X, \text{PGL}_n)$: a Čech 1-cocycle gives the transition data needed to glue sheaves of matrix algebras using fpqc descent.
The exact sequence
\[ 0 \to \mathbb{G}_m \to \text{GL}_n \to \text{PGL}_n \to 0 \]
of sheaves on \( X_{et} \) (or \( X_{fppf} \)) gives rise to a map
\[ H^1(X, \text{PGL}_n) \to H^2(X, \mathbb{G}_m) = \text{Br} \]
so each Azumaya algebra \( \mathcal{A} \) of rank \( n^2 \) gives rise to an element of \( \text{Br} \). If the rank of \( \mathcal{A} \) is not constant, one can apply the same construction on each open and closed subset of \( X \) where the rank is constant. It turns out that this induces a map
\[ (6.6.16) \quad \text{Br}_{Az} X \to \text{Br} X, \]
functorial in \( X \).

**Theorem 6.6.17.**

(i) For any scheme \( X \), the natural map
\[ \text{Br}_{Az} X \to \text{Br} X := H^2_{et}(X, \mathbb{G}_m). \]
is an injective homomorphism.

(ii) An Azumaya algebra \( \mathcal{A} \) on \( X \) that is locally free of rank \( n^2 \) defines an element of \( \text{Br}_{Az} X \) that is killed by \( n \). In particular, if \( X \) has at most finitely many connected components, \( \text{Br}_{Az} X \) is torsion.

(iii) If \( X \) has an ample invertible sheaf (e.g., \( X \) is quasi-projective over \( \text{Spec} A \) for some noetherian ring \( A \)), then the injection in (i) induces an isomorphism
\[ \text{Br}_{Az} X \cong (\text{Br} X)_{tors}. \]

**Proof.**

(i) See [Gro68b, equation (2.1)].

(ii) We have a commutative diagram of fppf group schemes
\[
\begin{array}{cccccc}
0 & \longrightarrow & \mu_n & \longrightarrow & \text{SL}_n & \longrightarrow \text{PSL}_n & \longrightarrow 0 \\
\downarrow & & \downarrow & & \downarrow & & \downarrow \\
0 & \longrightarrow & \mathbb{G}_m & \longrightarrow & \text{GL}_n & \longrightarrow \text{PGL}_n & \longrightarrow 0.
\end{array}
\]
The snake lemma, together with the surjectivity of \( \mathbb{G}_m \to \mathbb{G}_m \), shows that \( \text{PSL}_n \to \text{PGL}_n \) is an isomorphism. Taking cohomology gives a commutative diagram
\[
\begin{array}{ccc}
H^1(X, \text{PSL}_n) & \longrightarrow & H^2(X, \mu_n) \\
\downarrow & & \downarrow \\
H^1(X, \text{PGL}_n) & \longrightarrow & H^2(X, \mathbb{G}_m).
\end{array}
\]
Now $A$ corresponds to an element of $H^1(X, \text{PGL}_n)$. The diagram shows that its image in $H^2(X, \mathbb{G}_m)$ comes from an element of $H^2(X, \mu_n)$ and is hence killed by $n$. By [i], the class of $A$ in $\text{Br}_{\text{Az}}X$ is killed by $n$ too.

(iii) This is an unpublished theorem of Gabber. A different proof, using “$\alpha$-twisted sheaves” was found by de Jong [DJ]. □

Warning 6.6.18.

(i) Mumford constructed a normal singular surface $X$ over $\mathbb{C}$ such that $\text{Br}X$ is not torsion [Gro68c, Remarque 1.11b]. But $\text{Br}_{\text{Az}}X$ is torsion. This shows the necessity of taking the torsion subgroup on the right hand side of Theorem 6.6.17(iii).

(ii) There is a nonseparated normal surface with $\text{Br}_{\text{Az}}X \subseteq (\text{Br}X)_{\text{tors}}$, namely the cone $\text{Spec}\mathbb{C}[x, y, z]/(xy - z^2)$ with a doubled vertex. The original reference is [EHKV01, Corollary 3.11]; see [Ber05, §3] for a simpler proof.

Corollary 6.6.19. If $X$ is a regular quasi-projective variety over a field, then $\text{Br}_{\text{Az}}X \simeq (\text{Br}X)_{\text{tors}} = \text{Br}X$.

Proof. The first isomorphism comes from Theorem 6.6.17(iii). By Proposition 3.5.5, the variety $X$ is a finite disjoint union of integral varieties, and applying Proposition 6.6.7(ii) to each shows that $\text{Br}X$ is torsion. □

6.6.5. Computing Brauer groups. Two main methods for computing Brauer groups are

- the Hochschild–Serre spectral sequence in étale cohomology (see Corollary 6.7.8), and
- residue homomorphisms (see Theorem 6.8.3).

6.7. Spectral sequences

(References: [Mil80, Appendix B], [Sha72, II.§4], [Wei94, Chapter V])

Suppose that one has left exact functors between abelian categories

$$
\begin{align*}
A & \xrightarrow{f} B \\
& \xrightarrow{g} C.
\end{align*}
$$

Then the composite functor $gf : A \to C$ is also left exact. If $A$ and $B$ have enough injectives, one can form the derived functors $R^n f$, $R^n g$, and $R^n (gf)$. If moreover $f$ takes injectives to $g$-acyclics (that is, $R^q g(f(A)) = 0$ for any injective object $A \in A$ and any $q \in \mathbb{Z}_{>0}$), then there is a spectral sequence

$$
E_2^{p,q} := (R^p g)(R^q f)(A) \implies (R^{p+q}(gf))(A)
$$

that sometimes lets one compute $R^n (gf)$ in terms of the other two derived functors.
The notation
\[ E_2^{p,q} \Rightarrow L^{p+q} \]
used above means all of the following:

- For each \( r \in \mathbb{Z}_{\geq 2} \cup \{ \infty \} \), there is a page \( r \) consisting of objects \( E_r^{p,q} \) of \( \mathcal{C} \) for \( p, q \in \mathbb{Z} \) such that \( E_r^{p,q} = 0 \) when \( p < 0 \) or \( q < 0 \). (The objects on a given page are usually displayed in a table.)
- The objects \( E_2^{p,q} \) on page 2 are the ones given in the notation.
- For \( r \in \mathbb{Z}_{\geq 2} \), one has morphisms “of degree \( (r, 1 - r) \)”: this means that there is a morphism
  \[ d_r^{p,q} : E_r^{p,q} \to E_r^{p+r,q+1-r} \]
  for each \( p, q \in \mathbb{Z} \). For example, page 2 looks like

\[ \cdots \]

- For each \( r \in \mathbb{Z}_{\geq 2} \), the morphisms on page \( r \) form complexes:
  \[ d_r^{p,q} \circ d_r^{p-r,q+r-1} = 0 \]
  for all \( p, q \in \mathbb{Z} \).
- For each \( r \in \mathbb{Z}_{\geq 2} \), the objects on page \( r + 1 \) are the cohomology objects of the complexes on page \( r \):
  \[ E_{r+1}^{p,q} = \frac{\ker d_r^{p,q}}{\text{im} d_r^{p-r,q+r-1}}. \]
- For fixed \( p, q \in \mathbb{Z} \), the page \( \infty \) object \( E_\infty^{p,q} \) is equal to \( E_r^{p,q} \) for sufficiently large \( r \). (Note that for \( r \) sufficiently large, the \( d_r \) morphisms coming into and out of \( E_r^{p,q} \) extend outside the nonnegative quadrant, so they are automatically zero, and hence \( E_r^{p,q} = E_{r+1}^{p,q} = E_{r+2}^{p,q} = \cdots \).
- The “limit objects” \( L^n \) for \( n \in \mathbb{N} \) are objects of \( \mathcal{C} \).
The object \( L^n \) has a filtration

\[
L^n = L^n_0 \supseteq L^n_1 \supseteq \cdots \supseteq L^n_n \supseteq 0
\]

such that the quotients of successive terms equal (respectively) the objects

\[
E^{0,n}_\infty, E^{1,n-1}_\infty, \ldots, E^{n,0}_\infty
\]

along a diagonal on page \( \infty \). (Thus \( E^{0,n}_\infty \) is a subobject of \( L_n \).)

One says that \( E^{p,q}_2 \) converges to (or abuts to) \( L^{p+q} \).

**Proposition 6.7.1.** Suppose that

\[
E^{p,q}_2 \Longrightarrow L^{p+q}
\]

is a spectral sequence. Abbreviate \( E^{p,q}_2 \) as \( E^{p,q} \). Then there is an exact sequence

\[
0 \rightarrow E^{1,0} \rightarrow L^1 \rightarrow E^{0,1} \xrightarrow{d} E^{2,0} \rightarrow \ker (L^2 \rightarrow E^{0,2}) \rightarrow E^{1,1} \rightarrow E^{3,0}.
\]

**Remark 6.7.2.** Spectral sequences also arise in some situations not having to do with the composition of left exact functors. For instance, cohomology of the total complex of a double complex is the limit of a spectral sequence starting with page 1.

**6.7.1. The Hochschild–Serre spectral sequence in group cohomology.**

**Theorem 6.7.3.** Let \( G \) be a profinite group, and let \( H \) be a normal closed subgroup of \( G \). Then there is a spectral sequence

\[
E^{p,q}_2 := \mathbb{H}^p(G/H, \mathbb{H}^q(H, A)) \Longrightarrow \mathbb{H}^{p+q}(G, A)
\]

for each (continuous) \( G \)-module \( A \).

**Sketch of proof.** The composition of the left exact functors

\[
\{G\text{-modules}\} \rightarrow \{G/H\text{-modules}\} \rightarrow \text{Ab}
\]

\[
M \longrightarrow M^H
\]

\[
N \longrightarrow N^{G/H}
\]

equals

\[
M \longrightarrow M^G.
\]

(All actions are assumed continuous.) One checks that the first functor takes injectives to acyclics.

Applying Proposition 6.7.1 to Theorem 6.7.3 one gets the following extension of the inflation-restriction sequence:
**Corollary 6.7.4 (Inflation-restriction sequence).** Let $G$ be a profinite group, and let $H$ be a normal closed subgroup of $G$. Then for any $G$-module $A$, there is an exact sequence

$$0 \to H^1(G/H, A^H) \xrightarrow{\text{Inf}} H^1(G, A) \xrightarrow{\text{Res}} H^1(H, A)^{G/H}$$

$$\to H^2(G/H, A^H) \to \ker (H^2(G, A) \to H^2(H, A)) \to H^1(G/H, H^1(H, A))$$

$$\to H^3(G/H, A^H).$$

**6.7.2. The Hochschild–Serre spectral sequence in étale cohomology.** Recall from Example 6.5.4 that a Galois covering of schemes $X' \to X$ with Galois group $G$ (assumed finite) is the same thing as a torsor under the constant group scheme associated to $G$. Then $X' \to X$ is finite and surjective, so it is fpqc. Since $X' \to X$ becomes étale after base extension by $X' \to X$, it was étale to begin with (Theorem 4.3.7(ii)).

**Theorem 6.7.5.** Let $X' \to X$ be a Galois covering of schemes with Galois group $G$. Let $\mathcal{F}$ be a sheaf on $X_{et}$. Then there is a spectral sequence

$$H^p(G, H^q_{et}(X', \mathcal{F})) \Rightarrow H^{p+q}_{et}(X, \mathcal{F}).$$

**Sketch of proof.** The right action of $G$ on $X'$ makes $\mathcal{F}(X')$ a left $G$-module. The sheaf condition for the open covering $\{X' \to X\}$ implies that the composition of the functors

$$\{\text{sheaves on } X_{et}\} \to \{\text{G-modules}\} \to \text{Ab}$$

$$\mathcal{F} \mapsto \mathcal{F}(X')$$

$$N \mapsto N^G$$

equals

$$\mathcal{F} \mapsto \mathcal{F}(X).$$

Moreover, the first functor takes injectives to acyclics. □

**Remark 6.7.6.** A common application of Theorem 6.7.5 is to the case where $X$ is a $k$-variety and $X' = X_L$ for some finite Galois extension $L$ of $k$. By taking a direct limit, one obtains an analogous spectral sequence for an infinite Galois extension, such as $k_s$ over $k$.

Theorem 6.7.5 and Remark 6.7.6 help us compute Brauer groups of varieties over non-algebraically closed fields.

**Definition 6.7.7.** If $X$ is a variety over a field $k$, let $X^s = X_{k_s}$ and define the algebraic part of the Brauer group of $X$ by

$$\text{Br}_1 X := \ker (\text{Br} X \to \text{Br} X^s).$$

179
Corollary 6.7.8. Let $X$ be a proper and geometrically integral variety over a field $k$. Then there is an exact sequence

$$0 \to \text{Pic } X \to (\text{Pic } X^s)^{\mathcal{G}_k} \to \text{Br } k \to \text{Br}_1 X \to H^1(\mathcal{G}_k, \text{Pic } X^s) \to H^3(k, \mathbb{G}_m).$$

Proof. We apply Theorem 6.7.5 and Remark 6.7.6 with $\mathcal{F} = \mathbb{G}_m$, and plug

- $H^0_{\text{et}}(X^s, \mathbb{G}_m) = k_s^\times$ (Proposition 2.2.22)
- $H^1_{\text{et}}(X^s, \mathbb{G}_m) = \text{Pic } X^s$ (Proposition 6.6.1)
- $H^2_{\text{et}}(X^s, \mathbb{G}_m) = \text{Br } X^s$ (by definition)
- $H^1_{\text{et}}(X, \mathbb{G}_m) = \text{Pic } X$ (Proposition 6.6.1)
- $H^2_{\text{et}}(X, \mathbb{G}_m) = \text{Br } X$ (by definition)
- $H^1(\mathcal{G}_k, k^\times_s) = 0$ (Hilbert’s theorem 90)
- $H^2(\mathcal{G}_k, k^\times_s) = \text{Br } k$ (Theorem 1.5.12)

into the exact sequence of Proposition 6.7.1.

Remark 6.7.9. For a nice $k$-variety $X$, the homomorphism $(\text{Pic } X^s)^{\mathcal{G}_k} \to \text{Br } k$ given in Corollary 6.7.8 is the same as the homomorphism constructed in the proof of Proposition 4.5.12.

Remark 6.7.10. The cohomological approach to class field theory gives as a by-product that if $k$ is a local or global field, then $H^3(k, \mathbb{G}_m) = 0$. The local case is obtained by taking a direct limit of [NSW08, 7.2.2]. The number field case is [NSW08, 8.3.11(iv)] applied to the set $S$ of all places of $k$. The function field case follows from the fact $\text{scd } k \leq 2$ [NSW08, 8.3.17].

6.8. Residue homomorphisms

(References: [GS06, Chapter 6], [Gro68d, Section 2])

6.8.1. Residue homomorphisms for discrete valuation rings. Given an integral divisor $D$ on a variety $X$, one has the associated discrete valuation ring $R$ inside the function field $K := k(X)$. An element of $K^\times$ need not come from the subgroup $R^\times$; the obstruction is measured by the valuation $K^\times \to \mathbb{Z}$; in other words, a rational function has no zero or pole along $D$ if and only if its valuation is 0. Analogously, an element of $\text{Br } K$ need not come from the subgroup $\text{Br } R$; the obstruction is measured by a certain residue homomorphism:

Proposition 6.8.1. If $R$ is a discrete valuation ring with fraction field $K$ and residue field $k$, then there is an exact sequence

$$0 \to \text{Br } R \to \text{Br } K \to \text{res} H^1(k, \mathbb{Q}/\mathbb{Z}),$$

with the caveat that one must exclude the $p$-primary parts from all the groups if $k$ is imperfect of characteristic $p$. 

180
Proof. This is a special case of \cite{Gro68d}, Proposition 2.1. □

The residue homomorphism can be defined as follows. First, we may replace $R$ by its completion. Let $K^{\text{unr}}$ be the maximal unramified extension of $K$. If $k$ is perfect, then Example 1.2.4 implies that $K^{\text{unr}}$ is $C_1$, so $\text{Br} K^{\text{unr}} = 0$ by Proposition 1.5.28. If $k$ is imperfect of characteristic $p$, then Corollaire 1.3 implies that $\text{Br} K^{\text{unr}} = 0$ still holds after the $p$-primary part is excluded; in the rest of this paragraph, we exclude $p$-primary parts in this case. Proposition 1.3.15(iii) applied to the extension $K^{\text{unr}}$ of $K$ implies that $\text{Br} K \cong H^2(\text{Gal}(K^{\text{unr}}/K), (K^{\text{unr}})^\times)$, which maps to $H^2(\text{Gal}(K^{\text{unr}}/K), \mathbb{Z})$ via the valuation. Also, $\text{Gal}(K^{\text{unr}}/K) \cong \mathfrak{S}_k$. Finally, the long exact sequence associated to the exact sequence of groups $0 \to \mathbb{Z} \to \mathbb{Q} \to \mathbb{Q}/\mathbb{Z} \to 0$ with trivial $\mathfrak{S}_k$-action yields an isomorphism $H^1(k, \mathbb{Q}/\mathbb{Z}) \cong H^2(\text{Gal}(K^{\text{unr}}/K), \mathbb{Z})$. The composition $\text{Br} K \cong H^2(\text{Gal}(K^{\text{unr}}/K), (K^{\text{unr}})^\times) \to H^2(\text{Gal}(K^{\text{unr}}/K), \mathbb{Z}) \cong H^2(k, \mathbb{Z}) \cong H^1(k, \mathbb{Q}/\mathbb{Z})$ is the residue homomorphism.

\(\hat{\boxtimes}\) Warning 6.8.2. The caveat in Proposition 6.8.1 cannot be dropped. For example, if $k = k_s \neq \overline{k}$ and $R = k[[t]]$, then Proposition 6.9.1 below shows that $\text{Br} R \cong \text{Br} k = 0$, and $H^1(k, \mathbb{Q}/\mathbb{Z}) = 0$ (since $\mathfrak{S}_k = \{1\}$), but $\text{Br} k((t)) \neq 0$ (Exercise 1.26).

6.8.2. Residue homomorphisms for regular integral schemes; purity. For any discrete valuation $v$ on a field $K$ with residue field $k$, applying Proposition 6.8.1 to the valuation ring gives a homomorphism $\text{Br} K \to H^1(k, \mathbb{Q}/\mathbb{Z})$, modulo the caveat. On a regular integral noetherian scheme $X$, each integral divisor defines a discrete valuation $v$ on $k(X)$, and the integral divisors are in bijection with the set $X^{(1)}$ of codimension 1 points of $X$. Taking all the associated residue homomorphisms yields the following global variant of Proposition 6.8.1, saying roughly that an element of $\text{Br} k(X)$ belongs to the subgroup $\text{Br} X$ if and only if it has “no poles” along any integral divisor of $X$.

\textbf{Theorem 6.8.3.} Let $X$ be a regular integral noetherian scheme. Then the sequence $0 \to \text{Br} X \to \text{Br} k(X) \to \bigoplus_{x \in X^{(1)}} H^1(k(x), \mathbb{Q}/\mathbb{Z})$ is exact, with the caveat that one must exclude the $p$-primary part of all the groups if $X$ is of dimension $\leq 1$ and some $k(x)$ is imperfect of characteristic $p$, or if $X$ is of dimension $\geq 2$ and some $k(x)$ is of characteristic $p$.

\textbf{Proof.} This is a consequence of \cite{Gro68d}, Proposition 2.1 and Grothendieck’s “absolute cohomological purity” conjecture, proved by Gabber: see \cite{Fuj02}. □
Warning 6.8.4. The caveat in Theorem 6.8.3 cannot be removed completely. For example, suppose that \( k = k_s \neq \overline{k} \) and \( X := \mathbb{P}^1_k \). Then \( \text{Br} X = 0 \) (Theorem 6.9.7 below) and \( H^1(k(x), \mathbb{Q}/\mathbb{Z}) = 0 \) for every \( x \in X^{(1)} \), but \( \text{Br} k(X) \neq 0 \) (Exercise 1.26). On the other hand, it might be that excluding the \( p \)-primary parts for \( p \) such that some \( k(x) \) is imperfect of characteristic \( p \) is enough even when \( \dim X \geq 2 \).

**Corollary 6.8.5.** Let \( X \) be a regular integral noetherian scheme. Let \( Z \) be a closed subscheme of codimension \( \geq 2 \), and let \( U = X - Z \). Then the homomorphism \( \text{Br} X \to \text{Br} U \) is an isomorphism, with the caveat that one considers only the \( \ell \)-primary parts for primes \( \ell \) invertible on \( X \).

**Proof.** Theorem 6.8.3 describes \( \text{Br} X \) and \( \text{Br} U \) as the same subgroup of \( \text{Br} k(X) \). \( \square \)

**Remark 6.8.6.** The caveat in Corollary 6.8.5 might be unnecessary.

**Corollary 6.8.7.** Let \( X \) and \( X' \) be nice varieties over a field \( k \). If \( X \) and \( X' \) are birational, then \( \text{Br} X \) and \( \text{Br} X' \) are isomorphic, with the caveat that one considers only the prime-to-\( p \) parts if \( \text{char } k = p > 0 \).

**Proof.** We give the proof when \( \text{char } k = 0 \); restrict to the prime-to-\( p \) parts if \( \text{char } k = p > 0 \). The domain of definition \( U \) of the birational map \( X \dashrightarrow X' \) is the complement of a closed subscheme of codimension \( \geq 2 \) in \( X \). Corollary 6.8.5 implies that \( \text{Br} X \to \text{Br} U \) is an isomorphism. The composition \( \text{Br} X' \to \text{Br} U \xleftarrow{\sim} \text{Br} X \) is compatible with the embeddings of all three groups in \( \text{Br} k(X) = \text{Br} k(X') \). Thus \( \text{Br} X' \subseteq \text{Br} X \). Similarly \( \text{Br} X \subseteq \text{Br} X' \). \( \square \)

**Remark 6.8.8.** If in Corollary 6.8.7 we assume moreover that \( \dim X = \dim X' \leq 2 \), then \( \text{Br} X \simeq \text{Br} X' \); i.e., the caveat becomes unnecessary. See [Gro68d, Corollaire 7.5].

6.9. Examples of Brauer groups

6.9.1. Local rings and fields.

**Proposition 6.9.1.** Let \( R \) be a complete local ring with residue field \( k \). Then the quotient homomorphism \( R \to k \) induces an isomorphism \( \text{Br} R \to \text{Br} k \).

**Proof.** The (equivalent) analogue for \( \text{Br}_A \) was first proved in [Azu51, Theorem 31]. See [Mil80, III.3.11(a)] for a proof for \( \text{Br} k \). \( \square \)
Remark 6.9.2. Proposition 6.9.1 holds more generally for henselian local rings [Mil80, IV.2.13]. (See Section B.3 for the definition of henselian.) Even more generally, if \( R \) is henselian local ring with residue field \( k \), and \( G \) is a smooth commutative group scheme over \( R \), then \( H^q(R, G) \cong H^q(k, G) \) for all \( q \geq 1 \): see [Gro68d, equation (2.6)] for the case where \( R \) is a henselian discrete valuation ring, and [Mil80, III.3.11(b)] for the general case. For \( q = 1 \), we can formulate the same statement for noncommutative \( G \), and it is true [SGA 3, XXIV, Proposition 8.1].

Corollary 6.9.3. Let \( R \) be the valuation ring of a nonarchimedean local field \( K \). Then \( \text{Br} R = 0 \).

Proof. The residue field \( k \) is finite, so \( \text{Br} k = 0 \) by Theorem 1.5.32. Now use Proposition 6.9.1.

For \( R \) and \( K \) as in Corollary 6.9.3, we have \( H^1(k, \mathbb{Q}/\mathbb{Z}) = \text{Hom}_{\text{conts}}(\hat{\mathbb{Z}}, \mathbb{Q}/\mathbb{Z}) = \mathbb{Q}/\mathbb{Z} \), so the exact sequence of Proposition 6.8.1 becomes

\[
0 \to 0 \to \text{Br} K \xrightarrow{\text{res}} \mathbb{Q}/\mathbb{Z}.
\]

In fact, \( \text{res} \) is (up to sign) the homomorphism \( \text{inv}: \text{Br} K \to \mathbb{Q}/\mathbb{Z} \) in Theorem 1.5.34.

6.9.2. Rings of \( S \)-integers and arithmetic schemes.

Example 6.9.4. Let \( k \) be a global field. Let \( S \) be a nonempty set of places of \( k \) containing all the archimedean places. Let \( \mathcal{O}_{k,S} \) be as in Definition 1.1.1. For \( v \notin S \), let \( F_v \) be the residue field. Theorem 6.8.3 yields an exact sequence

\[
0 \to \text{Br} \mathcal{O}_{k,S} \to \text{Br} k \xrightarrow{\text{res}} \bigoplus_{v \notin S} H^1(F_v, \mathbb{Q}/\mathbb{Z}).
\]

By the previous discussion, the homomorphism \( \text{Br} k \to H^1(F_v, \mathbb{Q}/\mathbb{Z}) \) is the same as the homomorphism \( \text{inv}_v: \text{Br} k \to \mathbb{Q}/\mathbb{Z} \). Comparing with the description of \( \text{Br} k \) in Theorem 1.5.36(i) yields an exact sequence

\[
0 \to \text{Br} \mathcal{O}_{k,S} \to \bigoplus_{v \in S} \text{Br} k_v \xrightarrow{\sum \text{inv}_v} \mathbb{Q}/\mathbb{Z}.
\] (6.9.5)

Question 6.9.6 (M. Artin). If \( X \) is proper over \( \mathbb{Z} \), must \( \text{Br} X \) be finite? [Mil80, IV.2.19]

A positive answer to Question 6.9.6 in the special case of nice surfaces over finite fields would already have significant implications: see Theorem 7.6.8.

6.9.3. Curves.

Theorem 6.9.7. If \( X \) is a proper curve over a separably closed field \( k \), then \( \text{Br} X = 0 \).
Proof. If \( k \) is algebraically closed and \( X \) is nice, then this follows from Proposition 6.6.7(i) and Tsen’s theorem. For the general case, see [Gro68d, Corollaire 5.8]; the proof uses fppf cohomology. □

6.9.4. Rational varieties. Lemma 6.9.8 below will allow us to compute the Brauer group of \( \mathbb{P}^n_k \) and other rational varieties.

**Lemma 6.9.8.** Let \( \pi : X \to B \) be a morphism of regular integral noetherian schemes. Suppose that \( \pi \) has a section \( s : B \to X \), and that the generic fiber of \( \pi \) is isomorphic to \( \mathbb{P}^1_{k(B)} \) as a \( k(B) \)-scheme. Then \( \pi^* : \text{Br} B \to \text{Br} X \) is an isomorphism.

**Proof.** By functoriality, we have a diagram

\[
\begin{array}{ccc}
\text{Br} \mathbb{P}^1_{k(B)} & \xleftarrow{s^*} & \text{Br} X \\
\downarrow & & \downarrow \pi^* \\
\text{Br} k(B) & \xleftarrow{\pi^*} & \text{Br} B \\
\end{array}
\]

containing two commutative squares. By Proposition 6.6.7(i), we may view \( \text{Br} B \) as a subgroup of \( \text{Br} k(B) \). By Corollary 6.6.9, \( \text{Br} X \to \text{Br} \mathbb{P}^1_{k(B)} \) is injective. The left vertical homomorphism is an isomorphism by Theorem 6.9.7. Hence all four groups in the diagram may be viewed as subgroups of \( \text{Br} \mathbb{P}^1_{k(B)} \). Then \( \pi^* \) shows that \( \text{Br} B \subseteq \text{Br} X \), and \( s^* \) shows that \( \text{Br} X \subseteq \text{Br} B \). Thus \( \text{Br} B = \text{Br} X \).

**Proposition 6.9.9.** Let \( k \) be a field. Let \( n \in \mathbb{Z}_{\geq 0} \). Then \( \text{Br} k \to \text{Br} \mathbb{P}^n_k \).

**Proof.** We use induction on \( n \). The case \( n = 0 \) is trivial, so suppose that \( n \geq 1 \). Let \( P = (1 : 0 : \cdots : 0) \in \mathbb{P}^n(k) \), and let \( X \) be the blow-up of \( \mathbb{P}^n \) at \( P \). Projection from \( P \) is a rational map \( \mathbb{P}^n \to \mathbb{P}^{n-1} \) sending \((x_0 : x_1 : \cdots : x_n)\) to \((x_1 : \cdots : x_n)\), and it has a rational section sending \((x_1 : \cdots : x_n)\) to \((1 : x_1 : \cdots : x_n)\). Resolving the indeterminacy yields a morphism \( X \to \mathbb{P}^{n-1} \) with a section. Lemma 6.9.8 shows that \( \text{Br} X \simeq \text{Br} \mathbb{P}^{n-1} \), and the inductive hypothesis yields \( \text{Br} \mathbb{P}^{n-1} \simeq \text{Br} k \), so \( \text{Br} X \simeq \text{Br} k \).

By functoriality we have \( \text{Br} k \to \text{Br} \mathbb{P}^n \to \text{Br} X \), with the injectivity coming from Corollary 6.6.9. The previous paragraph showed that the composition is an isomorphism, so \( \text{Br} k \to \text{Br} \mathbb{P}^n \) is an isomorphism too. □

**Proposition 6.9.10.** Let \( X \) be a nice variety over a field \( k \). If \( X \) is birational to \( \mathbb{P}^n_k \) for some \( n \geq 0 \), then \( \text{Br} k \to \text{Br} X \).

**Proof.** If \( \text{char} k = 0 \), this follows from Proposition 6.9.9 and Corollary 6.8.7. For the general case, see [Sal85, Proposition 1.7 and the paragraph after Lemma 1.2]. □

**Corollary 6.9.11.** Let \( X \) be a nice variety over a field \( k \). If \( X_{k_s} \) is birational to \( \mathbb{P}^n_{k_s} \) for some \( n \geq 0 \), then \( \text{Br} X_{k_s} = 0 \) and \( \text{Br}_1 X = \text{Br} X \).
6.9.5. **Quadrics.** A *quadric* over a field $k$ is a degree 2 hypersurface in $\mathbb{P}^n_k$ for some $n \geq 2$.

**Proposition 6.9.12.** If $X$ is a smooth quadric over a field $k$, then $\text{Br}_k \to \text{Br}_X$ is surjective.

**Proof.** By Proposition 3.5.66, $X$ is geometrically integral. By Corollary 6.7.8 it will suffice to prove that $\text{Br}_X = 0$ and $H^1(\mathcal{O}_k, \text{Pic} X^s) = 0$. Corollary 6.9.11 yields $\text{Br}_X = 0$.

By [Har77, Exercise II.6.5(c) and Corollary II.6.16],

$$\text{Pic} X^s \simeq \begin{cases} \mathbb{Z} \times \mathbb{Z}, & \text{if } \dim X = 2 \\ \mathbb{Z}, & \text{if } \dim X = 1 \text{ or } \dim X \geq 3 \end{cases}$$

with $\mathcal{O}_{X^s}(1)$ corresponding to 2 if $\dim X = 1$, to $(1, 1)$ if $\dim X = 2$, and to 1 if $\dim X \geq 3$. If $\dim X = 1$ or $\dim X \geq 3$, then the Galois action on $\text{Pic} X^s \simeq \mathbb{Z}$ is trivial (ampleness must be preserved), so $H^1(\mathcal{O}_k, \text{Pic} X^s) = 0$.

Now suppose that $\dim X = 2$. If the $\mathcal{O}_k$-action on $\text{Pic} X^s \simeq \mathbb{Z} \times \mathbb{Z}$ is trivial, then $H^1(\mathcal{O}_k, \text{Pic} X^s) = 0$ again. If not, then $\text{Pic} X^s \simeq \mathbb{Z}[\mathcal{O}_k/\mathcal{O}_L]$ for some quadratic extension $L$ of $k$, so by Shapiro’s lemma, $H^1(\mathcal{O}_k, \text{Pic} X^s) = H^1(\mathcal{O}_L, \mathbb{Z}) = 0$. \qed

6.9.6. **Quadric bundles.**

**Lemma 6.9.13.** Let $k$ be a field of characteristic 0. Let $\pi: X \to B$ be a flat morphism of regular integral $k$-varieties. Let $\eta$ be the generic point of $B$. For $x \in X^{(1)}$ mapped by $\pi$ to some $b \in B^{(1)}$, the inclusion $k(b) \to k(x)$ induces a homomorphism $i_x: H^1(k(b), \mathbb{Q}/\mathbb{Z}) \to H^1(k(x), \mathbb{Q}/\mathbb{Z})$; also let $e_{x/b} \in \mathbb{Z}_{\geq 1}$ be the ramification index, and let $\epsilon_{x,b} = e_{x/b} i_x$. If $x \in X^{(1)}$ and $b \in B^{(1)}$ satisfy $\pi(x) \neq b$, then let $\epsilon_{x,b} = 0$. Together, these $\epsilon_{x,b}$ define a homomorphism $\epsilon$ in the diagram

$$
\begin{array}{cccccc}
0 & \longrightarrow & \text{Br} B & \longrightarrow & \text{Br} k(B) & \longrightarrow \bigoplus_{b \in B^{(1)}} H^1(k(b), \mathbb{Q}/\mathbb{Z}) \\
& & \downarrow \text{res} & & \downarrow & \\
0 & \longrightarrow & \text{Br} X & \longrightarrow & \text{Br} X_\eta & \longrightarrow \bigoplus_{x \in X^{(1)}, \pi(x) \neq \eta} H^1(k(x), \mathbb{Q}/\mathbb{Z}). \\
\end{array}
$$

(6.9.14)

This diagram commutes and has exact rows.

**Proof.** The first row is exact by Theorem 6.8.3. By Theorem 6.8.3, $\text{Br} X_\eta$ is cut out in $\text{Br} k(X)$ by the residue homomorphisms for $x \in X^{(1)}$ lying above $\eta$, while $\text{Br} X$ is cut out in $\text{Br} k(X)$ by the residue homomorphisms for all $x \in X^{(1)}$; thus the second row of (6.9.14)
is exact. The first square commutes since \( \text{Br} \) is a functor. The second square commutes by Exercise 6.12.

**Proposition 6.9.15.** Let \( k \) be a field of characteristic 0. Let \( \pi : X \to B \) be a flat morphism of regular integral \( k \)-varieties. Suppose that every fiber of \( \pi \) has an irreducible component of multiplicity 1 that is geometrically integral and that the generic fiber \( X_{k(B)} \) is a smooth quadric over \( k(B) \). Then \( \text{Br} B \to \text{Br} X \) is surjective.

**Proof.** Proposition 6.9.12 shows that the middle vertical homomorphism of (6.9.14) is surjective. Surjectivity of the left vertical homomorphism will follow from the four-lemma if the homomorphism \( \epsilon \) in (6.9.14) is injective.

Suppose that \( b \in B^{(1)} \). By hypothesis, the fiber \( X_b \) has an irreducible component \( Z \) of multiplicity 1 that is a geometrically integral \( k(b) \)-variety. Let \( x \) be the generic point of \( Z \). By flatness, \( x \in X^{(1)} \). By Proposition 2.2.19(i) \( \Rightarrow \) (iv), the extension \( k(x) \supseteq k(b) \) is primary, so the largest separable algebraic extension of \( k(b) \) in \( k(x) \) is \( k(b) \). Equivalently, by Galois theory, if we choose compatible separable closures \( k(b)_s \subseteq k(x)_s \), then the restriction homomorphism of absolute Galois groups \( G_{k(b)} \to G_{k(x)} \) is surjective. Applying \( \text{Hom}_{\text{conts}}(\_ , \mathbb{Q}/\mathbb{Z}) \) shows that \( i_x \) is injective. Also, \( e_{x/b} \) is the multiplicity of \( Z \), which is 1. Thus \( \epsilon_{x,b} = e_{x,b}i_x = i_x \), which is injective. Since for every \( b \in B^{(1)} \), there exists an \( x \) as above, \( \epsilon \) is injective. \( \square \)

**Exercises**

6.1. (Kummer sequence) Let \( X \) be a scheme, and let \( n \in \mathbb{Z}_{\geq 1} \). Consider the sequence of sheaves

\[
1 \longrightarrow \mu_n \longrightarrow \mathbb{G}_m \overset{n}{\longrightarrow} \mathbb{G}_m \longrightarrow 1
\]

on either \( X_{et} \) or \( X_{fppf} \), where \( \mu_n(U) \hookrightarrow \mathbb{G}_m(U) \) is the inclusion, and \( \mathbb{G}_m(U) \to \mathbb{G}_m(U) \) is the \( n \)th power homomorphism.

(a) Prove that the sequence is exact, when considered as a sequence of sheaves on \( X_{fppf} \).

(b) Give an example to show that it need not be exact, when considered as a sequence of sheaves on \( X_{et} \).

(c) Prove that if \( 1/n \in \mathcal{O}_X \) (that is, the image of \( n \) under \( \mathbb{Z} \to \mathcal{O}_X(X) \) is invertible), then the sequence is exact on \( X_{et} \).

6.2. Is it true that the groups \( H^q_{\text{Zar}}(X, \mathbb{G}_m) \) and \( H^q_{\text{et}}(X, \mathbb{G}_m) \) are isomorphic for all schemes \( X \) and all \( q \geq 0 \)?

6.3. Show that the general definition of “\( G \)-torsor over \( S \)” is equivalent, in the case where \( S = \text{Spec } k \) and \( G \) is a smooth algebraic group over \( k \), to the definition of “\( G \)-torsor over \( k \)” given earlier. (Hint: use the fact that smoothness is preserved by base extension and fpqc descent.)

6.4. Let \( k \) be an imperfect field of characteristic \( p \). Fix \( a \in k - k^p \), and let \( X = \text{Spec } k(a^{1/p}) \).
(a) Prove that $X$ can be made an $\alpha_p$-torsor over $k$.
(b) Prove that $X$ can also be made a $\mu_p$-torsor over $k$.

6.5. Let $k$ be a global field. Let $S$ be a finite nonempty set of places of $k$ containing all the archimedean places. Let $O_{k,S}$ be the ring of $S$-integers. Use familiar theorems of algebraic number theory to prove that $H^1_{\text{fppf}}(\text{Spec } O_{k,S}, \mu_n)$ is finite for each $n \geq 1$.

6.6. Let $\mathbb{H}$ be as in Example 1.5.8. Let $A = \mathbb{R}[x, y]/(x^2 + y^2)$ and let $K = \text{Frac } A$. Prove that the class $h$ of the Azumaya $A$-algebra $\mathbb{H} \otimes_{\mathbb{R}} A$ is a nonzero element of $\ker(\text{Br } A \to \text{Br } K)$.

6.7. Let $k$ be an algebraically closed field. Let $X$ be a nice $k$-curve of genus $g$. Let $n$ be a positive integer not divisible by $\text{char } k$. Using that $\text{Br } X = 0$, calculate $H^2_{et}(X, \mu_n)$ for $q = 0, 1, 2$. (You may assume the following fact: if $A$ is an abelian variety of dimension $g$ over an algebraically closed field $k$, and $(\text{char } k) \nmid n$, then the multiplication-by-$n$ homomorphism $A(k)^n \to A(k)$ is surjective and has kernel isomorphic to $(\mathbb{Z}/n\mathbb{Z})^{2g}$.)

6.8. Let $O$ be the ring of integers of a number field $k$. Using (6.9.5), show that $\text{Br } O$ is a finite abelian group, and compute its structure.

6.9. Let $k$ be a finite field. Let $X$ be a nice $k$-curve. Show that $\text{Br } X = 0$.

6.10. Let $X$ be a proper and geometrically integral variety over a field $k$. Assume that $X(k) \neq \emptyset$.
(a) Prove that the homomorphism $\text{Br } k \to \text{Br } X$ is injective.
(b) Prove that the homomorphism $\text{Pic } X \to (\text{Pic } X^s)^{\Phi_k}$ is an isomorphism.
(c) Show that the same two conclusions hold if $k$ is a global field and the hypothesis “$X(k) \neq \emptyset$” is weakened to “$X(k_v) \neq \emptyset$ for all places $v$ of $k$”.

6.11. (Brauer group of a conic) Let $k$ be a field. Let $X$ be a nice genus 0 curve over $k$. Let $c \in \text{Br } k$ be the class of $X$ viewed as a 1-dimensional Severi–Brauer variety. Prove that the homomorphism $\text{Br } k \to \text{Br } X$ is surjective with kernel generated by $c$. (Hint: use the theorem of Lichtenbaum mentioned in the proof of Proposition 4.5.12.)

6.12. (Functoriality of residue homomorphisms) Let $K \subseteq K'$ be an inclusion of fields. Suppose that $\nu: K \to \mathbb{Z} \cup \{\infty\}$ and $\nu': K' \to \mathbb{Z} \cup \{\infty\}$ are discrete valuations such that $\nu'|_K = e\nu$ for some $e \in \mathbb{Z}_{\geq 1}$ (called the ramification index). Let $R$ be the valuation ring in $K$, and let $k$ be the residue field. Let $R'$ be the valuation ring in $K'$, and let $k'$ be the residue field. The inclusion $k \hookrightarrow k'$ induces a homomorphism $i: H^1(k, \mathbb{Q}/\mathbb{Z}) \to H^1(k', \mathbb{Q}/\mathbb{Z})$. Then the diagram

$$
\begin{array}{c}
0 & \longrightarrow & \text{Br } R & \longrightarrow & \text{Br } K & \longrightarrow & H^1(k, \mathbb{Q}/\mathbb{Z}) \\
& & \downarrow & & \downarrow & & \downarrow e_i \\
0 & \longrightarrow & \text{Br } R' & \longrightarrow & \text{Br } K' & \longrightarrow & H^1(k', \mathbb{Q}/\mathbb{Z})
\end{array}
$$

(6.9.16)

commutes. (This may be viewed as a generalization of Theorem 1.5.34(ii).)
The Weil conjectures

(References: \[Har77\], Appendix C, \[FK88\])

The Weil conjectures give information about the number of points on varieties over finite fields. All of them have been proved.

7.1. Statements

Fix an algebraic closure \(\overline{\mathbb{Q}}\) of \(\mathbb{Q}\). Let \(\overline{\mathbb{Z}}\) be the integral closure of \(\mathbb{Z}\) in \(\overline{\mathbb{Q}}\).

**Theorem 7.1.1 (Weil conjectures).**

(i) Let \(X\) be a scheme of finite type over \(\mathbb{F}_q\). Then there exist \(\alpha_1, \ldots, \alpha_r, \beta_1, \ldots, \beta_s \in \overline{\mathbb{Z}}\) such that

\[
\#X(\mathbb{F}_q^n) = \alpha_1^n + \cdots + \alpha_r^n - \beta_1^n - \cdots - \beta_s^n
\]

for all \(n \geq 1\).

(ii) If \(X\) is a smooth proper variety of dimension \(d\) over \(\mathbb{F}_q\), then the plus and minus terms can be grouped as follows in alternating batches according to the absolute value of the terms:

\[
\#X(\mathbb{F}_q^n) = \sum_{j=1}^{b_0} \alpha_{0j}^n - \sum_{j=1}^{b_1} \alpha_{1j}^n + \sum_{j=1}^{b_2} \alpha_{2j}^n - \cdots + \sum_{j=1}^{b_{2d}} \alpha_{2dj}^n,
\]

where

- the \(b_i \in \mathbb{N}\) are the “\(\ell\)-adic Betti numbers”, and they satisfy \(b_{2d-i} = b_i\) for \(i = 0, \ldots, 2d\). (The terminology will be explained in Section 7.5.)
- the \(\alpha_{ij} \in \overline{\mathbb{Z}}\) are such that the \(\alpha_{2d-i,*}\) in the \((2d - i)\)-th batch equal the values \(q^{d/\alpha_{i,*}}\) in some order.
- \(|\alpha_{ij}| = q^{i/2}\) for all \(i\) and \(j\), for any archimedean absolute value \(|\cdot|\) on the number field \(\mathbb{Q}(\alpha_{ij})\). (This is called the Riemann hypothesis for \(X\) because of an analogy to be explained in Remark 7.4.4.)

If moreover \(X\) is geometrically irreducible, then

\[
b_0 = 1 \quad b_{2d} = 1 \quad \alpha_{01} = 1 \quad \alpha_{2d,1} = q^d.
\]

(iii) Let \(X\) be a smooth proper scheme over a finitely generated subring \(R\) of \(\mathbb{C}\). Let \(\mathfrak{m}\) be a maximal ideal of \(R\), so \(R/\mathfrak{m}\) is a finite field by Remark 2.4.5, and the reduction \(X_{R/\mathfrak{m}}\)
is a smooth proper scheme over $R/m$. Then for $i = 0, \ldots, 2d$, the $b_i$ in (iii) for $X_{R/m}$ equals $\text{rk} \, H^i(\mathbb{C}, \mathbb{Z})$, the $\mathbb{Z}$-rank of the singular cohomology group.

A typical choice of $R$ in (iii) is the ring of $S$-integers of a number field embedded in $\mathbb{C}$. Part (iii) is especially intriguing, in that it hints at a connection between singular cohomology and varieties over finite fields. This will be explained in Section 7.5.

7.2. The case of curves

If $X$ is a nice genus $g$ curve over $\mathbb{C}$, then

$$H^0(X(\mathbb{C}), \mathbb{Z}) \simeq \mathbb{Z}$$
$$H^1(X(\mathbb{C}), \mathbb{Z}) \simeq \mathbb{Z}^{2g}$$
$$H^2(X(\mathbb{C}), \mathbb{Z}) \simeq \mathbb{Z}.$$  

Analogously, if $X$ is a nice genus $g$ curve over $\mathbb{F}_q$, then it turns out that the $\ell$-adic Betti numbers of $X$ are

$$b_0 = 1$$
$$b_1 = 2g$$
$$b_2 = 1.$$  

The Weil conjectures in this case say that there exist $\lambda_1, \ldots, \lambda_{2g} \in \mathbb{Z}$ with $|\lambda_j| = q^{1/2}$ and $\lambda_{g+i} = q/\lambda_i$ for $i = 1, \ldots, g$, such that for all $n \geq 1$,

$$\#X(\mathbb{F}_{q^n}) = 1 - (\lambda_1^n + \cdots + \lambda_{2g}^n) + q^n.$$  

**Corollary 7.2.1 (Hasse–Weil bound).** Let $X$ be a nice genus $g$ curve over $\mathbb{F}_q$. Then

$$\#X(\mathbb{F}_q) = q + 1 - \epsilon$$

where the “error” $\epsilon$ is an integer satisfying $|\epsilon| \leq 2g\sqrt{q}$.

7.3. Zeta functions

(References: [Ser65][Tat65][Tat94])

7.3.1. The prototype: the Riemann zeta function.

(Reference: [Ahl78] Chapter 5, §4)

**Definition 7.3.1.** The Riemann zeta function is the meromorphic continuation of the holomorphic function defined for $s \in \mathbb{C}$ with $\text{Re} \, s > 1$ by

$$\zeta(s) := \sum_{n \geq 1} n^{-s}.$$
For future comparison to zeta functions of schemes, we recall some basic properties of $\zeta(s)$.

**Proposition 7.3.2.**

(i) The function $\zeta(s)$ is holomorphic on $\mathbb{C}$ except for a simple pole at $s = 1$.

(ii) There is a functional equation relating $\zeta(s)$ to $\zeta(1-s)$. More precisely, if $\Gamma$ denotes the gamma function [Ahl78, Chapter 5, §2.4], then the function $\xi(s) := \pi^{-s/2}\Gamma(s/2)\zeta(s)$ is entire and satisfies $\xi(s) = \xi(1-s)$.

(iii) The function $\zeta(s)$ vanishes at every negative even integer. The negative even integers are called the trivial zeros.

(iv) All other zeros of $\zeta(s)$ lie in the interior of the critical strip defined by $0 \leq \text{Re}(s) \leq 1$. The (unproven) Riemann hypothesis is the statement that these nontrivial zeros lie on the critical line defined by $\text{Re}(s) = 1/2$.

**Proof.**

(i) See [Ahl78, Chapter 5, §4.2].

(ii) See [Ahl78, Chapter 5, §4.3].

(iii) See [Ahl78, Chapter 5, end of §4.2].

(iv) See [Ahl78, Chapter 5, §4.4]. □

For $s \in \mathbb{C}$ with $\text{Re} \ s > 1$, the unique factorization of positive integers and the formula for an infinite geometric series let us rewrite $\zeta(s)$ as an Euler product:

$$
\zeta(s) := \sum_{n \geq 1} n^{-s} = \prod_{\text{primes } p} (1 - p^{-s})^{-1} = \prod_{\text{maximal ideals } m \subseteq \mathbb{Z}} (1 - (\#(\mathbb{Z}/m))^{-s})^{-1} = \prod_{\text{closed points } P \in \text{Spec } \mathbb{Z}} (1 - (\# k(P))^{-s})^{-1}.
$$

**Remark 7.3.3.** The factor $\pi^{-s/2}\Gamma(s/2)$ appearing in Proposition 7.3.2(ii) should be viewed as the analogue for the infinite place of $\mathbb{Q}$ of the Euler factor $(1 - p^{-s})^{-1}$ for a finite prime $p$.

**7.3.2. Schemes of finite type over $\mathbb{Z}$.**

**Definition 7.3.4.** If $X$ is a scheme of finite type over $\mathbb{Z}$, one defines the zeta function of $X$ as

$$
\zeta_X(s) := \prod_{\text{closed } P \in X} (1 - (\# k(P))^{-s})^{-1}.
$$
Remark 7.3.5. It is easy to show that $\zeta_X(s)$ converges in the half-plane $\{s \in \mathbb{C} : \text{Re}(s) > r\}$ for some $r \in \mathbb{R}$ depending on $X$ (see Exercise [7.2]), but less easy to find the smallest such $r$.

The Riemann zeta function $\zeta(s)$ is then $\zeta_{\text{Spec} \mathbb{Z}}(s)$. More generally, if $k$ is a number field and $\mathcal{O}_k$ is its ring of integers, then $\zeta_{\text{Spec} \mathcal{O}_k}(s)$ is called the Dedekind zeta function of $k$.

7.3.3. Schemes of finite type over a finite field. For schemes over a finite type over a finite field, there is a closely related definition.

Definition 7.3.6. Let $X$ be a scheme of finite type over $\mathbb{F}_q$. Define

$$Z_X(T) := \exp \left( \sum_{n \geq 1} \#X(\mathbb{F}_{q^n}) \frac{T^n}{n} \right) \in \mathbb{Q}[[T]].$$

Equivalently, $Z_X(T)$ is characterized by the equations

$$Z_X(0) = 1, \quad T \frac{d}{dT} \log Z_X(T) = \sum_{n \geq 1} \#X(\mathbb{F}_{q^n}) T^n.\tag{7.3.7}$$

Because of the following proposition, $Z_X(T)$ too is called the zeta function of $X$.

Proposition 7.3.8. If $X$ is a scheme of finite type over $\mathbb{F}_q$, then $X$ is also of finite type over $\mathbb{Z}$, and we have $\zeta_X(s) = Z_X(q^{-s})$.

Proof. See Exercise [7.3].

7.4. The Weil conjectures in terms of zeta functions

We can reformulate the Weil conjectures in terms of $Z_X(T)$, and in fact this is how they were originally expressed [Wei49, p. 507]:

Theorem 7.4.1 (restatement of Weil conjectures).

(i) Let $X$ be a scheme of finite type over $\mathbb{F}_q$. Then the power series $Z_X(T)$ is (the Taylor series of) a rational function in $\mathbb{Q}(T)$. The rational function will be of the form

$$\frac{(1 - \beta_1 T) \cdots (1 - \beta_s T)}{(1 - \alpha_1 T) \cdots (1 - \alpha_r T)},$$

for some $\alpha_1, \ldots, \alpha_r, \beta_1, \ldots, \beta_s \in \overline{\mathbb{Z}}$.

(ii) If $X$ is a smooth proper variety of dimension $d$ over $\mathbb{F}_q$, then

$$Z_X(T) = \frac{P_1(T) P_3(T) \cdots P_{2d-1}(T)}{P_0(T) P_2(T) P_4(T) \cdots P_{2d}(T)}.$$
where \( P_i \in 1 + T \mathbb{Z} [T] \) factors over \( \mathbb{C} \) as \( \prod_{j=1}^{b_i} (1 - \alpha_{ij} T) \), with \( |\alpha_{ij}| = q^{i/2} \) for any archimedean absolute value \( |\cdot| \) on the number field \( \mathbb{Q}(\alpha_{ij}) \) ("Riemann hypothesis"). Also, we have the functional equation

\[
Z_X \left( \frac{1}{q^{d/2} T} \right) = \pm q^{d x/2} T x Z_X (T),
\]

where \( \chi := b_0 - b_1 + b_2 - \cdots + b_{2d} \in \mathbb{Z} \) is the Euler characteristic of \( X \). (Equation (7.4.2) can be equivalently expressed as a functional equation relating \( \zeta_X (s) \) to \( \zeta_X (d - s) \), in analogy with Proposition 7.3.2ii.) The sign is specified in Exercise 7.4.) If in addition \( X \) is geometrically irreducible, then \( P_0 (T) = 1 - T \) and \( P_{2d} (T) = 1 - q^d T \).

**Remark 7.4.3.** The Euler characteristic \( \chi \) can also be defined geometrically, without reference to Betti numbers: it equals the self-intersection number \( \Delta \Delta \) where \( \Delta \subseteq X \times X \) is the diagonal (the graph of the identity morphism \( X \to X \)).

**Remark 7.4.4 (Riemann hypothesis for a curve over a finite field).** If \( X \) is a smooth proper curve, then the zeros of \( Z_X (T) \) satisfy \( |T| = q^{-1/2} \), so Proposition 7.3.8 implies that the zeros of \( \zeta_X (s) \) satisfy \( \text{Re}(s) = 1/2 \), in analogy with Proposition 7.3.2iv). This explains the use of the terminology "Riemann hypothesis" for varieties over finite fields.

### 7.5. Cohomological explanation

(Reference: [Del74 Sections 1 and 2])

#### 7.5.1. History.

Before Weil’s work, the Weil conjectures were already known for curves over finite fields, by work of E. Artin, Hasse, and Schmidt, except that the Riemann hypothesis was known only for curves of genus \( \leq 1 \). Weil was led to his conjectures by this work, and by his own proof of the Riemann hypothesis for curves of arbitrary genus [Wei48a] and for certain varieties of higher dimension such as diagonal hypersurfaces [Wei49].

Weil’s proof for curves proceeded by adapting the theory of correspondences to varieties in characteristic \( p \). As Hasse observed in 1936, the problem of determining \( \#X (\mathbb{F}_q^n) \) can be converted into a purely geometric problem: namely, if \( F \) is the relative \( q \)-power Frobenius morphism on \( X_{\mathbb{F}_q} \), then \( \#X (\mathbb{F}_q^n) \) equals the number of fixed points of \( F^n \). Weil reinterpreted this number as the intersection number of two curves in \( X \times X \), namely, the graphs of the identity and \( F^n \).

On the other hand, Lefschetz and Hopf had given a topological “trace formula” for the number of fixed points of a map from a compact manifold to itself, in terms of the action of the map on the associated singular cohomology spaces; this showed that the number of fixed points of powers of an endomorphism of a complex projective variety (assuming
nondegeneracy) would be given by a formula such as that in Theorem 7.1.1(i). Weil’s hope was that the theory of correspondences would serve in characteristic \( p \) as a substitute for the singular cohomology theory, given that correspondences had served him so well in the case of curves. Such a “motivic” approach (to use anachronistic terminology), however, has never been completed.

Instead, others, starting with Serre and Grothendieck in the 1950s, sought to develop an algebraic analogue of singular cohomology rich enough to accommodate a trace formula that would explain the Weil conjectures. It was this thinking that motivated the development of étale cohomology by Grothendieck, M. Artin, Verdier, and Deligne. Étale cohomology eventually proved the conjectures in full, even though the first of the conjectures, the rationality, was originally proved by a different method without cohomology, by Dwork [Dwo60].

For a more detailed account of the history of the Weil conjectures, see [Die75]. For an even more detailed account of the early history, see [Roq02, Roq04, Roq06].

7.5.2. The Lefschetz trace formula in topology. Let \( X \) be a compact differentiable real manifold of dimension \( d \). Let \( f : X \to X \) be a differentiable map. A fixed point of \( f \) is a point \( x \in X \) such that \( f(x) = x \). At such a point, the derivative \( df_x \) is an endomorphism of the tangent space \( T_x X \). Call a fixed point \( x \in X \) nondegenerate if \( 1 - df_x \) is invertible, where 1 is the identity endomorphism; this condition should be thought of as saying that the fixed point is of “multiplicity 1”.

For \( i \geq 0 \), the singular cohomology group \( H^i(X, \mathbb{Z}) \) is a finitely generated abelian group, and tensoring with \( \mathbb{Q} \) yields a finite-dimensional \( \mathbb{Q} \)-vector space isomorphic to \( H^i(X, \mathbb{Q}) \). Its dimension \( b_i \) is called the \( i \)th Betti number of \( X \). Then \( f \) induces a \( \mathbb{Q} \)-linear endomorphism \( f^* \) of each \( H^i(X, \mathbb{Q}) \), and its trace is an integer because the endomorphism comes from an endomorphism of \( H^i(X, \mathbb{Z}) \).

**Theorem 7.5.1 (Lefschetz trace formula).** With notation as above, if all fixed points of \( f \) are nondegenerate, then

\[
\# \{ \text{fixed points of } f \} = \sum_{i \geq 0} (-1)^i \text{tr} \left( f^*|H^i(X, \mathbb{Q}) \right).
\]

The alternating sum of traces is actually a finite sum since \( H^i(X, \mathbb{Q}) = 0 \) for \( i > d = \text{dim } X \).

**Definition 7.5.2.** From now on, in this and similar situations, we use the abbreviations

\[
\text{tr}(f|H^*(X, \mathbb{Q})) := \sum_{i \geq 0} (-1)^i \text{tr} \left( f^*|H^i(X, \mathbb{Q}) \right)
\]

\[
\det(1 - Tf|H^*(X, \mathbb{Q})) := \prod_{i \geq 0} \det \left( 1 - Tf^*|H^i(X, \mathbb{Q}) \right)^{(-1)^i},
\]

where \( T \) is an indeterminate.
The following is a simplified version of Poincaré duality, stated in a form suitable for adaptation to the étale setting.

**Theorem 7.5.3 (Poincaré duality).** If $X$ is an oriented connected compact real differentiable manifold of dimension $d$, then $H^d(X, \mathbb{Q}) \simeq \mathbb{Q}$, and there are cup-product pairings

$$H^i(X, \mathbb{Q}) \times H^{d-i}(X, \mathbb{Q}) \to H^d(X, \mathbb{Q}) \simeq \mathbb{Q}$$

that are perfect pairings for each $i$. In particular, $b_i = b_{d-i}$ for each $i$.

If $X$ is a connected compact complex manifold of complex dimension $d$, then $X$ is automatically oriented, and its dimension as a real manifold is $2d$.

**7.5.3. Some $\ell$-adic cohomology.** If $n \in \mathbb{Z}$, we write $1/n \in \mathcal{O}_X$ to mean that the image of $n$ in $\Gamma(X, \mathcal{O}_X)$ is a unit, or equivalently, that each point of $X$ has residue field of characteristic not dividing $n$.

**Definition 7.5.4.** Let $X$ be a scheme. Fix a prime $\ell$ with $1/\ell \in \mathcal{O}_X$. For $i \in \mathbb{N}$, define

$$H^i(X, \mathbb{Z}_\ell) := \varprojlim H^i_{et}(X, \mathbb{Z}/\ell^n\mathbb{Z}).$$

(To simplify notation, we omit the subscript $et$.) When equipped with the profinite topology, this is a continuous $\mathbb{Z}_\ell$-module. Also define a $\mathbb{Q}_\ell$-vector space

$$H^i(X, \mathbb{Q}_\ell) := H^i(X, \mathbb{Z}_\ell) \otimes \mathbb{Q}_\ell.$$

These definitions will be applied especially when $X$ is a variety over a separably closed field, since it is this case that models most closely the singular cohomology of a complex variety. If $X$ is a variety over a smaller field, typically one forms the base extension $X_K$ for some separably closed field $K \supseteq k$ before taking its cohomology; one can show that the resulting cohomology is unchanged upon passing from one separably closed field to a larger one, so it does not matter much which $K$ is chosen.

**Example 7.5.5.** Let $A$ be a $g$-dimensional abelian variety over a field $k$. Let $\ell$ be a prime not equal to char $k$. The **Tate module** of $A$ is defined by

$$T_\ell A := \text{Hom}_{\mathbb{Z}}(\mathbb{Q}_\ell/\mathbb{Z}_\ell, A(k_s)) = \varprojlim A(k_s)[\ell^n],$$

where each homomorphism $A(k_s)[\ell^{n+1}] \to A(k_s)[\ell^n]$ in the inverse system is multiplication-by-$\ell$. It turns out that $T_\ell A$ is a free $\mathbb{Z}_\ell$-module of rank $2g$ equipped with a continuous action of $\mathfrak{S}_k$. It acts as if it were an “étale homology group $H^1_{et}(A_{k_s}, \mathbb{Z}_\ell)$ in the sense that its $\mathbb{Z}_\ell$-dual $\text{Hom}_{\mathbb{Z}_\ell}(T_\ell A, \mathbb{Z}_\ell)$ is canonically isomorphic to $H^1(A_{k_s}, \mathbb{Z}_\ell)$, as it turns out. See Exercise 7.5 for another way in which $T_\ell A$ acts like homology. One also defines $V_\ell A := (T_\ell A) \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell$. 

194
Remark 7.5.6. More generally, it turns out that for any smooth proper variety $X$ over a separably closed field $k$, for any prime $\ell \neq \text{char } k$, and any $i \geq 0$, the $\mathbb{Z}_\ell$-module $H^i(X, \mathbb{Z}_\ell)$ is finitely generated. Its rank, which by definition equals $\dim_{\mathbb{Q}_\ell} H^i(X, \mathbb{Q}_\ell)$, is called the $i^{\text{th}}$ $\ell$-adic Betti number $b_i$ of $X$. This is in analogy with Section 7.5.2.

If $k$ is not separably closed, one generally base-extends $X$ to $k_s$ or $\overline{k}$ before defining its Betti numbers.

Remark 7.5.7. There is another approach to defining étale cohomology with $\mathbb{Z}_\ell$ or $\mathbb{Q}_\ell$ coefficients, via the pro-étale topology: see [BS15].

7.5.4. Tate twists. There is a “twisted” variant of $\ell$-adic cohomology:

Definition 7.5.8. Let $X$ be a scheme, and let $n \in \mathbb{Z}_{>0}$ be such that $1/n \in \mathcal{O}_X$. For $m \in \mathbb{Z}$, the Tate twist $(\mathbb{Z}/n\mathbb{Z})(m)$ is a sheaf on $X_{et}$ defined as follows:

$$(\mathbb{Z}/n\mathbb{Z})(m) := \begin{cases} 
\mathbb{Z}/n\mathbb{Z}, & \text{if } m = 0, \\
(\mu_n)^{\otimes m}, & \text{if } m > 0, \\
\text{Hom}(\mu_n^{\otimes (-m)}, \mathbb{Z}/n\mathbb{Z}), & \text{if } m < 0.
\end{cases}$$

Again fix a prime $\ell$ with $1/\ell \in \mathcal{O}_X$. Also fix $m \in \mathbb{Z}$. For each $n \geq 0$, there is a natural surjection $(\mathbb{Z}/\ell^{n+1}\mathbb{Z})(m) \to (\mathbb{Z}/\ell^n\mathbb{Z})(m)$. (For example, when $m = 1$, it is the $\ell$th-power homomorphism $\mu_{\ell^{n+1}} \to \mu_{\ell^n}$.) For $i \in \mathbb{N}$ and $m \in \mathbb{Z}$, define

$$H^i(X, \mathbb{Z}_\ell(m)) := \varprojlim_n H^i_{et}(X, (\mathbb{Z}/\ell^n\mathbb{Z})(m))$$

$$H^i(X, \mathbb{Q}_\ell(m)) := H^i(X, \mathbb{Z}_\ell(m)) \otimes \mathbb{Q}_\ell.$$

When $X = \text{Spec } k$, one can also view $(\mathbb{Z}/n\mathbb{Z})(m)$, $\mathbb{Z}_\ell(m)$, and $\mathbb{Q}_\ell(m)$ as continuous $\mathfrak{G}_k$-modules. In particular, $\mathbb{Q}_\ell(m)$ is a 1-dimensional continuous character of $\mathfrak{G}_k$, and $\mathbb{Q}_\ell(1)$ is called the cyclotomic character.

Suppose that $k$ is separably closed. Then $k$ contains all $\ell$-power roots of unity. If we choose generators $\zeta_{\ell^n}$ of the abelian group $\mu_{\ell^n}$ for all $n \geq 1$ compatibly (i.e., such that $\zeta_{\ell^{n+1}} = \zeta_{\ell^n}$), then we obtain compatible isomorphisms $\mathbb{Z}/\ell^n\mathbb{Z} \to \mu_{\ell^n}$ and $\mathbb{Z}_\ell \to \mathbb{Z}_\ell(1)$ and $\mathbb{Q}_\ell \to \mathbb{Q}_\ell(1)$. Thus the Tate twists do nothing.

Now let $k$ be an arbitrary field. The previous paragraph shows that $H^i(X_{k_s}, \mathbb{Q}_\ell(m))$ and $H^i(X_{k_s}, \mathbb{Q}_\ell)$ are isomorphic as abelian groups. But they may differ when the action of $\mathfrak{G}_k$ is taken into account; the precise relationship is as follows:

Proposition 7.5.9. There is an isomorphism of $\mathbb{Q}_\ell$-representations of $\mathfrak{G}_k$

$$H^i(X_{k_s}, \mathbb{Q}_\ell(m)) \simeq H^i(X_{k_s}, \mathbb{Q}_\ell) \otimes_{\mathbb{Q}_\ell} \mathbb{Q}_\ell(m).$$

Proof. A choice of generator $\zeta$ of $(\mathbb{Z}/\ell^n\mathbb{Z})(m)$ (viewed as a subgroup of $(k_s^\times)^{\otimes m}$) defines an isomorphism of sheaves $\mathbb{Z}/\ell^n\mathbb{Z} \to (\mathbb{Z}/\ell^n\mathbb{Z})(m)$ on $X_{k_s}$ and hence an isomorphism of abelian
groups $H^i(X_{k_0}, \mathbb{Z}/\ell^n \mathbb{Z}) \rightarrow H^i(X_{k_0}, (\mathbb{Z}/\ell^n \mathbb{Z})(m))$. This defines a isomorphism of abelian groups

$$H^i(X_{k_0}, \mathbb{Z}/\ell^n \mathbb{Z}) \otimes_{\mathbb{Z}/\ell^n \mathbb{Z}} (\mathbb{Z}/\ell^n \mathbb{Z})(m) \rightarrow H^i(X_{k_0}, (\mathbb{Z}/\ell^n \mathbb{Z})(m)),$$

and it is independent of the choice of $\zeta$ and hence $\mathfrak{G}_k$-equivariant. Take inverse limits and tensor with $\mathbb{Q}_\ell$. □

7.5.5. The Lefschetz trace formula in étale cohomology. If $X$ is a scheme of finite type over a separably closed field, and $d := \text{dim } X$, then it turns out that $H^i(X, \mathbb{Q}_\ell) = 0$ for all $i$ outside the range $0 \leq i \leq 2d$ (this is a consequence of [SGA 4III, X, Corollaire 4.3]).

Theorem 7.5.10 (Grothendieck–Lefschetz trace formula). Let $X$ be a smooth proper variety over an algebraically closed field $k$. Fix a prime $\ell \neq \text{char } k$. Let $f : X \rightarrow X$ be a $k$-morphism such that each fixed point in $X(k)$ is nondegenerate (in the same sense as in Section 7.5.2, but using the Zariski tangent space). Then

$$\# \{\text{fixed points of } f \text{ in } X(k)\} = \text{tr} (f|H^r(X, \mathbb{Q}_\ell)).$$

in $\mathbb{Q}_\ell$, where the right hand side is defined as in Definition 7.5.2.


Remark 7.5.11. More generally, without the nondegeneracy hypothesis, the formula remains true if we replace the left hand side by the intersection number $\Gamma . \Delta$ computed in $X \times X$, where $\Gamma$ is the graph of $f$, and $\Delta$ is the diagonal [SGA 4] Cycle, Corollaire 3.7.

Theorem 7.5.12 (Poincaré duality in $\ell$-adic cohomology). Let $X$ be a smooth proper integral variety of dimension $d$ over a separably closed field $k$. Fix a prime $\ell \neq \text{char } k$.

(a) There is a natural isomorphism $H^{2d}(X, \mathbb{Q}_\ell(d)) \simeq \mathbb{Q}_\ell$.

(b) Cup product defines a perfect pairing

$$H^r(X, \mathbb{Q}_\ell(i)) \times H^{2d-r}(X, \mathbb{Q}_\ell(d-i)) \rightarrow H^{2d}(X, \mathbb{Q}_\ell(d)) \simeq \mathbb{Q}_\ell$$

for each $r, i \in \mathbb{Z}$.

Proof. This is a consequence of [Mil80, VI.11.2]. □

Remark 7.5.13. As at the end of Section 7.5.4, the Tate twists do not change the $\mathbb{Q}_\ell$-vector spaces; they only change the Galois action in the setting that $X$ comes from a variety defined over a subfield $k_0 \leq k$. For fixed $r$, Proposition 7.5.9 shows that if Theorem 7.5.12 holds for some $i$, then it holds for all $i$.

7.5.6. Arithmetic and geometric Frobenius. Fix a power $q$ of a prime $p$. Define the arithmetic Frobenius $\sigma$ to be the field automorphism of $\overline{F}_q$ given by $\sigma(a) = a^q$. Write $\sigma$ also for the induced morphism $\text{Spec } \overline{F}_q \rightarrow \text{Spec } F_q$. 196
Let $X$ be a smooth proper variety over $\mathbb{F}_q$. Let $\overline{X} = X \times_{\mathbb{F}_q} \overline{\mathbb{F}}_q$. The field automorphism $\sigma$ gives rise to an automorphism

$$\overline{X} = X \times_{\mathbb{F}_q} 1 \times \sigma \quad X \times_{\mathbb{F}_q} = \overline{X}.$$ 

Let $F_{\overline{X}} : \overline{X} \to \overline{X}$ be the absolute $q$-power Frobenius morphism. Finally, let $F = F_{\overline{X}/\mathbb{F}_q} : \overline{X} \to \overline{X}$ be the relative $q$-power Frobenius morphism (Remark 3.7.6).

The diagram (3.7.1) for $\overline{X} \to \text{Spec} \overline{\mathbb{F}}_q$ (with $q$ in place of $p$) is

(7.5.14)

$\overline{X} \xrightarrow{F} \overline{X} \xrightarrow{1 \times \sigma} \overline{X} \xrightarrow{\sigma} \text{Spec} \overline{\mathbb{F}}_q.$

**Warning 7.5.15.** Of the three morphisms $F$, $F_{\overline{X}}$, and $1 \times \sigma$, only $F$ is a morphism of $\mathbb{F}_q$-varieties, and usually only $1 \times \sigma$ is an automorphism.

**Warning 7.5.16.** Diagram (7.5.14) for $\overline{X} \to \text{Spec} \overline{\mathbb{F}}_q$ is not the same as the base extension by $\text{Spec} \overline{\mathbb{F}}_q \to \text{Spec} \mathbb{F}_q$ of the corresponding diagram for $X \to \text{Spec} \mathbb{F}_q$. For example, the absolute Frobenius $F_{\overline{X}}$ is different from the base extension of $F_X$.

The $\mathbb{Q}_\ell$-vector space $H^i(\overline{X}, \mathbb{Q}_\ell)$ is finite-dimensional by Remark 7.5.6. By contravariant functoriality, each morphism of schemes $\overline{X} \to \overline{X}$ (not necessarily an $\overline{\mathbb{F}}_q$-morphism) induces a $\mathbb{Q}_\ell$-linear endomorphism of $H^i(\overline{X}, \mathbb{Q}_\ell)$. We compare these for the three morphisms at the top of (7.5.14).

**Proposition 7.5.17.** Let $X$ be a smooth proper variety over $\mathbb{F}_q$. With notation as above, the endomorphism of $H^i(\overline{X}, \mathbb{Q}_\ell)$ induced by the relative Frobenius morphism $F$ is the inverse of the endomorphism induced by $1 \otimes \sigma$.

**Proof.** Lemma 3.7.5 applied to étale morphisms to $\overline{X}$ implies that $F_{\overline{X}}$ acts as the identity on the category of étale $\overline{X}$-schemes, and hence as the identity on $H^i(\overline{X}, \mathbb{Q}_\ell)$. Now the result follows from (7.5.14). □

Because of Proposition 7.5.17, the field automorphism $\sigma^{-1} \in \text{Aut} \mathbb{F}_q$ and the corresponding automorphism $1 \times \sigma^{-1}$ of $\overline{X}$ are both called geometric Frobenius (cf. [Del74, 1.15]).

**7.5.7. Deducing the Weil conjectures.** Let $X$ be a smooth proper variety of dimension $d$ over $\mathbb{F}_q$. Let $\overline{X} = X_{\overline{\mathbb{F}}_q}$. Let $F : \overline{X} \to \overline{X}$ be the relative $q$-power Frobenius morphism. Then $\#X(\mathbb{F}_q^n)$ is the number of fixed points of the $n$th iterate $F^n$. Also, the derivative of $F$
is everywhere 0, so fixed points of $F$ and its powers are automatically nondegenerate. So applying the Grothendieck–Lefschetz trace formula (Theorem 7.5.10) to $X$ and $F^n$ yields

$$\#X(F_q^n) = \text{tr} \left( F^n|H^*(X, \mathbb{Q}_\ell) \right). \quad \text{(7.5.18)}$$

Thus

$$Z_X(T) = \exp \left( \sum_{n \geq 1} \frac{\#X(F_q^n)}{n} T^n \right) \quad \text{(Definition 7.3.6)}$$

$$= \exp \left( \sum_{n \geq 1} \text{tr} \left( F^n|H^*(X, \mathbb{Q}_\ell) \right) \frac{T^n}{n} \right)$$

$$= \det \left( 1 - TF|H^*(X, \mathbb{Q}_\ell) \right)^{-1} \quad \text{(by Exercise 7.6)}$$

$$= \frac{P_1(T) P_5(T) \cdots P_{2d-1}(T)}{P_0(T) P_2(T) P_4(T) \cdots P_{2d}(T)} ,$$

where

$$P_i(t) := \det \left( 1 - TF|H^i(X, \mathbb{Q}_\ell) \right) \in \mathbb{Q}_\ell[T].$$

In particular, $Z_X(T)$ is a rational function in $\mathbb{Q}_\ell(T)$. But $Z_X(T)$ is also in $1 + T \mathbb{Z}[[T]]$ by Proposition 7.3.8 so $Z_X(T) \in \mathbb{Q}(T)$.

For each $i$,

$$P_i(t) = \prod_{j=1}^{b_i} (1 - \alpha_{ij} T),$$

where $b_i := \dim H^i(X, \mathbb{Q}_\ell)$, and $\alpha_{i1}, \ldots, \alpha_{ib_i}$ are the eigenvalues of $F^*|H^i(X, \mathbb{Q}_\ell)$ counted with multiplicity. The $\alpha_{ij}$ turn out to be nonzero, so $\deg P_i = b_i$.

The identity $1_X : X \to X$ induces the identity on each space $H^i(X, \mathbb{Q}_\ell)$, so Remark 7.5.11 applied to $1_X$ yields

$$\Delta.\Delta = \sum_{i=0}^{2d} (-1)^i b_i = \chi,$$

as claimed in Remark 7.4.3.

Now suppose in addition that $\overline{X}$ is integral. Twisting the isomorphism in Theorem 7.5.12[a] by $-d$ shows that

$$H^{2d}(\overline{X}, \mathbb{Q}_\ell) \simeq \mathbb{Q}_\ell(-d).$$

In particular, $b_{2d} = 1$. With notation as in Section 7.5.6, Proposition 7.5.17 shows that $F^*$ acts on $H^{2d}(\overline{X}, \mathbb{Q}_\ell)$ as $\sigma^{-1}$ acts on $\mathbb{Q}_\ell(-d)$, i.e., as multiplication by $q^d$. The Galois equivariance of the perfect pairing in Theorem 7.5.12[b] shows that the eigenvalues $\alpha_{2d-i,*}$ of $F^*$ (or $\sigma^{-1}$) on $H^{2d-i}(\overline{X}, \mathbb{Q}_\ell)$ are the inverses of the eigenvalues of $\sigma^{-1}$ acting on $H^i(\overline{X}, \mathbb{Q}_\ell(d))$; the latter eigenvalues are $\alpha_i/q^d$, because of the twist. This explains the functional equation.
The relationship between $\ell$-adic Betti numbers and classical Betti numbers arises from a theorem comparing $\ell$-adic and singular cohomology for a $\mathbb{C}$-variety, and a theorem about how $H^i(X, \mathbb{Q}_\ell)$ behaves under specialization.

All that remains is to prove that each eigenvalue $\alpha_{ij}$ is an algebraic integer with $|\alpha_{ij}| = q^{i/2}$; this was shown by Deligne using further properties of $\ell$-adic cohomology; see [Del74, Théorème 1.6] and [Del80, Théorème 2]. See also [Kat76] for an overview of the proof.

### 7.5.8. Non-proper varieties

**Remark 7.5.19.** The cohomological approach generalizes to $\mathbb{F}_q$-varieties that are not proper. The Grothendieck–Lefschetz trace formula holds for a variety over a separably closed field once one replaces $H^r(X, \mathbb{Q}_\ell)$ with “cohomology with compact support” $H^r_c(X, \mathbb{Q}_\ell)$; cf. [Gro68a] and [Del74, Théorème 2.8]. And for a smooth integral variety of dimension $d$ over a separably closed field, Poincaré duality gives a perfect pairing

$$H^r_c(X, \mathbb{Q}_\ell(i)) \times H^{2d-r}(X, \mathbb{Q}_\ell(d-i)) \longrightarrow H^{2d}_c(X, \mathbb{Q}_\ell(d)) \simeq \mathbb{Q}_\ell$$

involving both kinds of cohomology; cf. [SGA 4III, XVIII, Théorème 2.14 and (3.2.6.2)].

**Lemma 7.5.20.** Let $X$ be a $d$-dimensional variety over a separably closed field $k$. If $U \subseteq X$ is a dense open subscheme, then the restriction map $H^{2d}_c(X, \mathbb{Q}_\ell(d)) \to H^{2d}_c(U, \mathbb{Q}_\ell(d))$ is an isomorphism.

**Proof.** This is a consequence of [SGA 4III, XVIII, Lemme 2.1].

**Corollary 7.5.21.** Let $X$ be a $d$-dimensional variety over a separably closed field $k$. Then $H^{2d}_c(X, \mathbb{Q}_\ell(d))$ is naturally the $\mathbb{Q}_\ell$-vector space having as basis the set of $d$-dimensional irreducible components of $X$.

**Proof.** Lemma 7.5.20 lets us replace $X$ by a dense open subscheme so that its irreducible components are disjoint. Then the statement reduces to the irreducible case already mentioned in Remark 7.5.19.

### 7.6. Cycle class homomorphism

In this section, $X$ is a variety that is smooth of dimension $d$ over a field $k$. We will occasionally impose more restrictive conditions.

#### 7.6.1. Algebraic cycles

(Reference: [Ful98, Chapter 1])

The group $\text{Pic} X$ may be identified with the group of Weil divisors modulo linear equivalence. And by definition, a Weil divisor is an integer combination of integral closed subschemes of codimension 1. We now generalize to higher codimension.
For \( r \in \mathbb{N} \), the group of codimension \( r \) cycles, denoted \( \mathcal{Z}^r(X) \), is defined as the free abelian group on the set of codimension \( r \) integral closed subschemes of \( X \). For instance, \( \mathcal{Z}^1(X) \) is the group of Weil divisors on \( X \). If \( r > d \), then \( \mathcal{Z}^r(X) = 0 \).

For each codimension \( r \) integral closed subscheme \( Z \), let \( [Z] \in \mathcal{Z}^r(X) \) denote the basis element corresponding to \( Z \). More generally, if \( Y \subseteq X \) is any closed subscheme whose irreducible components \( Y_i \) are of codimension \( r \) in \( X \), let \( y_i \) be the generic point of \( Y_i \), let \( \ell_i \) be the length of the artinian ring \( \mathcal{O}_{Y,y_i} \), and define \( [Y] := \sum \ell_i [Y_i] \in \mathcal{Z}^r(X) \).

There is a notion of rational equivalence of cycles that for \( r = 1 \) becomes linear equivalence of divisors, and the Chow group \( \text{CH}^r(X) \) is the group of codimension \( r \) cycles modulo rational equivalence; see [Ful98] Sections 1.3 and 1.6, where \( \text{CH}^r(X) \) is denoted by \( A^r(X) \). For instance, \( \text{CH}^1(X) = \text{Pic} X \).

**7.6.2. Changing the base field.** Given a field extension \( L \supseteq k \), there is a base change homomorphism \( \mathcal{Z}^r(X) \to \mathcal{Z}^r(X_L) \) sending each basis element \( [Z] \) to \( [Z_L] \). Even though \( Z \) is integral, \( Z_L \) might not be, so \( [Z_L] \) must be defined in terms of lengths as in Section 7.6.1.

**Proposition 7.6.1.** Let \( L \supseteq k \) be an extension of fields. Let \( X \) be a smooth \( k \)-variety. Let \( r \in \mathbb{N} \).

(a) The homomorphism \( \mathcal{Z}^r(X) \to \mathcal{Z}^r(X_L) \) is injective.

(b) If \( L \) is Galois over \( k \) with Galois group \( G \), then the homomorphism \( \mathcal{Z}^r(X) \to \mathcal{Z}^r(X_L)^G \) is an isomorphism.

**Proof.**

(a) For \( Z \) varying over codimension \( r \) integral closed subschemes of \( X \), the subschemes \( Z_L \) are nonempty and do not share irreducible components, so the classes \( [Z_L] \) are linearly independent.

(b) Consider a \( G \)-orbit of codimension \( r \) integral closed subscheme of \( X_L \), and let \( Y \) be their union, a closed subscheme of \( X_L \). Although descent of schemes is not in general effective, in the present setting we can descend the ideal sheaf of \( Y \) to show that \( Y = Z_L \) for some closed subscheme \( Z \subseteq X \). If \( Z \) were not reduced, then \( Y \) would not be reduced either. If \( Z \) were not irreducible, then \( Y \) would not consist of exactly one \( G \)-orbit. Thus \( Z \) is integral, and \([Z]\) maps to \([Y]\). Such classes \([Y]\) form a basis of \( \mathcal{Z}^r(X_L)^G \), so \( \mathcal{Z}^r(X) \to \mathcal{Z}^r(X_L)^G \) is an isomorphism. \( \square \)

**7.6.3. Cohomology classes of divisors.** Taking cohomology of the Kummer sequence

\[
1 \longrightarrow \mu_{\ell^n} \longrightarrow \mathbb{G}_m^{\ell^n} \longrightarrow \mathbb{G}_m \longrightarrow 1
\]

of sheaves on \( X_{\text{et}} \) yields a connecting homomorphism

\[
\text{Pic} X = H^1(X, \mathbb{G}_m) \longrightarrow H^2(X, (\mathbb{Z}/\ell^n\mathbb{Z})(1)).
\]
These are compatible as $n$ varies, so we obtain homomorphisms
\[(7.6.2) \quad \text{Pic } X \to H^2(X, \mathbb{Z}_\ell(1)) \to H^2(X, \mathbb{Q}_\ell(1)),\]
whose composition will be denoted $\text{cl}_{\text{et}}$.

### 7.6.4. Cohomology classes of higher-codimension cycles

In this section, $k$ is algebraically closed. Let $Z \subseteq X$ be an integral closed subscheme of codimension $r$, so $\dim Z = d - r$. Our goal is to define a cohomology class $\text{cl}_{\text{et}}(Z) \in H^{2r}(X, \mathbb{Q}_\ell(r))$.

**Case 1: X and Z are nice.** The inclusion $Z \hookrightarrow X$ induces
\[(7.6.3) \quad H^{2d-2r}(X, \mathbb{Q}_\ell(d-r)) \to H^{2d-2r}(Z, \mathbb{Q}_\ell(d-r)) \approx \mathbb{Q}_\ell,
\]
by Theorem 7.5.12(a) for $Z$. By Theorem 7.5.12(b) for $X$, this linear functional corresponds to an element of $H^{2r}(X, \mathbb{Q}_\ell(r))$ denoted $\text{cl}_{\text{et}}(Z)$.

**Case 2: X and Z are smooth and integral.** Replace (7.6.3) by
\[H_c^{2d-2r}(X, \mathbb{Q}_\ell(d-r)) \to H_c^{2d-2r}(Z, \mathbb{Q}_\ell(d-r)) \approx \mathbb{Q}_\ell,
\]
which again by Poincaré duality (Remark 7.5.19) defines an element $\text{cl}_{\text{et}}(Z) \in H^{2r}(X, \mathbb{Q}_\ell(r))$. (In fact, Case 1 was unnecessary since it is subsumed by Case 2.)

**Case 3: X smooth and integral, Z integral.** Let $X' = X - Z^{\text{sing}}$ and $Z' = Z - Z^{\text{sing}}$. Case 2 defines $\text{cl}_{\text{et}}(Z') \in H^{2r}(X', \mathbb{Q}_\ell(r))$. Using the fact that $X'$ differs from $X$ only in a subset of codimension $> r$, one can show that the map $H^{2r}(X, \mathbb{Q}_\ell(r)) \to H^{2r}(X', \mathbb{Q}_\ell(r))$ is an isomorphism (cf. SGA 4 1/2, Cycle, 2.2.10]). Let $\text{cl}_{\text{et}}(Z)$ be the element of $H^{2r}(X, \mathbb{Q}_\ell(r))$ corresponding to $\text{cl}_{\text{et}}(Z') \in H^{2r}(X', \mathbb{Q}_\ell(r))$.

**Case 4: X smooth, Z integral (the general case).** Extending $\mathbb{Z}$-linearly, and taking direct sums over the components of $X$ if $X$ is not integral, we obtain a **cycle class homomorphism**
\[\text{cl}_{\text{et}} : Z^r(X) \to H^{2r}(X, \mathbb{Q}_\ell(r)).\]

Rationally equivalent cycles have the same image under $\text{cl}_{\text{et}}$; in other words, $\text{cl}_{\text{et}}$ factors through the quotient $\text{CH}^r(X)$. Even better, **algebraically** equivalent cycles have the same image under $\text{cl}_{\text{et}}$ SGA 4 1/2, Cycle, Remarque 2.3.10].

The homomorphism $\text{CH}^1(X) \to H^2(X, \mathbb{Q}_\ell(1))$ is the same as the homomorphism (7.6.2).

### 7.6.5. The Tate conjecture

(Reference: Tat94)

Which cohomology classes in $H^{2r}(X, \mathbb{Q}_\ell(r))$ are in the image of $\text{cl}_{\text{et}}$, or at least in the $\mathbb{Q}_\ell$-span of the image? The Tate conjecture attempts to answer this question. It is analogous to the Hodge conjecture, which, for a smooth projective $\mathbb{C}$-variety, attempts to describe the $\mathbb{Q}$-span of the image of the analogous cycle class homomorphism from $Z^r(X)$ to the singular cohomology group $H^{2r}(X(\mathbb{C}), \mathbb{Q})$. 201
Let $X$ be a nice variety over a field $k$ that is not necessarily algebraically closed. Let $\mathcal{G} = \text{Gal}(k_s/k) = \text{Aut}(k/k)$. Fix $r \geq 0$. The homomorphisms

$$Z^r(X_{k_s}) \rightarrow Z^r(X_{\bar{k}}) \xrightarrow{\text{cl}_{\ell}} H^{2r}(X_{\bar{k}}, \mathbb{Q}_{\ell}(r)) \simeq H^{2r}(X_{k_s}, \mathbb{Q}_{\ell}(r))$$

are $\mathcal{G}$-equivariant, and taking $\mathcal{G}$-invariants yields a homomorphism

$$Z^r(X) \rightarrow H^{2r}(X_{k_s}, \mathbb{Q}_{\ell}(r))^\mathcal{G},$$

by Proposition [7.6.1][b]. Extending $\mathbb{Q}_{\ell}$-linearly yields a $\mathbb{Q}_{\ell}$-linear cycle class homomorphism (7.6.4)

$$Z^r(X) \otimes \mathbb{Q}_{\ell} \xrightarrow{\text{cl}_{\ell}} H^{2r}(X_{k_s}, \mathbb{Q}_{\ell}(r))^\mathcal{G}.$$

**Conjecture 7.6.5 (Tate conjecture).** Let $k$ be a finitely generated field (i.e., finitely generated as a field over $\mathbb{F}_p$ or $\mathbb{Q}$). Let $X$ be a nice variety over $k$. Then the cycle class homomorphism (7.6.4) is surjective.

Conjecture 7.6.5 implies a variant for $X_{k_s}$ instead of $X$, as we explain in the rest of this section.

**Definition 7.6.6.** The space of **algebraic classes** is the image of

$$Z^r(X_{k_s}) \otimes \mathbb{Q}_{\ell} \xrightarrow{\text{cl}_{\ell}} H^{2r}(X_{k_s}, \mathbb{Q}_{\ell}(r)).$$

The space of **Tate classes** is

$$\bigcup_{\text{open } H \leq \mathcal{G}} H^{2r}(X_{k_s}, \mathbb{Q}_{\ell}(r))^H,$$

where the union is over all (finite-index) open subgroups $H$ of the Galois group $\mathcal{G}$.

Every algebraic class is a Tate class. If Conjecture 7.6.5 holds for $X_L$ for every finite separable extension $L \supseteq k$ contained in $k_s$, then the converse holds.

**Remark 7.6.7.** Like the Hodge conjecture, the Tate conjecture is interesting because it predicts the existence of algebraic cycles in situations where there is no known way to construct them.

### 7.6.6. The Tate conjecture and the Birch and Swinnerton-Dyer conjecture.

(References: [Tat95a], [KT03])

**Theorem 7.6.8.** The following statements are equivalent:

(i) The Tate conjecture for divisors (the $r = 1$ case) on nice surfaces over finite fields holds.

(ii) For every nice surface $X$ over a finite field, $\text{Br} X$ is finite.

(iii) For every abelian variety $A$ over a global function field, $\text{III}(A)$ is finite.

(iv) The rank part of the Birch and Swinnerton-Dyer conjecture for abelian varieties over global function fields (the formula $\text{ord}_{s=1} L(A, s) = \text{rk} A(K)$) holds.
(v) The full Birch and Swinnerton-Dyer conjecture (Remark 5.7.34) for abelian varieties over global function fields holds.

Sketch of proof. The equivalence of these statements was proved by Artin and Tate, under some assumptions, and excluding the $p$-parts of some groups, where $p$ is the characteristic \[\text{Tat95a}.\] But since then the work of many people \[\text{Gro68d, Mil75, Mil81, Sch82, Bau92, KT03}\] proved the equivalence in full generality, as we now sketch.

\[\text{(i)} \iff \text{(ii)}:\] For each nice surface $X$ over a finite field $k$ and for each prime $\ell \neq \text{char } k$, the truth of the Tate conjecture for divisors on $X$ in $\ell$-adic cohomology is equivalent to the finiteness of $(\text{Br } X)[\ell^\infty]$ \[\text{Tat95a, Theorem 5.2(i)}\], and the finiteness of $(\text{Br } X)[\ell^\infty]$ implies the finiteness of the whole group $\text{Br } X$ (see \[\text{Mil75, Theorem 4.1}\] and \[\text{LLR05, p. 674, footnote}\]).

\[\text{(iii)} \Rightarrow \text{(ii)}:\] Let $X$ be a nice surface over a finite field $k$. There exists a nice curve $B$ over $k$ and a rational map $f : X \to B$ whose generic fiber $X_\eta$ (a variety over the global function field $k(B)$) is nice. In proving finiteness of $\text{Br } X$, Remark 6.8.8 lets us replace $X$ by a blow-up, so we may assume that $f$ is a morphism. Let $J$ be the Jacobian of $X_\eta$. In this context, $\text{Br } X$ is finite if and only if $X(J)$ is finite \[\text{Gro68d, Section 4}\].

\[\text{(ii)} \Rightarrow \text{(iii)}:\] Suppose that $A$ is an abelian variety over a global function field $K$. By Proposition 2.4, $A$ is a quotient of the Jacobian $J$ of some nice curve $C$ over $K$. Spread out $C$ to show that $C = X_\eta$ for some $X \to B$ as in the previous paragraph. Then finiteness of $\text{Br } X$ implies finiteness of $\text{III}(J)$, which implies finiteness of $\text{III}(A)$ (because $J$ is isogenous to $A \times A'$ for some $A'$, and finiteness of $\text{III}$ is invariant under isogeny).

\[\text{(iii) } \iff \text{(iv) and (iv)} \iff \text{(v)}:\] See \[\text{KT03, 1.8, Theorem}\].

7.7. Applications to varieties over global fields

7.7.1. Uniform estimates for the number of points over finite fields. The following application of the Weil conjectures is a variant of \[\text{LW54, Theorem 1}\].

**Theorem 7.7.1 (Lang–Weil).** Let $\pi : X \to Y$ be a morphism between schemes of finite type over $\mathbb{Z}$. For what follows, let $q$ be a prime power, let $y \in Y(\mathbb{F}_q)$, let $X_y$ be the fiber $\pi^{-1}(y)$ (i.e., the $\mathbb{F}_q$-scheme obtained by pulling back $\pi$ by $\text{Spec } \mathbb{F}_q \to Y$), and let $d = \dim X_y$. All implied constants below depend on $\pi : X \to Y$ but not on $q$, $y$, or $d$. We have

\[\begin{align*}
\text{(i) } & \#X_y(\mathbb{F}_q) = O(q^d). \\
\text{(ii) } & \text{If the } \mathbb{F}_q\text{-scheme } X_y \text{ is geometrically irreducible, then } \#X_y(\mathbb{F}_q) = q^d + O(q^{d-1/2}). \\
\text{(iii) } & \text{If } q \text{ is sufficiently large and } X_y \text{ is geometrically irreducible, then } X_y \text{ has an } \mathbb{F}_q\text{-point.} \\
\text{(iv) } & \text{If } q \text{ is sufficiently large and } X_y \text{ is geometrically integral, then } X_y \text{ has a smooth } \mathbb{F}_q\text{-point.}
\end{align*}\]

Sketch of proof.
(i) We may assume that $X$ and $Y$ are affine; then in particular each $X_y$ is separated. We may also assume that a prime $\ell$ is invertible on $X$ and $Y$, because in each, the open subschemes where two different $\ell$ are invertible cover the whole scheme. The result now follows from

- the generalized Lefschetz trace formula of Remark \[7.5.19\],
- a uniform bound on $\dim H^i_c(X_y, \mathbb{Q}_\ell)$ as $y$ varies [Kat01, Theorem 1], and
- the bound $q^{i/2}$ on the absolute values of the eigenvalues of the relative $q$-power Frobenius morphism on $H^i_c(X_y, \mathbb{Q}_\ell)$ [Del80, Théorème 1].

Alternatively, by fibering a variety into curves and using induction on the dimension, one can reduce to the case in which $X \to Y$ is a family of curves, in which case one does not need the ingredients above, but just the Weil conjectures for curves; this is the original argument of [LW54].

(ii) Combine the proof of (i) with the isomorphism $H^2_c(V, \mathbb{Q}_\ell(d)) \simeq \mathbb{Q}_\ell$ of Corollary \[7.5.21\] for a $d$-dimensional geometrically irreducible finite-type $\mathbb{F}_q$-scheme $V$. (Alternatively, one can again follow [LW54] and reduce to the case of curves.)

(iii) If $q$ is sufficiently large, then $q^d + O(q^{d-1/2}) > 0$.

(iv) Let $U$ be the smooth locus of $X \to Y$. If $X_y$ is geometrically integral, then so is its smooth locus $U_y$, by Proposition \[3.5.63\]. So (iv) follows from (iii) for $U \to Y$. □

7.7.2. Existence of local points. Recall the notation for global fields introduced in Section \[1.1.3\].

**Theorem 7.7.2.** Let $k$ be a global field. Let $X$ be a geometrically integral $k$-variety. Then $X(k_v)$ is nonempty for all but finitely many $v \in \Omega_k$.

**Proof.** There exists a finite subset $S \subseteq \Omega_k$ containing all archimedean places such that $X$ spreads out to a separated finite-type $\mathcal{O}_{k,S}$-scheme $\mathcal{X}$ with geometrically integral fibers. By Theorem 7.7.1(iv), for almost all $v \in \text{Spec} \mathcal{O}_{k,S}$, there is a point in $\mathcal{X}(\mathbb{F}_v)$ at which the morphism $\mathcal{X} \to \text{Spec} \mathcal{O}_{k,S}$ is smooth. By Hensel’s lemma (Theorem \[3.5.62\][a]), this point lifts to an element of $\mathcal{X}(\mathcal{O}_v) \subseteq \mathcal{X}(k_v) = X(k_v)$. □

**Remark 7.7.3.** Given $X$ as in Theorem 7.7.2, one can algorithmically determine a finite subset $S \subseteq \Omega_k$ such that $X(k_v)$ is nonempty for all $v \notin S$ (in practice, it might be easiest to begin by replacing $X$ by a geometrically integral curve in $X$). If $k$ is a number field, then in principle one can also determine whether $X(k_v)$ is nonempty for each of the finitely many $v \in S$: this was mentioned already in Remark \[2.6.4\].

7.7.3. Embedding finitely generated algebras into local fields.

(Reference: [Cas86, Chapter 5])

204
Theorem 7.7.4. Let $A$ be an integral domain of characteristic 0 that is finitely generated as a $\mathbb{Z}$-algebra. Let $k$ be the constant field of Frac $A$, so $k$ is a finite extension of $\mathbb{Q}$ (see Section 2.2.4). Then for all but finitely many $v \in \Omega_k$, there exists an embedding $A \hookrightarrow \mathcal{O}_v$.

Proof. Let $X = \text{Spec } A$. Let $X = \text{Spec}(\mathbb{Q}A)$, which is a geometrically integral $k$-variety by Propositions 2.2.19 and 2.2.20. We may replace $A$ by $A[1/f]$ for some nonzero $f \in A$ to assume that $X$ is as in the proof of Theorem 7.7.2, so $X^{\text{smooth}}$ has an $\mathcal{O}_v$-point for all but finitely many $v$. For any such $v$, Remark 3.5.75 yields a point in the open subset $X(\mathcal{O}_v)$ of $X(k)$ lying outside the countably many subvarieties $g = 0$ defined by nonzero $g \in A$. Any such $\mathcal{O}_v$-point is a homomorphism $A \to \mathcal{O}_v$ killing no nonzero $g \in A$. □

Corollary 7.7.5. Let $A$ be an integral domain of characteristic 0 that is finitely generated as a $\mathbb{Z}$-algebra. Then there are infinitely many primes $p$ such that $A$ embeds in $\mathbb{Z}_p$.

Proof. With notation as in Theorem 7.7.4, there are infinitely many places $v$ of $k$ that are unramified of degree 1 over $\mathbb{Q}$; then $\mathcal{O}_v \simeq \mathbb{Z}_p$. There are only finitely many $v$ above each $p$, so infinitely many primes $p$ occur. □

In the context of Corollary 7.7.5 for some applications one would like to force particular nonzero elements $a_1, \ldots, a_n \in A$ to map to units in $\mathbb{Z}_p$. To arrange this, apply Corollary 7.7.5 to $A[a_1^{-1}, \ldots, a_n^{-1}]$.

Corollary 7.7.6. Let $B$ be an integral domain that is also a finitely generated $\mathbb{Q}$-algebra. Then there are infinitely many primes $p$ such that $B$ embeds in $\mathbb{Q}_p$.

Proof. Choose $\mathbb{Q}$-algebra generators of $B$, and let $A$ be the $\mathbb{Z}$-subalgebra they generate. Apply Corollary 7.7.5 to $A$. If $A$ embeds in $\mathbb{Z}_p$, then its localization $B = \mathbb{Q}A$ embeds in $\mathbb{Q}\mathbb{Z}_p = \mathbb{Q}_p$. □

Corollaries 7.7.5 and 7.7.6 make it possible to reduce many questions over characteristic 0 fields to questions over $\mathbb{Z}_p$ or $\mathbb{Q}_p$. See Exercises 7.9 and 7.10 for examples.

Exercises

7.1. Find the smallest $g \geq 0$ such that there exists a finite field $\mathbb{F}_q$ and a nice curve $X$ of genus $g$ over $\mathbb{F}_q$ such that $X(\mathbb{F}_q)$ is empty.

7.2. (Convergence of zeta functions) Let $X$ be a scheme of finite type over $\mathbb{Z}$.
   (a) Prove that there is a polynomial $f(x)$ such that for every $q \geq 1$, the number of closed points $P \in X$ with $\#k(P) = q$ is less than or equal to $f(q)$.
   (b) Deduce that there exists $r \in \mathbb{R}$ such that the product defining $\zeta_X(s)$ converges for all $s \in \mathbb{C}$ with $\text{Re}(s) > r$.

7.3. Use Exercise 2.13 to prove Proposition 7.3.8.
7.4. Let notation be as in Theorem 7.4.1(ii). Let \( \mu \) be the multiplicity of \(-q^{d/2}\) as a zero of \( P_d(T) \). Assuming Theorem 7.1.1(ii), prove that

\[
Z_X \left( \frac{1}{q^d T} \right) = (-1)^{x+\mu} q^{d x/2} T^x Z_X(T).
\]

7.5. Let \( A \) be an abelian variety over \( \mathbb{C} \), so \( A(\mathbb{C}) \cong \mathbb{C}^g / \Lambda \) for some rank \( 2g \) discrete \( \mathbb{Z} \)-submodule \( \Lambda \) in \( \mathbb{C}^g \), and \( \Lambda \cong \text{H}^1(A(\mathbb{C}), \mathbb{Z}) \). Let \( \ell \) be any prime. Prove that there is a natural isomorphism of \( \mathbb{Z}_\ell \)-modules \( T_\ell A \cong \Lambda \otimes \mathbb{Z}_\ell \). (“Natural” means that it should be functorial with respect to abelian variety homomorphisms \( A \rightarrow B \).

7.6. Let \( V \) be a finite-dimensional vector space over a field \( k \) of characteristic 0. Let \( F : V \rightarrow V \) be an endomorphism. Then

\[
\exp \left( \sum_{n \geq 1} \text{tr}(F^n) \frac{T^n}{n} \right) = \det(1 - TF)^{-1}
\]

in \( k[[T]] \).

7.7. Prove that given \( n \geq 1 \), if \( p \) is sufficiently large (relative to \( n \)), then for any \( \epsilon_1, \ldots, \epsilon_n \in \{1, -1\} \), there exists \( x \in \mathbb{Z} \) such that for all \( i \in \{1, 2, \ldots, n\} \), the Legendre symbol \( \left( \frac{x+\epsilon_i}{p} \right) \) equals \( \epsilon_i \).

7.8. Generalize Theorem 7.7.1(ii): Show that if the hypothesis that \( X_y \) is geometrically irreducible is dropped, then \( \#X_y(\mathbb{F}_q) = C q^d + O(q^{d-1/2}) \), where \( C \) is the number of \( d \)-dimensional irreducible components of \( X_y \) that are geometrically irreducible.

7.9. (a) Let \( p \) be an odd prime, and let \( n \geq 1 \). Let \( N \in \text{M}_n(\mathbb{Z}_p) \). For each \( r \geq 1 \), prove that \( (1 + p^r N)^p \equiv 1 + p^{r+1} N \pmod{p^{r+2}} \).

(b) Prove that the group \( 1 + p \text{M}_n(\mathbb{Z}_p) \) of \( \text{GL}_n(\mathbb{Z}_p) \) is torsion-free; that is, its only element of finite order is the identity.

(c) (Selberg) Let \( k \) be a field of characteristic 0. Prove that any finitely generated subgroup \( G \) of \( \text{GL}_n(k) \) has a torsion-free finite-index subgroup.

(d) Does the previous statement hold for all fields of all characteristics?

7.10. (a) Let \( p \) be an odd prime. Let \( b \in 1 + p\mathbb{Z}_p \). Prove that there is a \( p \)-adic power series \( f \in \mathbb{Z}_p[[n]] \) with radius of convergence greater than 1 such that \( f(n) = b^n \) for all \( n \in \mathbb{Z} \). (Hint: Use properties of the \( p \)-adic logarithm and exponential maps in [Kob84 IV.1].)

(b) Let \( b \in \mathbb{Z}_p^* \). Prove that there are \( p \)-adic power series \( f_0, \ldots, f_{p-2} \in \mathbb{Z}_p[[n]] \) such that \( f_c(n) = b^{(p-1)n+c} \) for all \( c \in \{0, \ldots, p-2\} \) and \( n \in \mathbb{Z} \).

(c) A sequence \( (a_n)_{n \geq 0} \) in a field \( k \) is called a **linear recursive sequence** if there exist \( r \geq 1 \) and \( c_{r-1}, \ldots, c_0 \in k \) such that

\[
a_{n+r} = c_{r-1}a_{n+r-1} + \cdots + c_0a_n
\]
for all \( n \geq 0 \). Prove that if \( \text{char } k = 0 \), then there exist a nonnegative integer \( s \), polynomials \( p_1, \ldots, p_s \in \overline{k}[n] \), and elements \( b_1, \ldots, b_s \in \overline{k}^\times \) such that

\[
a_n = p_1(n) b_1^n + \cdots + p_s(n) b_s^n
\]

for all sufficiently large \( n \).

(d) The **Skolem–Mahler–Lech theorem** states that for any linear recursive sequence \( (a_n) \) in a field \( k \) of characteristic 0, the set \( \{n : a_n = 0\} \) is a finite union of arithmetic progressions and singletons. Prove it. (Hint: A \( p \)-adic power series with radius of convergence greater than 1 is either identically zero or has only finitely many zeros in \( \mathbb{Z}_p \).)

(e) Give an algorithm that takes as input the specification \((r, c_0, \ldots, c_{r-1}, a_0, \ldots, a_{r-1})\) of a linear recursive sequence \( (a_n)_{n \geq 0} \) of integers, and outputs YES if there exists \( n \) such that \( a_n = 0 \) and NO otherwise. (Warning: This is an unsolved problem! No such algorithm is known, and it may be that no such algorithm exists — that is, it could be undecidable.)
CHAPTER 8

Cohomological obstructions to rational points

In 1970, Manin [Man71] explained how, for a variety $X$ over a global field $k$, elements of $\text{Br} X$ could produce obstructions to the local-global principle. Meanwhile, Fermat’s method of infinite descent was generalized to show how a torsor under an algebraic group $G$ over $X$ could give rise to an obstruction, by Chevalley and Weil [CW30] for finite $G$, by Colliot-Thélène and Sansuc [CTS77, CTS80, CTS87] for commutative $G$, and by Harari and Skorobogatov [HS02] for general $G$. In this chapter, we will explain these and related obstructions.

8.1. Obstructions from functors

8.1.1. The $F$-obstruction to the local-global principle. Let $k$ be a global field, and let $A$ be its adele ring. Let $F : \text{Schemes}^\text{op} \to \text{Sets}$ be a functor. For a $k$-algebra $L$, write $F(L)$ for $F(\text{Spec} L)$. Let $X$ be a $k$-variety.

Suppose that $A \in F(X)$. For each $k$-algebra $L$, define $\text{ev}_A : X(L) \to F(L)$ as follows: given $x \in X(L)$, the corresponding morphism $\text{Spec} L \to X$ induces a map $F(X) \to F(L)$, sending $A$ to some element of $F(L)$ called $\text{ev}_A(x)$ or $A(x)$. Then the diagram

\[
\begin{array}{ccc}
X(k) & \longrightarrow & X(A) \\
\text{ev}_A \downarrow & & \downarrow \text{ev}_A \\
F(k) & \longrightarrow & F(A)
\end{array}
\]

(8.1.1)

commutes. Let $X(A)^A$ be the subset of $X(A)$ consisting of elements whose image in $F(A)$ lies in the image of $F(k) \to F(A)$. Then (8.1.1) shows that $X(k) \subseteq X(A)^A$. In other words, $A$ puts constraints on the locus in $X(A)$ where $k$-points can lie.

Imposing the constraints for all $A \in F(X)$ yields the subset $X(A)^F = X(A)^{F(X)} := \bigcap_{A \in F(X)} X(A)^A$, again containing $X(k)$.

**Definition 8.1.2.** If $X(A) \neq \emptyset$, but $X(A)^F = \emptyset$, then we say that there is an $F$-obstruction to the local-global principle; in this case $X(k) = \emptyset$.

8.1.2. The $F$-obstruction to weak approximation. We have $X(A) \subseteq X(\prod k_v) = \prod X(k_v)$; cf. Exercise 3.4. (If $X$ is proper, then all three sets are equal.) There is a variant of Definition 8.1.2 in which $X(A)$ is replaced by $X(\prod k_v) = \prod X(k_v)$ and $F(A)$ is replaced by $\prod F(k_v)$ in (8.1.1); call the resulting set $X(\prod k_v)^F$. 

208
Definition 8.1.3. If \( X(\prod k_v)^F \neq X(\prod k_v) \), we say that there is an \textit{F-obstruction to weak approximation}. Usually this terminology is used in a context where \( X(\prod k_v)^F \) is known to be closed in \( X(\prod k_v) \), in which case such an F-obstruction would imply that \( X(k) \) is not dense in \( X(\prod k_v) \).

8.1.3. Examples. In order for the F-obstruction to be nontrivial, \( F \) must be such that \( F(k) \to F(A) \) is not surjective. In order for the F-obstruction to be useful, the image of \( F(k) \to F(A) \) must be describable in some way. This is so in the following two examples, as will be explained in subsequent sections.

Example 8.1.4. Taking \( F = Br \) defines the \textbf{Brauer set} \( X(A)^{Br} \).

Example 8.1.5. Taking \( F = H^1(\_, G) \) for an affine algebraic group \( G \) over \( k \) defines a set \( X(A)^{H^1(X,G)} \).

Remark 8.1.6. To avoid having to understand the Brauer group of a non-noetherian ring like \( A \), in Section 8.2 we will replace \( Br A \) in (8.1.1) by \( \bigoplus_v Br k_v \) when defining \( X(A)^{Br} \); this in fact, was the original definition. It turns out that the natural homomorphism \( Br A \to \bigoplus_v Br k_v \) is an isomorphism \cite{Ces15}, so the resulting set \( X(A)^{Br} \) is the same. Similarly, we replace \( H^1(A,G) \) by \( \prod_v H^1(k_v,G) \) in Section 8.4; the natural map \( H^1(A,G) \to \prod_v H^1(k_v,G) \) is an injection (a consequence of \cite{Ces15}, Theorem 2.18), so again the resulting set \( X(A)^{H^1(X,G)} \) is the same.

Question 8.1.7. Are there other functors that one could use to obtain obstructions?

8.1.4. Functoriality. The proofs of the following three statements are left to the reader, as Exercise 8.1.

Proposition 8.1.8. Let \( \pi : X' \to X \) be a morphism of \( k \)-varieties. Let \( x' \in X'(L) \) for some \( k \)-algebra \( L \) and let \( A \in F(X) \). Then the two ways of evaluating \( A \) on \( x' \) yield the same result: if \( x := \pi(x) \in X(L) \) and \( A' := \pi^* A \in F(X') \), then \( A'(x') = A(x) \) in \( F(L) \).

Corollary 8.1.9. The assignment \( X \mapsto X(A)^F \) is functorial in \( X \).

Corollary 8.1.10. Let \( \pi : X' \to X \) be a morphism of \( k \)-varieties. If \( F(X) \to F(X') \) is surjective, then \( X'(A)^F \) is the inverse image of \( X(A)^F \) under \( X'(A) \to X(A) \).

8.2. The Brauer–Manin obstruction

Throughout this section, \( k \) is a field, and \( X \) is a \( k \)-variety.

8.2.1. Evaluation. Let \( A \in Br X \). If \( L \) is a \( k \)-algebra and \( x \in X(L) \), then \( Spec L \xrightarrow{x} X \) induces a homomorphism \( Br X \to Br L \), which maps \( A \) to an element of \( Br L \) that we call \( A(x) \); cf. Section 8.1.1.
8.2.2. The Brauer set.

(Reference: [Sko01, §5.2])

Now suppose that $k$ is a global field. Fix $A \in \text{Br } X$.

**Proposition 8.2.1.** If $(x_v) \in X(A)$, then $A(x_v) = 0$ for almost all $v$.

**Proof.** By Corollary 6.6.11, for some finite set of places $S$ (containing all the archimedean places), we can spread out $X$ to a finite-type $\mathcal{O}_{k,S}$-scheme $\mathcal{X}$ and spread out $A$ to an element $A \in \text{Br } \mathcal{X}$. Enlarging $S$ if necessary, we may also assume that $x_v \in X(\mathcal{O}_v)$ for all $v \notin S$. Then $A(x_v)$ comes from an element $A(x_v) \in \text{Br } \mathcal{O}_v$. But $\text{Br } \mathcal{O}_v = 0$ by Corollary 6.9.3. □

Thus $A$ determines a map

$$X(A) \longrightarrow \mathbb{Q}/\mathbb{Z}$$

$$(x_v) \longmapsto (A, (x_v)) := \sum_v \text{inv}_v(A(x_v)).$$

**Proposition 8.2.2.** If $x \in X(k) \subseteq X(A)$, then $(A, x) = 0$.

**Proof.** Use the commutativity of

$$
\begin{array}{cccc}
X(k) & \xrightarrow{\sim} & X(A) \\
\downarrow & & \downarrow \\
\text{Br } k & \xrightarrow{\bigoplus_v \text{Br } k_v} & \sum \text{inv}_v & \longrightarrow \mathbb{Q}/\mathbb{Z} & \longrightarrow 0.
\end{array}
$$

(8.2.3)

**Remark 8.2.4.** Compare (8.2.3) with (8.1.1).

**Definition 8.2.5.** For $A \in \text{Br } X$, define

$$X(A)^A := \{ (x_v) \in X(A) : (A, (x_v)) = 0 \}.$$

Also define

$$X(A)^{\text{Br}} := \bigcap_{A \in \text{Br } X} X(A)^A.$$

This agrees with the definition in Example 8.1.4 because of Remark 8.1.6.

**Corollary 8.2.6.** We have $X(k) \subseteq X(A)^{\text{Br}}$.

**Proof.** This is a restatement of Proposition 8.2.2. □

8.2.3. The Brauer–Manin obstruction to the local-global principle.

**Definition 8.2.7.** One says that there is a Brauer–Manin obstruction to the local-global principle for $X$ if $X(A) \neq \emptyset$, but $X(A)^{\text{Br}} = \emptyset$. 210
**Definition 8.2.8.** For a class of nice varieties $X$ over global fields, one says that the Brauer–Manin obstruction to the local-global principle is the only one if the implication

$$X(\mathbb{A})^{Br} \neq \emptyset \implies X(k) \neq \emptyset$$

holds.

See Conjecture 9.2.27 for a setting in which it is conjectured that the Brauer–Manin obstruction to the local-global principle is the only one.

**8.2.4. Brauer evaluation is locally constant.**

**Proposition 8.2.9.** Let $k$ be a local field. Let $X$ be a $k$-variety. Let $A \in \text{Br} X$.

(a) The map $X(k) \to \text{Br} k$ sending $x$ to $A(x)$ is locally constant with respect to the analytic topology on $X(k)$.

(b) If $k = \mathbb{R}$, the map $X(\mathbb{R}) \to \text{Br} \mathbb{R}$ is constant on each connected component of $X(\mathbb{R})$.

**Proof.**

(a) Given $\alpha \in \text{Br} k$, we need to show that $\{ x \in X(k) : A(x) = \alpha \}$ is open in $X(k)$. The structure morphism $X \to \text{Spec} k$ induces a homomorphism $\text{Br} k \to \text{Br} X$, which sends $\alpha$ to a “constant” element $\alpha_X \in \text{Br} X$. Replacing $A$ by $A - \alpha_X$ subtracts $\alpha$ from all the values $A(x)$. Thus we may reduce to showing that $\{ x \in X(k) : A(x) = 0 \}$ is open in $X(k)$.

Let $x_0 \in X(k)$. Consider pairs $(Y, y)$ where $Y$ is an étale $X$-scheme, $Y$ is affine, and $y \in Y(k)$ maps to $x_0 \in X(k)$. Let $R$ be the direct limit of $\mathcal{O}(Y)$ over the system of such $(Y, y)$. Then $R$ is the henselization of the local ring $\mathcal{O}_{X,x_0}$, so $R$ is a henselian local ring with residue field $k$ (see Section B.3). For each $(Y, y)$, we have morphisms $\text{Spec} k \to \text{Spec} R \to Y \to X$, inducing homomorphisms $\text{Br} X \to \text{Br} Y \to \text{Br} R \to \text{Br} k$, the composition of which sends $A$ to $A(x_0) = 0$. By Remark 6.9.2, the homomorphism $\text{Br} R \to \text{Br} k$ is an isomorphism, so $A$ maps to 0 already in $\text{Br} R$. By Theorem 6.4.3, $A$ maps to 0 in $\text{Br} Y$ for some $(Y, y)$. Let $\pi : Y \to X$ be the structure morphism, which is étale. By functoriality as in Proposition 8.1.8, $A(\pi(y)) = 0$ for every $y \in Y(k)$. Since $\pi : Y \to X$ is étale, Proposition 3.5.72 shows that $\pi(Y(k))$ is open in $X(k)$, and it contains $x_0$.

(b) A locally constant map is constant on connected components. \hfill $\square$

**Remark 8.2.10.** The proof of (b) works for every local field $k$. But if $k$ is nonarchimedean, then each connected component of $X(k)$ is a point. And if $k = \mathbb{C}$, then $\text{Br} k = 0$. So only the case $k = \mathbb{R}$ is interesting.

**Corollary 8.2.11.** Let $k$ be a global field. Let $X$ be a $k$-variety.
For any $A \in \text{Br} X$, the map $X(A) \rightarrow \mathbb{Q}/\mathbb{Z}$ sending $(x_v)$ to $(A, (x_v))$ is locally constant.

(b) For any $A \in \text{Br} X$, the set $X(A)^A$ is open and closed in $X(A)$.

(c) The set $X(A)^{\text{Br}}$ is closed in $X(A)$.

(d) Let $X(k)$ be the closure of $X(k)$ in $X(A)$. Then $X(k) \subseteq X(A)^{\text{Br}}$.

(e) If $X$ is proper and $X(A)^{\text{Br}} \neq X(A)$, then weak approximation for $X$ fails. In this case, one says that there is a Brauer–Manin obstruction to weak approximation for $X$.

**Proof.**

(a) Combine Propositions 8.2.1 and 8.2.9.

(b) A fiber of a locally constant map is open and closed.

(c) The set $X(A)^{\text{Br}}$ is the intersection of the closed sets $X(A)^A$ as $A$ varies.

(d) This follows from (c) and Corollary 8.2.6.

(e) If $X(k) \subseteq X(A)^{\text{Br}} \subseteq X(A)$, then $X(k) \neq X(A)$, while $X(A) = \prod_v X(k_v)$ if $X$ is proper. Thus weak approximation for $X$ fails.

**Remark 8.2.12.** Suppose that $X$ is a proper variety over a global field $k$. For a place $v$ of $k$, what does a locally constant function $f$ on $X(k_v)$ look like?

- Suppose that $v$ is archimedean. Then $f$ is constant on each connected component of $X(k_v)$.
- Suppose that $v$ is nonarchimedean. Let $O_v$ be the valuation ring, and let $\pi_v \in O_v$ be a uniformizer. Then $X(k_v) = X(O_v) = \varprojlim n X(O_v/\pi_v^n)$, which is compact, and $f$ factors through the finite set $X(O_v/\pi_v^n)$ for some $n$.

Now suppose that $A \in \text{Br} X$. Then the remarks above apply to the evaluation map $X(k_v) \rightarrow \text{Br} k_v$ given by $A$ for each $v$, and this map is 0 for all but finitely many $v$, by Proposition 8.2.1. Thus the map $X(A) \rightarrow \mathbb{Q}/\mathbb{Z}$ sending $(x_v)$ to $(A, (x_v))$ admits a finite explicit description, in principle. In Section 8.2.5, we will see an example of this.

**8.2.5. Example: Iskovskikh’s conic bundle with 4 singular fibers.**

(References: [Isk71], [Sko01], Chapter 7)

Let $U$ be the smooth, affine, geometrically integral surface

$y^2 + z^2 = (3 - x^2)(x^2 - 2)$

over $\mathbb{Q}$. We will construct a nice $\mathbb{Q}$-surface $X$ containing $U$ as an open subscheme, and then show that there is a Brauer–Manin obstruction to the local-global principle for $X$.

**8.2.5.1. Conic bundles.** The $X$ above will be a conic bundle. Before constructing it, let us discuss conic bundles more generally.

A (possibly degenerate) conic over a field $k$ is the zero locus in $\mathbb{P}^2$ of a nonzero degree 2 homogeneous polynomial $s$ in $k[x_0, x_1, x_2]$. It is a diagonal conic if $s$ is $ax_0^2 + bx_1^2 + cx_2^2$ for some $a, b, c \in k$ not all zero.
The generalization to conic bundles will be easier if we first re-express the situation over \( k \) in a coordinate-free way. If \( E \) is the \( k \)-vector space with basis \( x_0, x_1, x_2 \), then \( \mathbb{P}^2 = \text{Proj} \, k[x_0, x_1, x_2] = \text{Proj} \, \text{Sym} \, E =: \mathbb{P}E \), and a degree 2 homogeneous polynomial \( s \) is an element of \( \text{Sym}^2 E \). We have \( E = L_0 \oplus L_1 \oplus L_2 \) where \( L_i = k x_i \). To say that \( s = 0 \) is a diagonal conic is to say that \( s = s_0 + s_1 + s_2 \) for some \( s_i \in k x_i^2 = L_i^{\otimes 2} \) not all zero.

If \( B \) is a \( k \)-scheme, then a **conic bundle** over \( B \) is the zero locus of \( s \) in \( \mathbb{P}E := \text{Proj} \, \text{Sym} \, E \) where \( E \) is a rank 3 vector bundle on \( B \), and \( s \in \Gamma(B, \text{Sym}^2 E) \) vanishes nowhere on \( B \). In the special case where \( E = \mathcal{L}_0 \oplus \mathcal{L}_1 \oplus \mathcal{L}_2 \) for some line bundles \( \mathcal{L}_i \) on \( B \), and \( s = s_0 + s_1 + s_2 \) for some \( s_i \in \Gamma(B, \mathcal{L}_i^{\otimes 2}) \) such that \( s_0, s_1, s_2 \) do not simultaneously vanish anywhere on \( B \), the zero locus of \( s \) is called a **diagonal conic bundle**.

8.2.5.2. **Châtelet surfaces.** We now specialize further to the following setting:

\[
k : \text{ field of characteristic not } 2
\]

\[
B := \mathbb{P}^1_k
\]

\[
\mathcal{L}_0 := \mathcal{O}
\]

\[
\mathcal{L}_1 := \mathcal{O}
\]

\[
\mathcal{L}_2 := \mathcal{O}(2)
\]

where \( a \in k^\times \), and \( F(w,x) \in \Gamma(\mathbb{P}^1_k, \mathcal{O}(4)) \) is a separable homogeneous polynomial of degree 4 in the homogeneous coordinates \( w, x \) on \( B = \mathbb{P}^1 \). The result is a nice \( k \)-surface \( X \) containing the affine surface

\[
y^2 - ax^2 = f(x)
\]

as an open subscheme, where \( f(x) \) is the dehomogenization \( F(1,x) \). Such a surface \( X \) is called a **Châtelet surface**. It has a map to \( B = \mathbb{P}^1 \) and the fibers of \( X \to \mathbb{P}^1 \) are conics. In fact, all the fibers of \( X \to \mathbb{P}^1 \) above points in \( \mathbb{P}^1(k) \) are *nice* conics, except above 4 points (the zeros of \( F \)) where the fiber degenerates to the union of two intersecting lines in \( \mathbb{P}^2 \).

8.2.5.3. **Iskovskikh’s example.** Iskovskikh’s surface is the Châtelet surface \( X \) over \( \mathbb{Q} \) given by the choices \( a := -1 \) and \( f(x) := (3-x^2)(x^2-2) \in \mathbb{Q}[x] \).

**Remark 8.2.13.** One could choose other nice compactifications \( X' \) of the affine surface

\[
U : y^2 + z^2 = (3-x^2)(x^2-2).
\]

For instance, one could let \( X' \) be the blow-up of \( X \) at a closed point of \( X - U \). But the question of whether such a compactification has a rational point is independent of the choice, by Corollary 8.2.16.

Let \( K = k(X) \). Recall that given \( a, b \in k^\times \), one can define a quaternion algebra with class \( (a, b) \in (\text{Br } K)[2] \) (see Section 1.5.7). Let \( A = (3-x^2,-1) \in \text{Br } K \). By Proposition 6.6.7\[6\], we may view \( \text{Br } X \) as a subgroup of \( \text{Br } K \).

213
Proposition 8.2.14. The element $A \in \text{Br} K$ lies in the subgroup \text{Br} X.

Proof. By Theorem 6.8.3, we need only check that $A$ has no residue along any integral divisor on $X$. Therefore it will suffice to find a Zariski open covering $\{U_i\}$ of $X$ such that $A$ extends to an element of $\text{Br} U_i$ for each $i$.

To accomplish this, we rewrite $A$ in several ways. Define new elements $B = (x^2 - 2, -1)$ and $C = (3/x^2 - 1, -1)$ of $\text{Br} K$. We have $A + B = (y^2 + z^2, -1) = 0$ by Proposition 1.5.23, since $y^2 + z^2 = N_{K(\sqrt{-1})/K}(y + z\sqrt{-1})$. Also, $A - C = (x^2, -1) = 0$ since $x^2$ is a square. But $A, B, C$ are all killed by 2, so $A = B = C$.

Let $P_{3-x^2}$ and $P_{x^2-2}$ be the closed points of $\mathbb{P}^1_\mathbb{Q}$ given by $3-x^2 = 0$ and $x^2-2 = 0$, respectively. Now $A = (3-x^2, -1)$ represents a quaternion Azumaya algebra on all of $X$ except along integral divisors where $3-x^2$ or $-1$ has a zero or pole. Thus $A$ comes from $\text{Br} U_A$, where

$$U_A := X - (\text{fiber above } \infty) - (\text{fiber above } P_{3-x^2}).$$

Similarly, $B \in \text{Br} U_B$, where

$$U_B := X - (\text{fiber above } \infty) - (\text{fiber above } P_{x^2-2}),$$

and $C \in \text{Br} U_C$, where

$$U_C := X - (\text{fiber above } 0) - (\text{fiber above } P_{3-x^2}).$$

Since $U_A \cup U_B \cup U_C = X$ (in fact, $U_B \cup U_C = X$), the element $A = B = C \in \text{Br} K$ belongs to $\text{Br} X$. \qed

From now on, we consider $A$ as an element of $\text{Br} X$. To evaluate $A$ at a point $P \in X(k)$ for any field $k \supset \mathbb{Q}$, choose one of

$$(3-x^2, -1), \quad (x^2-2, -1), \quad (3/x^2 - 1, -1)$$

such that the rational function of $x$ is defined and nonzero at $P$, so that $A$ extends to an element of the Brauer group of an open subset $U_A, U_B, \text{ or } U_C$ containing $P$, and replace the rational function by its value at $P$. For example, if $P \in U_A(\mathbb{Q}_p)$ for some $p \leq \infty$, then

$$\text{inv}_p A(P) = \text{inv}_p (3 - x(P)^2, -1)$$

$$= \begin{cases} 
0, & \text{if } 3 - x(P)^2 \in N_{Q_p(\sqrt{-1})/Q_p}(Q_p(\sqrt{-1})^\times), \\
1/2, & \text{otherwise}, 
\end{cases}$$

by Proposition 1.5.23.

Proposition 8.2.15. We have $X(\mathbb{A}) \neq \emptyset$, but $X(\mathbb{A})^A = \emptyset$. In particular, $X(\mathbb{Q}) = \emptyset$, and there is a Brauer–Manin obstruction to the local-global principle for $X$.

Proof. A computation involving Hensel’s lemma (Theorem 3.5.62(a)) shows that $X(\mathbb{A}) \neq \emptyset$. 214
Suppose that \( P \in X(\mathbb{Q}_p) \) for some \( p \leq \infty \). If \( p \neq \infty \), let \( v_p: \mathbb{Q}_p \to \mathbb{Z} \cup \{\infty\} \) denote the \( p \)-adic valuation. Let \( x = x(P) \in \mathbb{Q}_p \cup \{\infty\} \).

**Case I:** \( p \notin \{2, \infty\} \)

If \( v_p(x) < 0 \) (or \( x = \infty \)), then \( 3/x^2 - 1 \in \mathbb{Z}_p^\times \). If \( v_p(x) \geq 0 \), then either \( 3 - x^2 \) or \( x^2 - 2 \) is in \( \mathbb{Z}_p^\times \) because their sum is 1. In either case, \( A(P) \) has the form \((u_1, u_2)\) with \( u_1, u_2 \in \mathbb{Z}_p^\times \), so \( A(P) \in \text{Br} \mathbb{Z}_p \) (this uses \( p \neq 2 \)). But \( \text{Br} \mathbb{Z}_p = 0 \) by Corollary 6.9.3, so \( \text{inv}_p A(P) = 0 \).

**Case II:** \( p = \infty \)

The leading coefficient of \((3 - x^2)(x^2 - 2)\) is not a sum of squares in \( \mathbb{R} \), so any \( P \in X(\mathbb{R}) \) satisfies \( x(P) \neq \infty \). Then \( x(P)^2 < 3 \) or \( x(P)^2 > 2 \), so \( 3 - x(P)^2 \) or \( x(P)^2 - 2 \) is in \( \mathbb{R}_{>0} = N_{\mathbb{C}/\mathbb{R}}(\mathbb{C}^\times) \). Thus \( \text{inv}_\infty A(P) = 0 \).

**Case III:** \( p = 2 \)

Let \( P \in X(\mathbb{Q}_2) \). Let \( x = x(P) \). Then

\[
\begin{align*}
v_2(x) > 0 & \implies 3 - x^2 \equiv 3 \equiv -1 \pmod{4} \\
v_2(x) = 0 & \implies x^2 - 2 \equiv -1 \pmod{4} \\
v_2(x) < 0 & \implies 3/x^2 - 1 \equiv -1 \pmod{4}.
\end{align*}
\]

But an element of \( \mathbb{Z}_2 \) that is \(-1 \pmod{4}\) is not of the form \( a^2 + b^2 \) with \( a, b \in \mathbb{Q}_2 \), so it is not a norm from \( \mathbb{Q}_2(\sqrt{-1})/\mathbb{Q}_2 \). Thus \( \text{inv}_2 A(P) = 1/2 \).

Cases I, II, III together imply that if \( \{P_p\} \in X(A) \), then \( (A, \{P_p\}) = 1/2 \neq 0 \). Thus \( X(A)^A = \emptyset \). \( \square \)

**Remark 8.2.16.** Iskovskikh’s original proof that \( X(\mathbb{Q}) = \emptyset \) used only ad hoc methods based on quadratic reciprocity. Ironically, according to [CTPS16 Section 1], Iskovskikh’s intention was to produce an example that the Brauer–Manin obstruction could not explain! It was only a few years later that it was realized that the Brauer–Manin obstruction could explain it, as above.

**Remark 8.2.17.** Theorem B of [CTSSD87a, CTSSD87b] shows that for any Châtelet surface over a number field, the Brauer–Manin obstruction to the local-global principle is the only one, and even better, the Brauer–Manin obstruction to weak approximation is the only one; that is, \( X(k) \) is dense in \( X(A)^{Br} \). These results were generalized in [Sal90, CT90, SS91] to conic bundle surfaces over \( \mathbb{P}^1 \) with at most 5 degenerate fibers. Moreover, Schinzel’s hypothesis on prime values of polynomials would imply the same when the number of degenerate fibers is arbitrary, and more generally for “generalized Severi–Brauer bundles over \( \mathbb{P}^1 \)” [CTSD94, Theorem 4.2]. A key ingredient in these works is the fibration method: for an introduction, see [CT92 Section 3] and [CT98 Section 2]; for examples of the further development of this method, see [Har94, Har97, Lia14, HW16].
8.2.6. Effectivity. Let $X$ be a nice variety over a global field $k$. One can imagine the following procedure for attempting to decide whether $X$ has a $k$-point:

- by day, search for $k$-points;
- by night, search for a finite set of Azumaya $\mathcal{O}_X$-algebras that obstructs $k$-points.

If the Brauer–Manin obstruction to the local-global principle is the only one for $X$, then this procedure terminates successfully. See [Poo06, Remark 5.3] for more details.

Under additional assumptions on $X$, one can give more reasonable algorithms and even compute a kind of finite description of $X(\mathbb{A})^{\mathrm{Br}}$: see [KT08, KT11].

8.3. An example of descent

Suppose (as in [Fly00, Section 6]) that we want to find the rational solutions to

$$y^2 = (x^2 + 1)(x^4 + 1).$$

Write $x = X/Z$ where $X, Z$ are integers with gcd 1. Then $y = Y/Z^3$ for some integer $Y$ with gcd$(Y, Z) = 1$. We get

$$y^2 = (X^2 + Z^2)(X^4 + Z^4).$$

If a prime $p$ divides both $X^2 + Z^2$ and $X^4 + Z^4$, then

$$Z^2 \equiv -X^2 \pmod{p}$$
$$Z^4 \equiv -X^4 \pmod{p}$$

so

$$2Z^4 = (Z^2)^2 + Z^4 \equiv (-X^2)^2 + (-X^4) = 0 \pmod{p}$$

and similarly

$$2X^4 = (X^2)^2 + X^4 \equiv (-Z^2)^2 + (-Z^4) = 0 \pmod{p}.$$ 

But gcd$(X, Z) = 1$, so this forces $p = 2$. (Alternatively, the resultant of the homogeneous forms $X^2 + Z^2$ and $X^4 + Z^4$ is 4, so the only prime $p$ modulo which these forms have a common nontrivial zero is $p = 2$.)

Each odd prime $p$ divides at most one of $X^2 + Z^2$ and $X^4 + Z^4$, but the product $(X^2 + Z^2)(X^4 + Z^4)$ is a square, so the exponent of $p$ in each must be even. In other words,

$$X^4 + Z^4 = cW^2$$

for some $c \in \{\pm 1, \pm 2\}$. Since $X, Z$ are not both zero, the left hand side is positive, so $c > 0$. Thus $c \in \{1, 2\}$.
Dividing by \( Z^4 \) and setting \( w = W/Z^2 \), we obtain a rational solution to one of the following smooth curves

\[
\begin{align*}
Y_1: & \quad w^2 = x^4 + 1 \\
Y_2: & \quad 2w^2 = x^4 + 1.
\end{align*}
\]

Each curve \( Y_c \) is of geometric genus \( g \) where \( 2g + 2 = 4 \); i.e., \( g = 1 \). The point \((x, w) = (0, 1)\) belongs to \( Y_1(\mathbb{Q}) \), and \((1, 1)\) belongs to \( Y_2(\mathbb{Q}) \), so both \( Y_1 \) and \( Y_2 \) are open subsets of elliptic curves.

One can show that \( Y_1 \) and \( Y_2 \) are birational to the curves

\[
\begin{align*}
32A2: & \quad y^2 = x^3 - x \\
64A1: & \quad y^2 = x^3 - 4x,
\end{align*}
\]

where the labels are as in [Cre97]. A “2-descent” (or a glance at Table 1 of [Cre97]) shows that both elliptic curves have rank 0. One also can compute that their torsion subgroups are isomorphic to \( \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \). Thus the nice models of \( Y_1 \) and \( Y_2 \) have \( 4 \) rational points each. So the answer to the original problem is that there are six solutions, namely:

\[(0, 1), (0, -1), (1, 2), (1, -2), (-1, 2), (-1, -2).\]

8.3.1. Explanation. We are asked to find \( U(\mathbb{Q}) \), where \( U \) is the smooth affine curve

\[y^2 = (x^2 + 1)(x^4 + 1)\]

in \( \mathbb{A}^2_\mathbb{Q} \). Let \( X \) be the nice genus 2 curve over \( \mathbb{Q} \) containing \( U \) as an open subscheme; explicitly, \( X = \text{Proj} k[x, y, z]/(y^2 - (x^2 + z^2)(x^4 + z^4)) \), where \( \deg x = \deg z = 1 \) and \( \deg y = 3 \). From this description, we also see that \( X - U \) consists of 2 rational points. In particular, finding \( U(\mathbb{Q}) \) is equivalent to finding \( X(\mathbb{Q}) \), and the latter is finite by Faltings’s theorem (Theorem 2.6.8).

Let \( Z \) be the nice curve over \( \mathbb{Q} \) birational to the curve in \((x, y, w)\)-space defined by the system

\[
\begin{align*}
y^2 &= (x^2 + 1)(x^4 + 1) \\
w^2 &= x^4 + 1,
\end{align*}
\]

so \( k(Z) = \mathbb{Q}(x, \sqrt{x^2 + 1}, \sqrt{x^4 + 1}) \). For \( c \in \mathbb{Q}^* \), let \( Z_c \) be the twist of \( Z \) that is birational to the curve

\[
\begin{align*}
y^2 &= (x^2 + 1)(x^4 + 1) \\
cw^2 &= x^4 + 1.
\end{align*}
\]
For each $c$, there is a degree 2 morphism

$$Z_c \longrightarrow X$$

$$(x, y, w) \mapsto (x, y).$$

The argument of the previous section can be reinterpreted as follows:

- Each point in $X(\mathbb{Q})$ is the image of $f_c : Z_c(\mathbb{Q}) \to X(\mathbb{Q})$ for some $c \in \mathbb{Q}^\times$.
- Up to multiplying $c$ by $\mathbb{Q}^\times$, there are only finitely many $c \in \mathbb{Q}^\times$ for which $Z_c$ has $\mathbb{Q}_p$-points for all $p \leq \infty$. Moreover, such a finite set of $c$'s can be computed effectively.

The finite set of $c$'s turned out to be $\{1, 2\}$. Thus the problem of determining $X(\mathbb{Q})$ was reduced to the problem of determining $Z_c(\mathbb{Q})$ for $c \in \{1, 2\}$.

If $Y_c$ is the nice genus 1 curve birational to

$$cy^2 = x^4 + 1,$$

then we have a morphism

$$\pi_c : Z_c \longrightarrow Y_c$$

$$(x, y, w) \mapsto (x, w).$$

Fortunately, for $c \in \{1, 2\}$, the curve $Y_c$ is an elliptic curve of rank 0, so $Y_c(\mathbb{Q}) = Y_c(\mathbb{Q})_{\text{tors}}$ is a computable finite set. We determine the $\mathbb{Q}$-points in the 0-dimensional preimage $\pi_c^{-1}(Y_c(\mathbb{Q})) \subset Z_c$; this gives $Z_c(\mathbb{Q})$. Finally we compute $X(\mathbb{Q}) = \bigcup_{c \in \{1, 2\}} f_c(Z_c(\mathbb{Q}))$.

**Remark 8.3.1.** The elliptic curve

$$E : \quad y^2 = (t + 1)(t^2 + 1)$$

is dominated by $X$, by the morphism

$$\phi : X \longrightarrow E$$

$$(x, y) \mapsto (x^2, y).$$

Unfortunately, the approach of computing $E(\mathbb{Q})$ and then computing $\phi^{-1}(P)$ for each $P \in E(\mathbb{Q})$ cannot be carried out directly, since $E(\mathbb{Q})$ is infinite, of rank 1. Moreover, one can show that the Jacobian $J$ of $X$ is isogenous to $E \times E$, so $\text{rk } J(\mathbb{Q}) = 2$ is not less than $g(X) = 2$, so Chabauty’s method (see [Ser97] §5.1 or [MP12]) cannot be applied directly to $X$. On the other hand, $X$ has two independent maps to $E$, so the DEMYANENKO–MANIN method [Ser97, §5.2] could be applied to determine $X(\mathbb{Q})$.

**8.3.2. Galois covering.** One of the key points is the argument was that there are only finitely many $c$ such that $Z_c$ has $\mathbb{Q}_p$-points for all $p \leq \infty$. What makes this work is the fact that $Z \to X$ is a Galois covering.
Let us first explain why \( f : Z \to X \) is étale. Over the affine open subset \( V_1 \) of \( U \subseteq X \) where \( x^4 + 1 \) is nonvanishing, the open subset \( f^{-1}V_1 \subseteq Z \) is obtained by adjoining \( \sqrt{x^4 + 1} \) to the affine coordinate ring; this is an étale extension. Similarly, over the affine open subset \( V_2 \) of \( U \) where \( x^2 + 1 \) is nonvanishing, \( f^{-1}V_2 \) is obtained by adjoining \( \sqrt{x^2 + 1} \). Since \( V_1 \) and \( V_2 \) cover \( U \), it follows that \( f \) is étale above \( U \). A similar argument shows that \( f \) is étale above the other affine open piece \( U' \) of \( X \). Thus \( f : Z \to X \) is étale.

Remark 8.3.2. The argument that \( f \) is étale is a special case of the proof of Abhyankar’s lemma [SGA 1, X.3.6]. It is analogous to the proof that the field \( \mathbb{Q}(\sqrt{15}, \sqrt{3}) = \mathbb{Q}(\sqrt{15}, \sqrt{5}) \) is an everywhere unramified extension of \( \mathbb{Q}(\sqrt{15}) \).

In fact, the following shows that \( Z \to X \) is a Galois covering with Galois group \( \mathbb{Z}/2\mathbb{Z} \):

Proposition 8.3.3. Let \( Z \to X \) be an étale morphism between nice \( k \)-curves. If \( k(Z)/k(X) \) is a Galois extension of field with Galois group \( G \), then \( Z \to X \) is a Galois covering with Galois group \( G \).

Proof. By the equivalence of categories between curves and function fields, the left \( G \)-action on \( k(Z) \) induces a right \( G \)-action on \( Z \) considered as an \( X \)-scheme. Since \( k(Z)/k(X) \) is Galois, the \( X \)-morphism

\[
\psi : Z \times G \longrightarrow Z \times_X Z
\]

is an isomorphism above the generic point of \( X \). By spreading out (Theorem [3.2.1][v]), \( \psi \) gives an isomorphism from an open dense subscheme of \( Z \times G \) to an open dense subscheme of \( Z \times_X Z \). Both \( Z \times G \) and \( Z \times_X Z \) are smooth, proper, and 1-dimensional over \( k \), so any birational maps between their components are isomorphisms. \( \square \)

8.4. Descent

(Reference: [Sko01, §5.3])

In our example, \( Z \) was a \( \mathbb{Z}/2\mathbb{Z} \)-torsor over \( X \). We now generalize by replacing \( \mathbb{Z}/2\mathbb{Z} \) by an arbitrary smooth affine algebraic group \( G \) over \( k \). When we speak of a \( G \)-torsor over \( X \), we mean a right fppf \( G_X \)-torsor over \( X \), where \( G_X \) is the base extension. Throughout the rest of Chapter 8, all cohomology is fppf cohomology, and we use \( H^1(X, G) \) as an abbreviation for the pointed set \( \hat{H}^1_{\text{fppf}}(X, G) \) (which is a group if \( G \) is commutative). By Theorem [6.5.10][i], isomorphism classes of \( G \)-torsors over \( X \) are in bijection with \( H^1(X, G) \).

8.4.1. Evaluation. Let \( k \) be a field. Let \( X \) be a \( k \)-variety. Let \( G \) be a smooth algebraic group over \( k \). Let \( Z \to X \) be an \( G \)-torsor over \( X \), and let \( \zeta \) be its class in \( H^1(X, G) \). If \( x \in X(k) \), then the fiber \( Z_x \to \{ x \} \) is a \( G \)-torsor over \( k \), and its class in \( H^1(k, G) \) will be
denoted $\zeta(x)$. Equivalently, $x$ determines a morphism in cohomology mapping $\zeta$ to $\zeta(x)$:

$$x : \text{Spec } k \longrightarrow X$$

$$\text{H}^1(k, G) \leftarrow \text{H}^1(X, G)$$

$$\zeta(x) \leftarrow \zeta.$$  

Thus the torsor $Z \to X$ gives rise to an “evaluation” map

$$X(k) \longrightarrow \text{H}^1(k, G)$$

$$x \mapsto \zeta(x).$$

In other words, $Z \to X$ can be thought of as a family of torsors parameterized by $X$, and $\zeta(x)$ gives the class of the fiber above $x$.

8.4.2. The fibers of the evaluation map. We may partition $X(k)$ according to the class of the fiber above each rational point:

$$X(k) = \bigsqcup_{\tau \in \text{H}^1(k, G)} \{ x \in X(k) : \zeta(x) = \tau \}.$$  

The following key theorem reinterprets the right hand side.

**Theorem 8.4.1.** Let $k$ be a field. Let $X$ be a $k$-variety. Let $G$ be a smooth affine algebraic group. Suppose that $f : Z \to X$ is a $G$-torsor over $X$, and let $\zeta \in \text{H}^1(X, G)$ be its class. For each $\tau \in \text{H}^1(k, G)$, let $f^\tau : Z^\tau \to X$ be the twisted torsor constructed in Example 6.5.12. Then

$$\{ x \in X(k) : \zeta(x) = \tau \} = f^\tau(Z^\tau(k)).$$  

In particular,

$$X(k) = \bigsqcup_{\tau \in \text{H}^1(k, G)} f^\tau(Z^\tau(k)).$$

**Proof.** For $x \in X(k)$, we have

$$x \in f^\tau(Z^\tau(k)) \iff \text{the fiber } Z_x^\tau \text{ is a trivial } G^\tau\text{-torsor over } k \quad \text{(Proposition 5.12.14)}$$

$$\iff Z_x^G \times T^{-1} \text{ is a trivial } G^\tau\text{-torsor over } k$$

$$\iff Z_x \simeq T \text{ as } G\text{-torsor}$$

(by taking the contracted product with $T$ on the right)

$$\iff \zeta(x) = \tau. \quad \Box$$

8.4.3. The evaluation map over a local field.

**Proposition 8.4.2.** Let $k$ be a local field. Let $X$ be a proper $k$-variety. Let $F$ be a finite étale algebraic group over $k$. Let $f : Z \to X$ be an $F$-torsor over $X$. Then the image of $X(k) \to \text{H}^1(k, F)$ is finite.
Proof. For each \( x \in X(k) \), the fiber \( f^{-1}(x) \) is Spec \( L \) for some étale \( k \)-algebra \( L \). By Krasner’s lemma (Proposition 3.5.73), there exists an open neighborhood \( U \) of \( x \) in \( X(k) \) such that for \( u \in U \), the fiber \( f^{-1}(u) \) is isomorphic to \( f^{-1}(x) \) as a \( k \)-scheme. In other words, if \( H^1(k,F) \) is given the discrete topology, then the evaluation map \( X(k) \to H^1(k,F) \) is continuous.

On the other hand, \( X \) is proper, so \( X(k) \) is compact by Proposition 2.6.1(i). Thus the image of \( X(k) \to H^1(k,F) \) is compact, and hence finite. \( \square \)

Remark 8.4.3. If \( \text{char } k = 0 \), then the whole set \( H^1(k,F) \) is finite by Theorem 5.12.24(a).

8.4.4. The Selmer set. Return to the notation of Theorem 8.4.1, but assume moreover that \( k \) is a global field. For each place \( v \) of \( k \), the inclusion \( k \hookrightarrow k_v \) induces a homomorphism of fppf cohomology \( H^1(k,G) \to H^1(k_v,G) \). (Equivalently, it is the restriction homomorphism of Galois cohomology associated with the inclusion of \( \text{Gal}(k^s_v/k_v) \) as a decomposition group in \( \text{Gal}(k^s/k) \).) If \( \tau \in H^1(k,G) \), let \( \tau_v \in H^1(k_v,G) \) be its image.

Definition 8.4.4. The Selmer set is the following subset of \( H^1(k,G) \):

\[
\text{Sel}_Z(k,G) := \left\{ \tau \in H^1(k,G) : \tau_v \in \text{im} \left( X(k_v) \to H^1(k_v,G) \right) \text{ for all } v \in \Omega_k \right\}.
\]

Remark 8.4.5. This terminology and notation is compatible with the notion of the Selmer group, in the case where \( f : Z \to X \) is an isogeny between abelian varieties, viewed as a torsor under \( G := \ker f \). For instance, if \( f : E \to E \) is the multiplication-by-2 map on an elliptic curve over a number field, then \( \text{Sel}_E(k,E[2]) \subseteq H^1(k,E[2]) \) is the 2-Selmer group defined in [Sil92, X.§4].

By Theorem 8.4.1 applied over each \( k_v \), we have

\[
\text{Sel}_Z(k,G) = \left\{ \tau \in H^1(k,G) : Z^\tau(k_v) \neq \emptyset \text{ for all } v \in \Omega_k \right\} \\
\supseteq \left\{ \tau \in H^1(k,G) : Z^\tau(k) \neq \emptyset \right\}.
\]

In particular,

\[
X(k) = \coprod_{\tau \in \text{Sel}_Z(k,G)} f^\tau(Z^\tau(k)).
\]

Theorem 8.4.6. If \( X \) is proper over a global field \( k \), then \( \text{Sel}_Z(k,G) \) is finite.

Proof. Let \( F \) be the component group of \( G \). For a suitable finite nonempty subset \( S \subseteq \Omega_k \) containing the archimedean places, Theorem 3.2.1 lets us spread out \( G \) to a smooth finite-type separated group scheme \( G \) over \( O_{k,S} \), spread out \( X \) to a proper scheme \( X \) over \( O_{k,S} \), and spread out \( Z \) to a \( G \)-torsor over \( X \). Let \( \tau \in H^1(k,G) \). For \( v \notin S \), the commutative
shows that if $\tau_v$ comes from $X(k_v)$, then $\tau_v$ also comes from $H^1(O_v, G)$. Thus $\text{Sel}_Z(k, G)$ is contained in $H^1_S(k, G)$. Moreover, for each $v \in S$, the image of $X(k_v) \to H^1(k_v, F)$ is finite by Proposition 8.4.2, so the image of $\text{Sel}_Z(k, G)$ in $\prod_{v \in S} H^1(k_v, F)$ is finite. The preceding two sentences combined with Theorem 6.5.13(a) show that $\text{Sel}_Z(k, G)$ is finite. \hfill \Box

**Remark 8.4.7.** One can show that $\text{Sel}_Z(k, G)$ is not only finite, but also effectively computable, even if one does not know $X(k)$. This makes it potentially useful for the determination of $X(k)$.

**Corollary 8.4.8.** There exists a finite separable extension $k'$ of $k$ such that $X(k) \subseteq f(Z(k'))$.

**Proof.** For each $\tau \in H^1(k, G)$, there exists a finite separable extension $k'$ such that the image of $\tau$ in $H^1(k', G)$ is trivial. By taking a compositum, one can find a $k'$ that works simultaneously for all $\tau \in \text{Sel}_Z(k, G)$. Extending the base from $k$ to $k'$ makes $Z^\tau \xrightarrow{f^\tau} X$ isomorphic to $Z \xrightarrow{f} X$. \hfill \Box

### 8.4.5. The weak Mordell–Weil theorem.

The Mordell–Weil theorem states that for any abelian variety $A$ over a global field $k$, the abelian group $A(k)$ is finitely generated. The following statement is weaker, and is proved along the way to proving the Mordell–Weil theorem:

**Theorem 8.4.9 (Weak Mordell–Weil theorem).** Let $A$ be an abelian variety over a global field $k$, and let $m$ be a positive integer not divisible by $\text{char } k$. Then $A(k)/mA(k)$ is finite.

**Proof of Theorem 8.4.9.** By Proposition 5.7.4, the multiplication-by-$m$ map $A \xrightarrow{m} A$ is étale, so it is locally surjective in the étale topology. Thus we get an exact sequence of sheaves on $(\text{Spec } k)_{\text{et}}$

$$0 \to A[m] \to A \xrightarrow{m} A \to 0$$

(or equivalently of $\mathfrak{S}_k$-modules), where $A[m]$ is the kernel of $A \xrightarrow{m} A$. Taking cohomology gives

$$A(k) \xrightarrow{m} A(k) \to H^1(k, A[m]).$$
On the other hand, we may view $[m] : A \to A$ as a torsor under the smooth affine algebraic group $A[m]$, and hence we get an evaluation map

$$A(k) \to H^1(k, A[m])$$

sending $a \in A(k)$ to the class of the torsor $[m]^{-1}(a)$. The image of the evaluation map is contained in the Selmer set, which is finite by Theorem 8.4.6.

One checks that the two maps

$$A(k) \to H^1(k, A[m])$$

coincide, so the image of the evaluation map is isomorphic to $A(k)/mA(k)$. Thus $A(k)/mA(k)$ is finite.

\[ \square \]

8.4.6. Application of descent to failure of strong approximation. We will use an integral point analogue of descent to prove a theorem of Minchev [Min89, Theorem 1] on the failure of strong approximation. Minchev worked over number fields, but with a little more work we can generalize to global fields.

**Theorem 8.4.10.** Let $k$ be a global field. Let $S$ be a finite set of places of $k$. Let $f : Y \to X$ be a finite étale morphism of geometrically integral $k$-varieties. If $X(A^S) \neq \emptyset$ and $f$ is not an isomorphism, then the image of $X(k) \to X(A^S)$ is not dense; that is, $X$ does not satisfy strong approximation with respect to $S$.

**Proof.** Let $n = \dim X = \dim Y$. Let $d = \deg f > 1$. Use Theorem 3.2.1 to enlarge $S$ so that $f$ spreads out to a finite étale morphism $F : Y \to X$ of separated $O_{k,S}$-schemes such that $X \to \text{Spec } O_{k,S}$ and $Y \to \text{Spec } O_{k,S}$ have geometrically integral fibers and $X(O_v) \neq \emptyset$ for $v \notin S$. For any nonarchimedean $v \in S$, as $x_v$ varies over the compact set $X(O_v)$, there are only finitely many possibilities for the finite étale $O_v$-scheme $F^{-1}(x_v)$, by Krasner’s lemma (Proposition 3.5.73). Therefore, as $x$ varies over $X(O_{k,S})$, the finite étale $O_{k,S}$-scheme $F^{-1}(x)$ has bounded degree and bounded ramification over $S$, so there are only finitely many possibilities for $F^{-1}(x)$. In particular, there exists an infinite set $T$ of nonarchimedean $v \notin S$ such that $v$ splits in $F^{-1}(x)$ for every $x \in X(O_{k,S})$.

Let $X'$ be the smooth locus of $X \to \text{Spec } O_{k,S}$, and let $Y' = F^{-1}X'$. For $v \notin S$, let $\mathbb{F}_v$ be the residue field, and let $q_v = \#\mathbb{F}_v$. By Theorem 7.7.1(iii), $\#X'(\mathbb{F}_v)$ and $\#Y'(\mathbb{F}_v)$ are both $q_v^n + O(q_v^{n-1/2})$ as $q_v \to \infty$. In particular, we may choose $w \in T$ such that $\#Y'(\mathbb{F}_w) < d \cdot \#X'(\mathbb{F}_w)$. Thus there exists $\bar{a}_w \in X'(\mathbb{F}_w)$ that does not split in $Y'$. By Hensel’s lemma (Theorem 3.5.62(ii)), $\bar{a}_w$ lifts to some $a_w \in X'(O_w)$. By Krasner’s lemma (Proposition 3.5.73), the set $U_w := \{u_w \in X'(O_w) : F^{-1}(u_w) \simeq F^{-1}(a_w)\}$ is an open neighborhood of $a_w$ in $X(k_w)$. Let $U$ be the nonempty open set $U_w \times \prod_{v \notin S \cup \{w\}} X(O_{k,S})$ of $X(A^S)$. If $x \in X(k) \cap U$, then $x \in X'(O_{k,S})$, so the definition of $T$ implies that $w$ splits in
Let \( k \) be a global field. Let \( S \) be a finite set of places of \( k \). Let \( X \) be a normal geometrically integral \( k \)-variety. If \( X(\mathbb{A}^S) \neq \emptyset \) and \( X_k \) is not algebraically simply connected, then \( X \) does not satisfy strong approximation with respect to \( S \).

**Corollary 8.4.11** (cf. [Min89, Theorem 1]). Let \( k \) be a global field. Let \( S \) be a finite set of places of \( k \). Let \( X \) be a normal geometrically integral \( k \)-variety. If \( X(\mathbb{A}^S) \neq \emptyset \) and \( X_k \) is not algebraically simply connected, then \( X \) does not satisfy strong approximation with respect to \( S \).

**Proof.** If \( X(k) \) is empty, strong approximation fails by definition. If \( X(k) \) is nonempty, apply Lemma 3.5.56 to obtain a nontrivial geometrically integral finite étale cover \( Y \to X \), and apply Theorem 8.4.10. □

**Remark 8.4.12.** Corollary 8.4.11 can fail if \( X \) is not normal. For example, if \( X \) is a nodal cubic curve in \( \mathbb{P}^2 \) over a global field such that the tangent lines to the branches at the node have irrational slope, then \( X \) is not algebraically simply connected, but \( X \) satisfies strong approximation with respect to any finite \( S \), because there is a dominant morphism \( \mathbb{P}^1 \to X \).

### 8.4.7. The descent obstruction to the local-global principle.

Let \( k \) be a global field. Let \( X \) be a \( k \)-variety. One can show that there is a injection \( X(\mathbb{A}) \hookrightarrow \prod_v X(k_v) \), so an element of \( X(\mathbb{A}) \) will be written as a sequence \((x_v)\) indexed by the places \( v \) of \( k \). The set \( X(k) \) embeds diagonally into \( X(\mathbb{A}) \).

A torsor \( Z \to X \) under a smooth affine algebraic group \( G \) over \( k \) restricts the locations in \( X(\mathbb{A}) \) where rational points can lie. Namely, the commutativity of

\[
\begin{array}{ccc}
X(k) & \rightarrow & X(\mathbb{A}) \\
\downarrow & & \downarrow \\
\text{H}^1(k; G) & \rightarrow & \prod_v \text{H}^1(k_v; G)
\end{array}
\]

(cf. (8.1.1)) shows that \( X(k) \) is contained in the subset

\[
X(\mathbb{A})^f := \left\{ (x_v) \in X(\mathbb{A}) \; \text{whose image in} \; \prod_v \text{H}^1(k_v; G) \; \text{comes from} \; \text{H}^1(k; G) \right\}.
\]

of \( X(\mathbb{A}) \). One can show also that

\[
X(\mathbb{A})^f = \bigcup_{\tau \in \text{H}^1(k; G)} f^\tau(Z^f(\mathbb{A})),
\]

and that \( X(\mathbb{A})^f \) is closed in \( X(\mathbb{A}) \) if \( X \) is proper: see Exercise 8.7. Moreover, one can replace \( \text{H}^1(k; G) \) by its subset \( \text{Sel}_Z(k; G) \) in either of the two descriptions of \( X(\mathbb{A})^f \) above. The condition \( X(\mathbb{A})^f = \emptyset \) is equivalent to \( \text{Sel}_Z(k; G) = \emptyset \).
One can constrain the possible locations of rational points further by using many torsors:

\[
X(A)_{H^1(X,G)} := \bigcap_{\text{all } G}\text{-torsors } f: Z \to X \quad X(A)_{\text{descent}} := \bigcap_{\text{all smooth affine } G} X(A)^{H^1(X,G)}.
\]

Then

\[
X(k) \subseteq X(A)_{\text{descent}} \subseteq X(A).
\]

Recall that one says that the local-global principle holds for \( X \) if and only if the implication

\[
X(A) \neq \emptyset \implies X(k) \neq \emptyset
\]

holds.

**Definition 8.4.14.** One says that there is a descent obstruction to the local-global principle if \( X(A) \neq \emptyset \) but \( X(A)_{\text{descent}} = \emptyset \).

Sometimes we wish to study the adelic subset cut out by torsors under a subset of the possible smooth affine algebraic groups. In particular, we define

\[
X(A)^{\text{et}} := \bigcap_{\text{finite étale } G} X(A)^{H^1(X,G)}
\]

\[
X(A)^{\text{conn}} := \bigcap_{\text{smooth connected affine } G} X(A)^{H^1(X,G)}
\]

\[
X(A)^{\text{PGL}} := \bigcap_{n \geq 1} X(A)^{H^1(X,PGL_n)}.
\]

### 8.5. Comparing the descent and Brauer–Manin obstructions

**8.5.1. Descent is stronger than Brauer–Manin.**

(Reference: [Sko01, Proposition 5.3.4])

Proposition 8.5.3 below shows that the Brauer–Manin obstruction is equivalent to the special case of the descent obstruction using only \( PGL_n \)-torsors for all \( n \).

Recall from Section 6.6.4 that for any scheme \( X \), we have a map of sets

\[
(8.5.1) \quad H^1(X,PGL_n) \rightarrow (\text{Br } X)[n].
\]

(We used Theorem 6.6.17[1] to know that the image is killed by \( n \).)

**Lemma 8.5.2.** Let \( k \) be a global field. Let \( X \) be a \( k \)-variety. Let \( Z \xrightarrow{f} X \) be a \( PGL_n \)-torsor for some \( n \geq 1 \). Its class in \( H^1(X,PGL_n) \) is mapped by \((8.5.1)\) to some \( A \in \text{Br } X \). Then \( X(A)^f = X(A)^A \).
Proof. Let \((x_v) \in X(A)\). Then we have a commutative diagram

\[
\begin{array}{c}
\text{H}^1(X, \text{PGL}_n) \xrightarrow{(x_v)} (\text{Br} X)[n] \\
\downarrow \quad \downarrow \quad \downarrow \quad \downarrow \\
\prod_v \text{H}^1(k_v, \text{PGL}_n) \xrightarrow{\text{res}_1} \prod_v (\text{Br} k_v)[n] \\
\end{array}
\]

in which the downward maps are evaluation at \((x_v)\), the upward maps \(\text{res}_1, \text{res}_2\) are restriction maps induced by \(k \to k_v\), and the horizontal maps are given by (8.5.1). The lower two horizontal maps are bijections by Remark 1.5.18.

The middle horizontal bijection identifies \(\text{im}(\text{res}_1)\) with \(\text{im}(\text{res}_2)\), so the class of \(f\) in \(\text{H}^1(X, \text{PGL}_n)\) maps down into \(\text{im}(\text{res}_1)\) if and only if \(A \in (\text{Br} X)[n]\) maps down into \(\text{im}(\text{res}_2)\). In other words, \((x_v) \in X(A)^f\) if and only if \((x_v) \in X(A)^A\). \(\square\)

Proposition 8.5.3. Let \(k\) be a global field. Let \(X\) be a regular quasi-projective \(k\)-variety. Then

\[X(A)^{\text{descent}} \subseteq X(A)^{\text{PGL}} = X(A)^{\text{Br}}.\]

Proof. By Corollary 6.6.19 every \(A \in \text{Br} X\) is in the image of (8.5.1) for some \(n\). So intersecting the equality of Lemma 8.5.2 over all \(\text{PGL}_n\)-torsors over \(X\) yields \(X(A)^{\text{PGL}} = X(A)^{\text{Br}}\). The inclusion \(X(A)^{\text{descent}} \subseteq X(A)^{\text{PGL}}\) holds by definition since each \(\text{PGL}_n\) is a smooth affine algebraic group. \(\square\)

8.5.2. The étale-Brauer set.

(References: [Poo10][Dem09][Sko09])

Let \(k\) be a global field. Let \(X\) be a \(k\)-variety. Let \(G\) be a smooth affine algebraic group. Recall that if \(Z \xrightarrow{f} X\) is a \(G\)-torsor, the determination of \(X(k)\) can be reduced to the determination of \(Z^\tau(k)\) for various twists \(Z^\tau\) of \(Z\):

\[X(k) = \coprod_{\tau \in \text{H}^1(k,G)} f^\tau(Z^\tau(k)) \subseteq \bigcup_{\tau \in \text{H}^1(k,G)} f^\tau(Z^\tau(A)).\]

We can produce a possibly better “upper bound” on \(X(k)\) by replacing \(Z^\tau(A)\) by \(Z^\tau(A)^{\text{Br}}\). If we do so for every \(G\)-torsor for every finite étale group scheme \(G\), we are led to define the étale-Brauer set

\[X(A)^{\text{et, Br}} := \bigcap_{\text{finite étale } G \text{ all } G\text{-torsors } f : Z \to X} \bigcup_{\tau \in \text{H}^1(k,G)} f^\tau(Z^\tau(A)^{\text{Br}}),\]
which is the upper bound on $X(k)$ obtained from applying the Brauer–Manin obstruction to étale covers. One can define possibly even smaller subsets

$$X(A)^{\text{et, descent}} := \bigcap_{\text{finite étale } G} \bigcup_{f: Z \to X} \bigcup_{\tau \in H^1(k, G)} f^\tau (Z^\tau(A)^{\text{descent}})$$

and

$$X(A)^{\text{descent, descent}} := \bigcap_{\text{all smooth affine } G} \bigcup_{f: Z \to X} \bigcup_{\tau \in H^1(k, G)} f^\tau (Z^\tau(A)^{\text{descent}}).$$

One can even define $X(A)^{\text{descent, descent, descent}}$ and so on.

### 8.5.3. Étale-Brauer equals descent.

(References: [Dem09], [Sko09])

The proof of the following theorem combines work of Demarche, Harari, Skorobogatov, and Stoll.

**Theorem 8.5.4.** Let $k$ be a number field. Let $X$ be a nice $k$-variety. Then

$$X(A)^{\text{et, Br}} = X(A)^{\text{et, descent}} = X(A)^{\text{descent}}.$$

**Sketch of proof.** It suffices to prove

$$X(A)^{\text{descent}} \subseteq X(A)^{\text{et, descent}} \subseteq X(A)^{\text{et, Br}} \subseteq X(A)^{\text{descent}}.$$

The first inclusion is [Sko09, Theorem 1.1], which generalizes [Sto07, Proposition 5.17] (a statement that we would write as $X(A)^{\text{et}} = X(A)^{\text{et, et}}$). The idea in both results is, roughly speaking, to show that if $Y \to X$ is an torsor under a finite étale group scheme, and $Z \to Y$ is a torsor under a smooth affine algebraic group, then $Z \to X$ is dominated by some torsor under an even larger smooth affine algebraic group over $X$; this is analogous to the fact that a Galois extension of a Galois extension of a field $k$ is contained in some even larger Galois extension of $k$.

The second inclusion is deduced by applying Proposition 8.5.3 to the étale covers of $X$.

The third inclusion is the main result of [Dem09], which generalizes [Har02, Théorème 2, 2., and Remarque 4], which shows that $X(A)^{\text{conn}} = X(A)^{\text{Br}}$. (The latter already is striking in that it implies that the torsors under all smooth connected affine algebraic groups give no more information than the torsors under all the groups $\text{PGL}_n$.)

**Question 8.5.5.** Does $X(A)^{\text{descent, descent}}$ equal $X(A)^{\text{descent}}$ in general?

### 8.6. Insufficiency of the obstructions

#### 8.6.1. A bielliptic surface.
Skorobogatov proved that the Brauer–Manin obstruction is insufficient to explain all counterexamples to the local-global principle:

**Theorem 8.6.1** ([Sko99]). There exists a nice $\mathbb{Q}$-variety $X$ such that $X(\mathbb{A}^\text{Br}) \neq \emptyset$ but $X(\mathbb{Q}) = \emptyset$.

The proof is involved, so we only outline it. First, we describe the kind of variety used.

**Definition 8.6.2.** A bielliptic surface over an algebraically closed field $k$ is a surface isomorphic to $(E_1 \times E_2)/G$ for some elliptic curves $E_1$ and $E_2$ and some finite group scheme $G$ such that $G$ is a subgroup scheme of $E_1$ acting by translations on $E_1$ and $G$ acts on $E_2$ so that the quotient $E_2/G$ is isomorphic to $\mathbb{P}^1$. (Since $G$ acts freely on $E_1$, it acts freely on $E_1 \times E_2$; i.e., $E_1 \times E_2 \to (E_1 \times E_2)/G$ is $G$-torsor.) A surface over an arbitrary field $k$ is called bielliptic if $X_k$ is bielliptic.

**Warning 8.6.3.** Some authors use the term hyperelliptic surface to mean bielliptic surface, but these surfaces have nothing to do with hyperelliptic curves.

Skorobogatov’s example was a bielliptic surface $X := Y/G$ where $Y$ was a product of two genus 1 curves over $\mathbb{Q}$, and $G$ was a group generated by a fixed-point free automorphism of order 2 of $Y$. Explicitly, his $X$ was birational to the affine surface defined by

$$(x^2 + 1)y^2 = (x^2 + 2)z^2 = 3(t^4 - 54t^2 - 117t - 243).$$

To show that $X(\mathbb{Q}) = \emptyset$, Skorobogatov proved $X(\mathbb{A})^\text{et,Br} = \emptyset$, by applying the Brauer–Manin obstruction to the étale cover $Y \to X$ and its twists.

**Remark 8.6.4.** Because $X(\mathbb{A})^\text{et,Br} = X(\mathbb{A})^\text{descent}$, the nonexistence of rational points must also be explained by a descent obstruction. In fact, it can be explained by the obstruction from a single torsor under a noncommutative finite étale group scheme ([HS02, Section 5.1]).

**8.6.2. A quadric bundle over a curve.**

(References: [Poo10], [CTPS16])

We next construct an “even worse” example:

**Theorem 8.6.5** ([Poo10]). There exists a nice $\mathbb{Q}$-variety $X$ such that $X(\mathbb{A})^\text{et,Br} \neq \emptyset$ but $X(\mathbb{Q}) = \emptyset$.

Combined with Theorem 8.5.4, this shows that even the descent obstruction is not enough to explain all counterexamples to the local-global principle. In the original proof of Theorem 8.6.5, $X$ was a Châtelet surface bundle over a curve of positive genus. We will present a simpler variant, based on [CTPS16, Section 3.1], using quadrics instead of Châtelet surfaces. In this section, all varieties are over $\mathbb{Q}$.  

228
Start with a nice curve $C$ such that $C(\mathbb{Q})$ consists of a single point $c$. (For example, $C$ could be the elliptic curve $y^2 = x^3 - 3$, named 972B1 in [Cre97].) Let $f : C \to \mathbb{P}^1$ be a morphism that is étale at $c$ (for instance, take $f$ corresponding to a uniformizing parameter at $c$). Compose with an automorphism of $\mathbb{P}^1$ to assume that $f(c) = \infty$. Let $U$ be a connected open neighborhood of $c$ in $C(\mathbb{R})$. By the implicit function theorem, $f(U)$ contains an open neighborhood of $\infty$ in $\mathbb{P}^1(\mathbb{R})$. Compose $f$ with a translation automorphism of $\mathbb{P}^1$ to assume that $1 \in f(U)$ and that $f$ is étale above $0, 1 \in \mathbb{P}^1$.

Next we construct a quadric bundle $Y \to \mathbb{P}^1$. View $\mathbb{P}^1$ as the result of glueing $\mathbb{A}^1_{\mathbb{Q}} := \text{Spec} \mathbb{Q}[t]$ and $\mathbb{A}^1_{\mathbb{T}} := \text{Spec} \mathbb{Q}[T]$ using $t = 1/T$. In $\mathbb{P}^4 \times \mathbb{A}^1_{\mathbb{T}}$, define the closed subscheme

$$Y(t) := (t(t - 1)x_0^2 + x_1^2 + x_2^2 + x_3^2 + x_4^2 = 0.$$ 

Similarly, in $\mathbb{P}^4 \times \mathbb{A}^1_{\mathbb{T}}$, define the closed subscheme

$$Y^{(T)} := (1 - T)X_0^2 + x_1^2 + x_2^2 + x_3^2 + x_4^2 = 0.$$ 

Glue $Y(t)$ to $\mathbb{A}^1_{\mathbb{T}}$ and $Y^{(T)}$ to $\mathbb{A}^1_{\mathbb{T}}$ using $t = 1/T$ and $x_0 = T/X_0$ to obtain $Y \to \mathbb{P}^1$. Alternatively, if $\mathcal{E}$ denotes the rank 5 vector bundle $\mathcal{O}(1) \oplus \mathcal{O}^{\oplus 4}$ on $\mathbb{P}^1$, then $Y$ is the zero locus in $\mathbb{P}^\mathcal{E} := \text{Proj} \text{Sym} \mathcal{E}$ of a section of $\text{Sym}^2 \mathcal{E}$; in particular, $Y$ is projective over $\mathbb{Q}$. A calculation shows that $Y(t)$ and $Y^{(T)}$ are smooth over $\mathbb{Q}$, so $Y$ is smooth over $\mathbb{Q}$. Thus $Y$ is a family of 3-dimensional quadrics over the base $\mathbb{P}^1$, with two degenerate fibers, above 0 and 1. For each $t \in \mathbb{P}^1$, let $Y_t$ denote the fiber above $t$. In particular, the locus in $Y^{(T)}$ above $T = 0$ is the fiber

$$Y_\infty : X_0^2 + x_1^2 + x_2^2 + x_3^2 + x_4^2 = 0,$$

a smooth quadric in $\mathbb{P}^4$. See Figure 1.

Let $\pi : X \to C$ be the base extension of $Y \to \mathbb{P}^1$ by $f$:

$$\begin{array}{ccc}
X & \longrightarrow & Y \\
\pi \downarrow & & \downarrow \\
C & \longrightarrow & \mathbb{P}^1.
\end{array}$$

**Proposition 8.6.6.** The $\mathbb{Q}$-variety $X$ is nice.

**Proof.** Since $Y \to \mathbb{P}^1$ is projective with geometrically integral fibers, the same is true of $X \to C$; in particular, $X$ is a projective and geometrically integral $\mathbb{Q}$-variety. The morphism $Y \to \mathbb{P}^1$ is smooth above all points except 0, 1, so $X \to C$ is smooth above all points of $C$ outside those above 0, 1 $\in \mathbb{P}^1$; since $C$ is smooth over $\mathbb{Q}$, this implies that $X$ is smooth over $\mathbb{Q}$ outside the points above 0, 1 $\in \mathbb{P}^1$. Similarly, $C \to \mathbb{P}^1$ is smooth above 0, 1, so $X \to Y$ is smooth at the points above 0, 1; since $Y$ is smooth over $\mathbb{Q}$, this implies that $X$ is smooth over $\mathbb{Q}$ also at the points above 0, 1 $\in \mathbb{P}^1$. Thus $X$ is nice. $\square$

**Proposition 8.6.7.** We have $X(\mathbb{Q}) = \emptyset$. 

229
Figure 1. Real points of the varieties $C$ and $Y$ over $\mathbb{P}^1$ are shown in black and blue. Some fibers of $Y \to \mathbb{P}^1$ are shown with imaginary points in green.

Proof. The sole point of $C(\mathbb{Q})$ maps to $\infty \in \mathbb{P}^1$, but $Y_\infty$ has no $\mathbb{Q}$-points. \hfill \square

As a warm-up to proving that $X(\mathbb{A})^{et,Br} \neq \emptyset$, we prove that $X(\mathbb{A})^{Br} \neq \emptyset$.

For each finite prime $p$, any quadratic form over $\mathbb{Q}_p$ of rank $\geq 5$ has a nontrivial zero [Ser73, IV.2.2, Theorem 6], so we may choose $y_p \in Y_\infty(\mathbb{Q}_p)$ and let $x_p = (y_p, c) \in X(\mathbb{Q}_p)$. Let $y_\mathbb{R}$ be the unique point in $Y_1(\mathbb{R})$, let $c_\mathbb{R} \in U \subseteq C(\mathbb{R})$ be such that $f(c_\mathbb{R}) = 1 \in \mathbb{P}^1(\mathbb{R})$, and let $x_\mathbb{R} = (y_\mathbb{R}, c_\mathbb{R}) \in X(\mathbb{R})$ (we use the subscript $\mathbb{R}$ for the archimedean place, to avoid confusion with the point $\infty \in \mathbb{P}^1$). Together, these define $x = (x_v) \in X(\mathbb{A})$.

Proposition 8.6.8. We have $x \in X(\mathbb{A})^{Br}$. 

230
Proof. The adeles $\pi(x)$ and $c$ agree except for their archimedean parts $c_R$ and $c$, which lie in the same connected component of $C(\mathbb{R})$. By this and Proposition 8.2.9 any $A \in Br C$ takes the same value at $\pi(x)$ as at $c \in C(\mathbb{Q})$; by Proposition 8.2.2 that value is 0. Thus $\pi(x) \in C(A)^{Br}$. Also, $Br C \to Br X$ is surjective by Proposition 6.9.15 Corollary 8.1.10 then implies $x \in X(A)^{Br}$. □

To generalize Proposition 8.6.8 to prove that $x \in X(A)_{et,Br}^c$, we must understand the category $\text{F}\text{E}t(X)$ of finite étale covers of $X$.

Lemma 8.6.9. The morphism $X \to C$ induces an equivalence of categories $\text{F}\text{E}t(C) \to \text{F}\text{E}t(X)$.

Proof. This follows (by [SGA 1] IX.6.8)] from the fact that each geometric fiber of $X \to C$ (a smooth 3-dimensional quadric or a cone over a smooth 2-dimensional quadric) is algebraically simply connected. □

Proposition 8.6.10. We have $x \in X(A)_{et,Br}^c$.

Proof. Suppose that $G$ is a finite étale group scheme over $\mathbb{Q}$, and $X' \to X$ is a $G$-torsor. We must show that one of the twists of $X' \to X$ has an adelic point not obstructed by the Brauer group. By Lemma 8.6.9, $X' \to X$ is the base extension of a $G$-torsor $C' \to C$. We may replace $C'$ by a twist to assume that $c$ lifts to some $c'' \in C'(\mathbb{Q})$. Let $C''$ be the irreducible component of $C''$ containing $c''$. The fiber product $X'' := X \times_C C''$ fits in a diagram

\[ X'' \leftarrow X' \xrightarrow{G\text{-torsor}} X \xrightarrow{f} Y \]

\[ C'' \leftarrow C' \xrightarrow{G\text{-torsor}} C \xrightarrow{\pi} \mathbb{P}^1. \]

Since $C'' \to C$ is finite étale, $C''$ is smooth and projective; moreover, $C''$ is integral and has a $\mathbb{Q}$-point, so $C''$ is a nice curve. Similarly, $X''$ is smooth and projective, and $X'' \to C''$ has geometrically integral fibers (just like $Y \to \mathbb{P}^1$), so $X''$ is nice too.

We claim that $x$ lifts to a point $x'' \in X''(A)$. For each finite prime $p$, let $x_p'' = (x_p, c'') \in X''(\mathbb{Q}_p)$. Since $U$ is algebraically simply connected, the inverse image of $U$ in $C''(\mathbb{R})$ is a disjoint union of copies of $U$; let $U''$ be the copy containing $c''$, let $c_R'' \in U''$ be the point mapping to $c_R \in U$, and let $x_R'' = (x_R, c_R'') \in X''(\mathbb{R})$. Thus we have $x'' \in X''(A)$ mapping to $x \in X(A)$.

The same proof as for Proposition 8.6.8 shows that $x'' \in X''(A)^{Br}$, so $X'(A)^{Br}$ is nonempty. This argument applies to all finite étale torsors over $X$, so $X(A)_{et,Br}^c$ is nonempty. □

This completes the proof of Theorem 8.6.5.
8.6.3. Hypersurfaces and complete intersections.

(Reference: [PV04])

**Definition 8.6.11.** A scheme-theoretic intersection \( X = H_1 \cap \cdots \cap H_r \) of hypersurfaces \( H_i \subseteq \mathbb{P}^n \) is called a **complete intersection** if \( \dim X = n - r \).

In particular, any hypersurface in \( \mathbb{P}^n \) is a complete intersection.

**Theorem 8.6.12.** Let \( k \) be a number field. If \( X \) is a smooth complete intersection in some \( \mathbb{P}^n_k \) and \( \dim X \geq 3 \), then the descent obstruction and Brauer–Manin obstruction for \( X \) are vacuous; that is, \( X(\mathbb{A})^{\text{descent}} = X(\mathbb{A})^{\text{Br}} = X(\mathbb{A}) \).

**Sketch of proof.** By Theorem 8.5.4, it suffices to prove \( X(\mathbb{A})^{\text{et,Br}} = X(\mathbb{A}) \). This follows immediately from the following two claims:

(i) The variety \( X_{\bar{k}} \) is algebraically simply connected (Definition 3.5.45).

(ii) The homomorphism \( \text{Br} k \to \text{Br} X \) is an isomorphism.

Part (i) follows from the weak Lefschetz theorem, which says that the homomorphism of fundamental groups \( \pi_1(X(\mathbb{C}), x) \to \pi_1(\mathbb{P}^n(\mathbb{C}), x) \) is an isomorphism (here an embedding \( \bar{k} \to \mathbb{C} \) is chosen and \( x \in X(\mathbb{C}) \)) [Mil63, Theorem 7.4]. For the proof of (ii), see [PV04, Proposition A.1].

Heuristics suggest that most smooth hypersurfaces \( X \subseteq \mathbb{P}^n_Q \) of degree \( d > n+1 = \dim X + 2 \) have no rational points. On the other hand, a positive fraction of such hypersurfaces have \( \mathbb{Q}_p \)-points for all \( p \leq \infty \) [PV04, Theorem 3.6]. Thus one expects many counterexamples to the local-global principle among such hypersurfaces. But there is no smooth hypersurface of dimension \( \geq 3 \) for which the local-global principle has been proved to fail! The reason we are unable to prove anything in this setting is that our only available tools, the descent and Brauer–Manin obstructions, give no information.

We need some new obstructions!

**Remark 8.6.13.** The Brauer–Manin obstruction does yield counterexamples to the local-global principle for some 2-dimensional hypersurfaces, such as some cubic surfaces: see Section 9.4.9.

**Remark 8.6.14.** There are some conditional counterexamples among hypersurfaces of higher dimension. For instance, Lang’s conjecture [Lan74, (1.3)] that \( V(\mathbb{Q}) \) is finite for every nice hyperbolic \( \mathbb{Q} \)-variety \( V \) implies the existence of nice hypersurfaces in \( \mathbb{P}^4 \) that violate the local-global principle: see [SW95, Poo01]. (A smooth variety \( V \) over a subfield of \( \mathbb{C} \) is (Brody) hyperbolic if every holomorphic map \( \mathbb{C} \to V(\mathbb{C}) \) is constant.)
Exercises

8.1. Prove Proposition 8.1.8, Corollary 8.1.9 and Corollary 8.1.10.

8.2. Let $k$ be a global field. Let $X$ be a proper $k$-variety such that $X(A) \neq \emptyset$. Let $A \in \text{Br } X$. Suppose that there exists a place $w$ such that the evaluation map $X(k_w) \to \text{Br } k_w$ given by $A$ is not constant. Prove that weak approximation for $X$ fails.

8.3. (Brauer–Manin obstruction for a degree 4 del Pezzo surface) Let $X$ be the smooth surface defined by $uv = x^2 - 5y^2$ and $(u + v)(u + 2v) = x^2 - 5z^2$ in $\mathbb{P}^4$. (This example is from [BSD75, Section 4].) Let $K = k(X)$.
(a) Prove that $X(A) \neq \emptyset$. (Suggestion: Let $Y$ be the smooth genus 1 curve obtained by intersecting $X$ with the hyperplane $x = 0$. Spread out $Y$ to a smooth proper scheme over $\mathbb{Z} - S^{-1}$ for some finite set of places $S$. For $p \notin S$, use the Hasse–Weil bound or Lang’s theorem on $H^1$ over finite fields to show that $Y$ has an $\mathbb{F}_p$-point, and deduce that $Y$ has a $\mathbb{Q}_p$-point.)
(b) Let $A$ be the class of the quaternion algebra $(5, \frac{u+v}{u})$ in $\text{Br } K$. Find other representations of $A$ to show that $A \in \text{Br } X$. (Hint: Why does it suffice to find representations on open subsets that cover the codimension 1 points of $X$?)
(c) Prove that if $P = (u : v : x : y : z) \in X(\mathbb{Q}_p)$ for some $p \leq \infty$, then
\[
\text{inv}_p A(P) = \begin{cases} 
0, & \text{if } p \neq 5; \\
1/2, & \text{if } p = 5.
\end{cases}
\]
(Hint: If $5 \in \mathbb{Q}_p^{\times 2}$, what can be said about the image of $A$ in $\text{Br } X_{\mathbb{Q}_p}$?)
(d) Deduce that $X(A)^{\text{Br}} = \emptyset$, so $X(\mathbb{Q}) = \emptyset$.

8.4. Let $S$ be a finite set of places of a number field $k$, containing all the archimedean places. Let $\mathcal{O}_{k,S}$ be the ring of $S$-integers. Let $\mathcal{G}$ be a finite étale group scheme over $\mathcal{O}_{k,S}$. Prove that $H^1(\mathcal{O}_{k,S}, \mathcal{G})$ is finite.

8.5. (Integral descent) Let $\mathcal{O}_{k,S}$ and $\mathcal{G}$ be as above. Let $X$ be a finite-type separated $\mathcal{O}_{k,S}$-scheme, and let $Z \to X$ be a $\mathcal{G}$-torsor. For each $\tau \in H^1(\mathcal{O}_{k,S}, \mathcal{G})$, define a twisted torsor $f^\tau : Z^\tau \to X$ such that
\[
X(\mathcal{O}_{k,S}) = \coprod_{\tau \in H^1(\mathcal{O}_{k,S}, \mathcal{G})} f^\tau(Z^\tau(\mathcal{O}_{k,S})).
\]

8.6. Let $\mathcal{O}_{k,S}$ be as above. Let $\mathcal{U}$ be an “affine curve of genus 1 over $\mathcal{O}_{k,S}$,” by which we mean a smooth, separated, finite-type $\mathcal{O}_{k,S}$-scheme whose generic fiber is an affine open subset $U$ of a nice $k$-curve $E$ of genus 1. Show that Faltings’s theorem implies that $\mathcal{U}(\mathcal{O}_{k,S})$ is finite. (Hints: Show that you may enlarge $S$ and/or extend $k$ as needed. Find a sequence
of Galois coverings $U'' \to U' \to U$, where $U' = X' - F'$ with $X'$ a nice genus 1 curve and $F' \subseteq X'$ a closed subscheme with $\#F(\overline{k}) \geq 4$, and $U''$ is an affine open subset of a ramified covering $X'' \to X'$ branched only over $F'$.

8.7. Let $k$ be a number field. Let $X$ be a $k$-variety. Let $G$ be a smooth affine algebraic group over $k$. Let $Z \to X$ be a $G$-torsor.

(a) Prove that for each place $v$, the set $f(Z(k_v))$ is open in $X(k_v)$. (Hint: Proposition 3.5.72(ii).)

(b) Prove that for each place $v$, the evaluation map $X(k_v) \to H^1(k_v, G)$ associated to $f$ is continuous (for the $v$-adic topology on $X(k_v)$ and the discrete topology on $H^1(k_v, G)$).

(c) Prove that for each place $v$, the set $f(Z(k_v))$ is closed in $X(k_v)$.

(d) Use results from the proof of Theorem 6.5.13 to prove that

$$f(Z(A)) = X(A) \cap \prod_v f(Z(k_v))$$

as subsets of $\prod_v X(k_v)$.

(e) Prove that $f(Z(A))$ is closed in $X(A)$.

(f) Prove that for each $\tau \in H^1(k, G)$,

$$\{ (x_v) \in X(A) : x_v \text{ maps to } \tau_v \in H^1(k_v, G) \text{ for all } v \} = f^\tau(Z^\tau(A)),$$

where $\tau_v$ denotes the image of $\tau$ in $H^1(k_v, G)$.

(g) Prove that $X(A)^f = \bigcup_{\tau \in H^1(k, G)} f^\tau(Z^\tau(A))$.

(h) Prove that if $X$ is proper, then $X(A)^f$ is closed in $X(A)$. 

234
CHAPTER 9

Surfaces

Curves can be divided into those of genus 0, those of genus 1, and those of genus > 1. In these three cases, the canonical sheaf $\omega_X$ is anti-ample, trivial ($\mathcal{O}_X$), and ample, respectively.

Similarly, one can classify higher-dimensional varieties according to how ample $\omega_X$ is. At one extreme lie the Fano varieties, for which $\omega_X^\otimes (-1)$ is ample; at the other lie the varieties of general type.

9.1. Kodaira dimension

(Reference: [Iit82, §10.5])

Let $X$ be a nice variety over a field $k$. We will associate to $X$ an element

$$\kappa = \kappa(X) \in \{-\infty, 0, 1, \ldots, \dim X\}$$

called the Kodaira dimension of $X$.

Let $\omega_X$ be the canonical sheaf.

Case 1. We have $H^0(X, \omega_X^\otimes m) = 0$ for all $m \in \mathbb{Z}_{\geq 1}$.

Then define $\kappa := -\infty$.

Case 2. We have $H^0(X, \omega_X^\otimes m) \neq 0$ for some $m \in \mathbb{Z}_{\geq 1}$.

If $m$ is such that $H^0(X, \omega_X^\otimes m) \neq 0$, then a choice of basis defines a rational map

$$\phi_m: X \rightarrow \mathbb{P}^{N(m)}$$

(defined on the open subscheme $U_m$ of points at which the global sections generate $\omega_X^\otimes m$).

In this case, let $\overline{\phi_m(X)}$ denote the Zariski closure of $\phi_m(U_m)$ in $\mathbb{P}^{N(m)}$. Then for $m > 1$ sufficiently large and divisible, $\overline{\phi_m(X)}$ is independent of $m$ up to birational equivalence (cf. [Iit82, §10.1]), and we let $\kappa$ be its dimension. Alternatively, in Case 2 one can use one of the following equivalent definitions:

(i) $\kappa := \max_m \dim \overline{\phi_m(X)}$.

(ii) $\kappa$ is the integer such that there exist $c_1, c_2 \in \mathbb{R}_{>0}$ such that

$$c_1 m^\kappa < \dim_k H^0(X, \omega_X^\otimes m) < c_2 m^\kappa$$

for all $m > 0$ such that $H^0(X, \omega_X^\otimes m) \neq 0$.

(iii) $\kappa := (\text{tr deg}_k \text{Frac } R) - 1$, where $R$ is the canonical ring $\bigoplus_{m \geq 0} H^0(X, \omega_X^\otimes m)$. 

235
The equivalence of (i) and (ii) is \[\text{[Lit82, Theorem 10.2]}\]. The equivalence of (i) and (iii) follows since the function field of \(\phi_m(X)\) for sufficiently large and divisible \(m\) is the degree 0 homogeneous part of \(\text{Frac} R\) (and for other \(m\) it is smaller).

**Proposition 9.1.1.** Let \(X\) be a nice curve of genus \(g\). Then

\[
\begin{align*}
g = 0 & \implies \kappa(X) = -\infty \\
g = 1 & \implies \kappa(X) = 0 \\
g \geq 2 & \implies \kappa(X) = 1.
\end{align*}
\]

**Proof.** Exercise. \(\square\)

**Proposition 9.1.2.**

(a) If \(X\) and \(Y\) are birationally equivalent nice \(k\)-varieties, then \(\kappa(X) = \kappa(Y)\).

(b) If \(X\) is a nice \(k\)-variety, and \(L/k\) is a field extension, then \(\kappa(X_L) = \kappa(X)\).

**Proof.**

(a) The proof of \([\text{Har77, II.8.19]}\] generalizes to prove that the birational map \(X \dashrightarrow Y\) induces a natural isomorphism \(H^0(Y, \omega_Y^{\otimes m}) \to H^0(X, \omega_X^{\otimes m})\) for any \(m \geq 0\), so these vector spaces have the same dimension.

(b) The formation of \(H^0(X, \omega_X^{\otimes m})\) commutes with field extension. \(\square\)

**Definition 9.1.3.** If \(X\) is a geometrically integral \(k\)-variety that is birational to a nice \(k\)-variety \(Y\), define \(\kappa(X) = \kappa(Y)\).

Proposition 9.1.2 shows that the definition is independent of the choice of \(Y\). Resolution of singularities is known if \(\text{char} k = 0\), so then a \(Y\) exists and \(\kappa(X)\) is automatically defined. (The paper \([\text{Luo87]}\] contains a definition of \(\kappa(X)\) that does not rely on resolution of singularities, and hence works in every characteristic.)

**Definition 9.1.4.** If \(\kappa(X) = \dim X\) (the maximum possible), then \(X\) is said to be of \textbf{general type}, or \textbf{pseudo-canonical}. For a nice variety of general type, one can show that for \(m\) sufficiently large, \(\phi_m\) is birational onto its image \([\text{Lit82, §10.2a, §10.6b]}\]. For instance, if \(X\) is a nice curve of general type, then the Riemann–Roch theorem shows that \(m \geq 3\) suffices (more specifically, this follows from \([\text{Har77, Corollary 3.2(b)}]\], since for \(g \geq 2\), we have \(3(2g - 2) \geq 2g + 1\). If \(X\) is a nice surface of general type, then \(m \geq 5\) suffices \([\text{Bom73, Eke88}].\)

**Example 9.1.5.** Let \(X\) be a nice variety. If \(\omega_X\) is ample, then \(X\) is of general type.

**Warning 9.1.6.** The converse need not hold. Suppose that \(Y\) is a nice surface of degree 5 in \(\mathbb{P}^3\), so \(\omega_Y \simeq O(1)\) by \([\text{Har77, II.8.20.3}].\) Let \(X \to Y\) be the blow-up of \(Y\) at a point
$P \in Y(\mathbb{C})$. By the proof of Proposition 9.1.2, the rational map $f_m$ determined by $\omega_X^{\otimes m}$ equals the composition

$$X \longrightarrow Y \overset{m\text{-uple}}{\longrightarrow} \mathbb{P}^N(m).$$

Thus $X$ is of general type, but $f_m$ is not a closed immersion for any $m \geq 1$, so $\omega_X$ is not ample.

### 9.2. Varieties that are close to being rational

(Reference: [Kol96])

#### 9.2.1. Rational, stably rational, and unirational varieties.

**Definition 9.2.1.** Let $X$ be an $n$-dimensional integral variety over an algebraically closed field $k$. Call $X$ **rational** if it is birational to $\mathbb{P}^n$. Call $X$ **stably rational** if there exists $m \in \mathbb{N}$ such that $X \times \mathbb{P}^m$ is rational. Call $X$ **unirational** if there exists a dominant rational map $\mathbb{P}^N \dashrightarrow X$ for some $N \geq 0$.

**Remark 9.2.2.** Suppose that $X$ is unirational, so there exists a dominant rational map $\phi : \mathbb{P}^N \dashrightarrow X$ for some $N \geq 0$. Then there exists also a dominant rational map $\mathbb{P}^n \dashrightarrow X$ with $n = \dim X$; in fact, one can show that there exists a rational map $\mathbb{P}^m \dashrightarrow \mathbb{P}^N \dashrightarrow X$ is dominant.

**Example 9.2.3.** Fix integers $0 \leq m \leq n$ and an $n$-dimensional $k$-vector space $V$. The Grassmannian $\text{Gr}(m,n) = \text{Gr}(m,V)$ is the moduli space of $m$-dimensional subspaces of $V$. It is birational to $\mathbb{P}^m_{k(n-m)}$ (even if $k$ is not algebraically closed) since if we identify $V$ with $k^m \times k^{n-m}$, then $\text{Gr}(m,n)$ has a Zariski open subspace $U \simeq \mathbb{A}^m(n-m)$ parametrizing the graphs of linear maps $k^m \to k^{n-m}$.

**Example 9.2.4.** Consider $\mathbb{P}\mathcal{E} \to \mathbb{P}^1$, where $\mathcal{E}$ is a rank 2 vector bundle on $\mathbb{P}^1$. By [Har77, Corollary V.2.14], $\mathcal{E} \simeq \mathcal{O}(m) \oplus \mathcal{O}(n)$ for some $m, n \in \mathbb{Z}$. Tensoring $\mathcal{E}$ with a line bundle does not change $\mathbb{P}\mathcal{E}$, so we may assume that $\mathcal{E} \simeq \mathcal{O} \oplus \mathcal{O}(n)$ for some $n \geq 0$; the corresponding $\mathbb{P}\mathcal{E}$ is called the Hirzebruch surface $F_n$. Since $\mathcal{E}$ is locally free of rank 2, there exists a dense open subscheme $U$ of $\mathbb{P}^1$ such that the part of $\mathbb{P}\mathcal{E}$ above $U$ is isomorphic to $\mathbb{P}^1 \times U$; thus $F_n$ is a rational surface for each $n$.

**Remark 9.2.5 (Rationality in a family).** In a family of varieties $\mathcal{X} \xrightarrow{f} B$, rationality of one fiber $\mathcal{X}_b := f^{-1}(b)$ does not imply rationality of the other fibers. In fact, there exists a smooth projective morphism $\mathcal{X} \to B$ of $\mathbb{C}$-varieties such that $\{b \in B(\mathbb{C}) : \mathcal{X}_b \text{ is rational}\}$ and $\{b \in B(\mathbb{C}) : \mathcal{X}_b \text{ is not rational}\}$ are both dense in $B(\mathbb{C})$ for the analytic topology [HPT16, Theorem 1.1]. In the example constructed, for $b \in B(\mathbb{C})$ outside a countable union of lower-dimensional closed subvarieties, the fiber $\mathcal{X}_b$ is not even stably rational.
Remark 9.2.5 is one of the reasons for introducing rational connectedness, which is weaker than rationality and stable rationality: see Theorem 9.2.18.

Proposition 9.2.6 (Cohomology of a rational surface). Let $X$ be a nice rational surface over a separably closed field $k$. Then $	ext{Pic} \, X$ is a free finite-rank abelian group, and for any prime $\ell \neq \text{char} \, k$,

$$
\begin{align*}
H^0_{\text{et}}(X, \mathbb{Q}_\ell) &\simeq \mathbb{Q}_\ell \\
H^1_{\text{et}}(X, \mathbb{Q}_\ell) &\simeq 0 \\
H^2_{\text{et}}(X, \mathbb{Q}_\ell) &\simeq (\text{Pic} \, X) \otimes \mathbb{Q}_\ell(-1) \\
H^3_{\text{et}}(X, \mathbb{Q}_\ell) &\simeq 0 \\
H^4_{\text{et}}(X, \mathbb{Q}_\ell) &\simeq \mathbb{Q}_\ell(-2).
\end{align*}
$$

Sketch of proof. The middle isomorphism is induced by (7.6.2). The statements are true for $\mathbb{P}^2$, and one can show that their truth is unaffected by blowing up a point. □

Remark 9.2.7. Here we explain a variant of unirationality. A dominant rational map $Y \dasharrow X$ is called separably dominant if $k(Y)$ is a finite separable extension of $k(X)$. Call an $n$-dimensional integral variety $X$ separably unirational if there exists a separably dominant rational map $\mathbb{P}^n \dasharrow X$. In characteristic 0 there is no difference between unirational and separably unirational. But in characteristic $p$, the property of being separably unirational is better behaved in many regards.

9.2.2. Ruled and uniruled varieties.

Definition 9.2.8. Let $X$ be an $n$-dimensional integral variety over an algebraically closed field $k$. Call $X$ ruled if it is birational to $Y \times \mathbb{P}^1$ for some integral $k$-variety $Y$. Call $X$ uniruled if there exists a dominant rational map $Y \times \mathbb{P}^1 \dasharrow X$ for some integral $k$-variety $Y$ of dimension $n - 1$. (A point is not uniruled.)

Proposition 9.2.9. If $X$ is uniruled, there is a rational curve through a general point of $X$, i.e., there is a dense open subset $U \subset X$ such that for every $x \in U(k)$, there is a nonconstant rational map $\mathbb{P}^1 \dasharrow X$ whose image contains $x$. The converse holds if $k$ is uncountable.

Proof. Suppose that $X$ is uniruled, say via $Y \times \mathbb{P}^1 \dasharrow X$. We may replace $Y$ by the dense open set consisting of $y \in Y$ such that $\{y\} \times \mathbb{P}^1 \dasharrow X$ is defined and nonconstant. The image of the dominant rational map $Y \times \mathbb{P}^1 \dasharrow X$ contains a dense open subset $U$ of $X$; this proves the first part.

Now let us prove the converse. Let $n = \dim X$. Replace $X$ by a birationally equivalent variety to assume that $X$ is projective. The theory of the Hilbert scheme shows that the
nonconstant rational maps $\mathbb{P}^1 \to X$ fall into countably many algebraic families $B \times \mathbb{P}^1 \to X$. If any of these rational maps $B \times \mathbb{P}^1 \to X$ is dominant, then for a general linear $(n - 1)$-dimensional section $Y$ of a nonempty affine open subscheme of $B$, the rational map $Y \times \mathbb{P}^1 \to X$ is dominant, so $X$ is uniruled. Otherwise, each rational map $B \times \mathbb{P}^1 \to X$ has image contained in a positive-codimensional subvariety of $X$. Since $k$ is uncountable, the union of these images cannot cover the $k$-points of any dense open subset $U$ of $X$. □

**Remark 9.2.10.** As in Remark 9.2.7, one can also define *separably uniruled*.

There is also a criterion for being separably uniruled in terms of the existence of a single rational curve satisfying a condition that guarantees that it moves in a family, as we now explain. Let $X$ be a nice variety of dimension $d$ over an algebraically closed field. Let $\mathcal{TX}$ be the *tangent bundle* of $X$, defined as the $\mathcal{O}_X$-dual of the sheaf of 1-forms $\Omega_X$; it is a rank $d$ vector bundle. Given a rational curve $f : \mathbb{P}^1 \to X$, we obtain a rank $d$ vector bundle $f^* \mathcal{TX}$ on $\mathbb{P}^1$. Every vector bundle on $\mathbb{P}^1$ is a direct sum of line bundles, so $f^* \mathcal{TX} \cong \mathcal{O}(a_1) \oplus \cdots \oplus \mathcal{O}(a_d)$ for some $a_1, \ldots, a_d \in \mathbb{Z}$. Call the rational curve *free* if $a_i \geq 0$ for all $i$, and *very free* if $a_i \geq 1$ for all $i$.

**Theorem 9.2.11.** Let $X$ be a nice variety over an algebraically closed field. Then $X$ is separably uniruled if and only if $X$ contains a free rational curve.

**Proof.** See [Kol96, Theorem IV.1.9]. □

**9.2.3. Rationally connected varieties.** Suppose that $X$ is a nice variety over an algebraically closed field $k$. Roughly, $X$ is called rationally connected if there is an algebraic family of rational curves such that for almost every pair of points $(x, x')$, there is a rational curve in the family joining them.

Let us make this precise. In this section, by a *rational curve* in $X$, we mean a (possibly constant) rational map $f : \mathbb{P}^1 \to X$; by Proposition 3.6.5(b), it would be equivalent to require $f$ to be a morphism. Say that two points $x, x' \in X(k)$ can be *joined by a rational curve* if there is a rational curve $f$ such that $x, x' \in f(\mathbb{P}^1)$. An *algebraic family of rational curves*, parametrized by a base variety $B$, is a rational map $F : B \times \mathbb{P}^1 \to X$; this is a family in the sense that for (almost every) $b \in B(k)$, the restriction of $F$ to $\{b\} \times \mathbb{P}^1$ defines a rational map $\mathbb{P}^1 \to X$. Given such a family, the pairs of points that it joins are the pairs of the form $(F(b, t), F(b, t'))$ for some $b \in B(k)$ and $t, t' \in \mathbb{P}^1(k)$.

**Definition 9.2.12.** The variety $X$ is *rationally connected* if there is a variety $B$ and a rational map $F : B \times \mathbb{P}^1 \to X$ such that the rational map

$$B \times \mathbb{P}^1 \times \mathbb{P}^1 \to X \times X$$

$$(b, t, t') \mapsto (F(b, t), F(b, t'))$$

is dominant.
is dominant.

**Proposition 9.2.13.** If $X$ is rationally connected, then any general pair of points can be joined by a rational curve; i.e., there is a dense open subset $U$ of $X \times X$ such that any pair $(x, x') \in U(k)$ can be joined by a rational curve. The converse holds if $k$ is uncountable.

**Proof.** The proof is the same as that of Proposition 9.2.9. □

We define **separably rationally connected** by replacing “dominant” by “separably dominant” in the definition of rationally connected. Here is the analogue of Theorem 9.2.11.

**Theorem 9.2.14.** Let $X$ be a nice variety over an algebraically closed field. Then $X$ is separably rationally connected if and only if $X$ contains a very free rational curve.

**Proof.** See [Kol96, Theorem IV.3.7]. □

Moreover, it turns out that if $X$ is separably rationally connected, then any finite subset of $X(k)$ is contained in a very free rational curve.

Rational connectedness also has a topological implication:

**Theorem 9.2.15.** If $X$ is a rationally connected variety over $\mathbb{C}$, then the manifold $X(\mathbb{C})$ is simply connected.

**Proof.** See [Cam91, Theorem 3.5] or [KMM92b, 2.5.3]. □

**9.2.4. Rationally chain connected varieties.**

**Definition 9.2.16.** A variety $X$ over an algebraically closed field $k$ is **rationally chain connected** if there exists a variety $B$, a proper morphism $C \to B$ whose fibers are connected unions of rational curves, and a rational map $C \to X$ such that the induced rational map $C \times_B C \to X \times X$ is dominant.

If $X$ is rationally chain connected, then a general pair $(x, x')$ of points on $X$ can be joined by a chain of rational curves, i.e., there exist points $x_0, \ldots, x_n$ with $x_0 = x$ and $x_n = x'$ such that for $i = 0, 1, \ldots, n - 1$, the points $x_i$ and $x_{i+1}$ can be joined by a rational curve.

Although rational chain connectedness seems weaker than rational connectedness, the definitions turn out to be equivalent under mild hypotheses:

**Theorem 9.2.17 ([KMM92b, (2.1)] and [Kol96, Theorem IV.3.10.3]).** A smooth variety $X$ over a field of characteristic 0 is rationally chain connected if and only if it is rationally connected.

Theorem 9.2.17 implies that rational connectedness behaves well in families:
Theorem 9.2.18 (Deformation invariance of rational connectedness [KMM92b, 2.4]). Let $k$ be an algebraically closed field of characteristic 0. Let $S$ be a connected $k$-variety. Let $\pi: X \rightarrow S$ be a smooth proper morphism with geometrically integral fibers. If one fiber is rationally connected, then all fibers are rationally connected.

Sketch of proof. One shows that

- the set of $s \in S$ such that the fiber $\pi^{-1}(s)$ has a very free rational curve is open; and
- the set of $s \in S$ such that the fiber $\pi^{-1}(s)$ is rationally chain connected is closed.

By Theorems 9.2.14 and 9.2.17, both sets equal the set of $s \in S$ such that $\pi^{-1}(s)$ is rationally connected. A nonempty open and closed subset of a connected space is the whole space. □

9.2.5. Fano varieties.

Definition 9.2.19. Let $X$ be a nice variety over a field $k$, and let $\omega_X$ be its canonical sheaf. Call $X$ **Fano** if $\omega_X^{\otimes(-1)}$ is ample.

Example 9.2.20. If $X = \mathbb{P}^n$, then $\omega_X^{\otimes(-1)} \cong \mathcal{O}(n + 1)$ [Har77, II.8.20.1], so $X$ is Fano.

Example 9.2.21. Let $X$ be a nice curve. A line bundle $\mathcal{L}$ on $X$ is ample if and only if $\deg \mathcal{L} > 0$; applying this to $\omega_X^{\otimes(-1)}$ shows that $X$ is Fano if and only if $2 - 2g > 0$, which holds if and only if $g = 0$.

Example 9.2.22. A nice hypersurface of degree $d$ in $\mathbb{P}^n$ is Fano if and only if $d \leq n$.

Remark 9.2.23. If $L/k$ is an extension of fields, then $X$ is Fano if and only $X_L$ is Fano, since the formation of $\omega_X$ commutes with base change and ampleness is unaffected by field extension (for ampleness, observe that the property of global sections of a power of a line bundle determining a closed immersion is unaffected, or see [EGA IV$_2$ 2.7.2] for a more general statement).

Let $X$ be a Fano variety. Let $m = \dim X$. Let $K$ be a canonical divisor on $X$. If $-K$ is very ample, then the complete linear system $|{-K}|$ embeds $X$ as a subvariety of some $\mathbb{P}^n$, and the degree of this subvariety is the number of points (counted with multiplicity) resulting from cutting it with $m$ general hyperplanes in $\mathbb{P}^n$; equivalently, this degree equals the self-intersection number $(-K)^m$ on $X$. In general, $-K$ is only ample, but some positive integer multiple of $-K$ is very ample, so again $(-K)^m$ is positive. We define the **degree** of $X$ as $(-K)^m$.

Warning 9.2.24. The property of being Fano is not invariant under birational maps between nice varieties. See Remark 9.4.6.
9.2.6. Implications. Throughout this section, $X$ is a nice variety of dimension $d \geq 1$ over $\mathbb{C}$. The following diagram summarizes the known implications between the properties we have been discussing:

```
  rational
  ↓ ≠
  stably rational
  ↓ ≠
  unirational
  ↓ ≠
  Fano

rationally chain connected ⇔ rationally connected ⇔ $H^0(X, \Omega_X^m) = 0 \forall m \geq 1$
  ↓ ≠
  uniruled
  ↓
  $\kappa = -\infty$
```

The symbol $\neq$ means that the properties are not equivalent, i.e., that there is a known counterexample to the converse of the implication.

Some remarks:

- Unirational varieties of dimension 1 are rational. Separably unirational varieties of dimension 2 are rational. In higher dimensions, unirational does not imply rational, even over $\mathbb{C}$. In fact, there are several invariants that can be used to prove non-rationality:
  - Intermediate Jacobian: Every smooth cubic 3-fold $X$ in $\mathbb{P}^4$ is unirational, but Clemens and Griffiths proved that $X$ is never rational. They proved that the intermediate Jacobian $J^3(Y)$ of a rational 3-fold $Y$ is a product of Jacobians of nice curves, but $J^3(X)$ does not have this form [CG72, (0.12)]. Beauville, Colliot-Thélène, Sansuc, and Swinnerton-Dyer constructed a nice 3-fold $X$ that is stably rational but not rational [BCTSSD85]; their non-rationality proof again relied on the intermediate Jacobian.
  - Birational automorphism group: Some (and maybe all) smooth quartic 3-folds $X$ in $\mathbb{P}^4$ are unirational [Seg60, V.19], but Iskovskikh and Manin proved that such $X$ are never rational [IM71]. In fact, they showed that Bir $X$ is isomorphic to Aut $X$, which is finite [MM63, Theorem 2], while Bir $\mathbb{P}^3$ is enormous.
  - Torsion in $H^3(X, \mathbb{Z})$: Artin and Mumford gave the example of a double cover $X$ of $\mathbb{P}^3$ branched along a quartic surface [AM72, §2]. They showed that $X$ is
not rational by showing that $H^3(X, \mathbb{Z})_{\text{tors}}$ is a birational invariant of 3-folds that distinguishes $X$ from $\mathbb{P}^3$ [AM72, Proposition 1]. In fact, for the same reason, $X$ is not even stably rational. The group $H^3(X, \mathbb{Z})_{\text{tors}}$ can also be interpreted as the unramified cohomology group $H^2_{\text{nr}}(X, \mathbb{Q}/\mathbb{Z})$.

Higher unramified cohomology: Colliot-Thélène and Ojanguren constructed a nice 6-fold $X$ such that the unramified cohomology group $H^3_{\text{nr}}(X, \mathbb{Q}/\mathbb{Z})$ is nonzero even though $H^2_{\text{nr}}(X, \mathbb{Q}/\mathbb{Z}) = 0$; the former implies that $X$ is not stably rational [CTO89]. For rationally connected varieties, the group $H^3_{\text{nr}}(X, \mathbb{Q}/\mathbb{Z})$ also measures the failure of the integral Hodge conjecture [CTV12, Théorème 1.1].

- The theorem that Fano varieties in characteristic 0 are rationally connected was proved independently in [Cam92, Corollaire 3.2] and [KMM92a, Theorem 0.1].
- It is expected that there exist Fano varieties (and hence rationally connected varieties) that are not unirational. For instance, smooth hypersurfaces of degree $n$ in $\mathbb{P}^m$ are Fano, but maybe for large $n$ they are not unirational.
- It is easy to construct rationally connected varieties that are not Fano, or even rational varieties that are not Fano. See Remark 9.4.6 for example.
- Mumford conjectured that $X$ is rationally connected if and only if $H^0(X, \Omega_X^m) = 0$ for all $m \geq 1$ [Kol96, Conjecture IV.3.8.1]. This is known for $d \leq 3$ [KMM92b, Theorem 3.2]. (Here $\Omega_X$ is the sheaf of 1-forms, not the canonical sheaf, so $\Omega_X^m$ is a vector bundle of rank $d^m$.)
- If $C$ is a curve of positive genus, then $C \times \mathbb{P}^1$ is uniruled, but not rationally connected, because any rational curve in $C \times \mathbb{P}^1$ maps to a point under the projection to $C$.
- It is conjectured that uniruled is equivalent to $\kappa = -\infty$.

Remark 9.2.25. It is not known whether there exists a single nice hypersurface of degree at least 4 that is rational.

9.2.7. Non-algebraically closed ground fields.

Definition 9.2.26. Let $X$ be a nice variety over an arbitrary field $k$. Call $X$ rational, unirational, separably unirational, ruled, uniruled, separably uniruled, rationally connected, separably rationally connected, or rationally chain connected, if $X_{\overline{k}}$ is.

If we want to say that the property truly holds over $k$, we use the prefix $k$-$. For instance, $X$ is $k$-unirational if there exists a dominant rational map $\mathbb{P}^N_k \dashrightarrow X$ for some $N \geq 0$.

Conjecture 9.2.27 (Colliot-Thélène). Let $X$ be a nice variety over a number field $k$. Suppose that $X$ is rationally connected. Then the Brauer–Manin obstruction to the local-global principle is the only obstruction.

See [PV04, Remark 3.3] for the history of Conjecture 9.2.27.
9.3. Classification of surfaces

9.3.1. Proper birational morphisms.

(References: [Lic68], [Lip69] §27, [Mor82] Chapter 2, Section 3)

9.3.1.1. Terminology. Throughout Section 9.3.1 we use the following terminology. A regular surface is a regular integral separated noetherian scheme \( X \) of dimension 2. A curve in \( X \) is an integral codimension 1 subscheme \( C \subset X \) such that \( C \) is proper over some field \( k \) (the latter condition is automatic if \( X \) itself is proper over \( k \)). The properness assumption is there so that for any divisor \( D \) on \( X \) we may define \( C.D := \deg_k \mathcal{O}_X(D)|_C \) (cf. [Lic68], Section I.1); since there may be more than one possibility for \( k \) given \( C \), we write \( (C.D)_k \) when necessary.

Curves are called skew if they do not intersect. Call a curve \( C \) contractible if there is a proper birational morphism \( f: X \to Y \) to another regular surface such that \( f(C) \) is a closed point \( P \in Y \) and \( f \) restricts to an isomorphism from \( X - C \) to \( Y - \{P\} \). (Some authors relax the regularity requirement on \( Y \) and allow \( Y \) to be only normal at \( P \); see [Lip69] §27.) If \( C \) is contractible, then \( Y, P, \) and \( f \) are uniquely determined up to isomorphism: the key point is that normality forces \( \mathcal{O}_{Y,P} \) to equal \( \bigcap_{x \in C} \mathcal{O}_{X,x} \subseteq k(X) \). Call a curve \( C \) a \((-1)\)-curve if \( C \cong \mathbb{P}_L^1 \) and \( (C.C)_L = -1 \) for some field \( L \); then call \( L = H^0(C, \mathcal{O}_C) \) the constant field of \( C \).

9.3.1.2. Blowing up a regular surface at a closed point. The blow-up of a regular surface \( Y \) at a closed point \( P \) is another regular surface \( X \) with a proper birational morphism \( X \to Y \) [Lic68 II.A.1.5]; in this case, the fiber above \( P \) is a contractible curve \( C \subseteq X \) called the exceptional divisor. Moreover, \( C \) is a \((-1)\)-curve with constant field \( k(P) \) [Lic68] Propositions II.A.2.9 and II.A.2.8.

9.3.1.3. Factorization of birational maps. Any finite composition of blow-ups as above is a birational morphism. Part (a) of the following is a converse.

Theorem 9.3.1 (Factorization of birational morphisms). Let \( f: X \to Y \) be a proper birational morphism between regular surfaces.

(a) The morphism \( f \) factors as a sequence of blow-ups at closed points.

(b) If moreover \( X \) is smooth over a field \( k \) and \( f \) is a \( k \)-morphism, then

(i) \( Y \) is smooth over \( k \), and

(ii) each point \( P \) blown up in (a) is such that \( k(P)/k \) is separable.

Proof.

(a) See [Lic68], Theorem 1.15.

(b) (This proof is loosely inspired by [Coo88].) By working our way down the sequence of blow-ups, it suffices to handle the case in which \( X = \text{Bl}_P Y \) for some regular surface \( Y \) and closed point \( P \in Y \).

(ii) Factor \( |k(P)/k| \) as \( si \), where \( s \) is the separable degree, and \( i \) is the inseparable degree. By Section 9.3.1.2, the exceptional divisor \( C \subset X \) is isomorphic to \( \mathbb{P}^1_{k(P)} \).
and satisfies $C.C = \left[ k(P) : k \right] (C.C)_{k(P)} = -\left[ k(P) : k \right] = -si$. On the other hand, since $k(P) \otimes_k k$ is a product of $s$ local rings each of length $i$ over itself, the pullback of $C$ to a divisor on $X_k$ equals $\sum_{j=1}^{s} iD_j$ for some skew integral divisors $D_j \in X_k$ conjugate to each other; thus $C.C = \sum_{j=1}^{s} (iD_j) = si^2 D_1. D_1$. So $si^2$ divides $-si$. Hence $i = 1$; i.e., $k(P)/k$ is separable.

(i) By Proposition 3.5.22[iii], $Y$ is smooth at $P$. On the other hand, $Y - \{P\}$ is isomorphic to an open subscheme of the smooth scheme $Bl_P Y$, so $Y - \{P\}$ is smooth. Hence $Y$ is smooth. $\square$

**Theorem 9.3.2 (Factorization of birational maps).** Let $\phi: X \dashrightarrow Y$ be a birational map between regular proper surfaces over a field $k$.

(a) There exists a regular surface $Z$ with proper birational morphisms $f$ and $g$ forming a commutative diagram of rational maps

$$
\begin{array}{ccc}
Z & \xrightarrow{f} & X \\
g & \searrow & \phi \\
 & X & \dashrightarrow & Y \\
\end{array}
$$

(b) The rational map $\phi$ factors into blow-ups at closed points and inverses of such blow-ups.

**Proof.**

(a) This is a consequence of [Lip69, Theorem 26.1].

(b) Combine [a] with Theorem 9.3.1[a]. $\square$

**9.3.1.4. Criteria for contractibility.** One would like an intrinsic criterion for contractibility of a curve $C \subset X$, instead of a criterion involving an unspecified proper birational morphism to some unspecified $Y$. For smooth projective varieties $X$ over an algebraically closed field, Castelnuovo gave the following criterion: $C$ is contractible if and only if $C \cong \mathbb{P}^1_k$ and $C.C = -1$ [Har77, Theorem V.5.7]. Here is the generalization to regular surfaces.

**Theorem 9.3.3 (Criteria for contractibility).** Let $X$ be a regular surface that is proper over a noetherian ring $A$. For a curve $C \subset X$ mapping to a point in $\text{Spec} A$, the following are equivalent.

(i) $C$ is contractible.

(ii) There is a regular surface $Y$ proper over $A$, a closed point $P \in Y$, and an $A$-isomorphism $X \cong \text{Bl}_P Y$ sending $C$ to the exceptional divisor.

(iii) $C$ is a $(-1)$-curve.

If $X$ is a nice surface over a field $A = k$, with canonical divisor $K$, then additional equivalent criteria may be given:

(iv) $C.C < 0$ and $C.K < 0$. 

245
(v) \( C_{k_s} = \bigcup_{i=1}^n E_i \) for some \( \text{Gal}(k_s/k) \)-orbit \( \{E_1, \ldots, E_n\} \) of skew \((-1)\)-curves on \( X_{k_s} \) with constant field \( k_s \). In this case, \( C.C = -n \), \( C.K = -n \), and \( C \) is geometrically reduced.

**Proof.**

\[ (i) \Rightarrow (ii) \]: The proper birational morphism contracting \( C \) factors into blow-up morphisms, by Theorem 9.3.1. Since \( C \) is integral, there can be only one blow-up.

\[ (ii) \Rightarrow (iii) \]: This was mentioned already in Section 9.3.1.2.

\[ (iii) \Rightarrow (i) \]: (This is the difficult part.) The morphism \( X \to \text{Spec} \ A \) is projective ([Lip69, Corollary 27.2]), so this is a special case of [Lip69, Theorem 27.1].

From now on, \( X \) is a nice surface over a field \( k \).

\[ (ii) \Rightarrow (v) \]: By Theorem 9.3.1, \( X \simeq \text{Bl}_P Y \) for some nice \( Y \) and closed point \( P \in Y \) with \( k(P)/k \) separable. Then \( X_{k_s} \) is the blow-up of \( Y_{k_s} \) along the subscheme \( P_{k_s} \), which consists of a \( \text{Gal}(k_s/k) \)-orbit in \( Y(k_s) \), so \( C_{k_s} \) is as described. We can compute \( C.C \) and \( C.K \) after base extension to \( k_s \): since \( E_i.E_j = 0 \) for \( i \neq j \), all the quantities are the sum of the quantities for the individual \( E_i \). We have \( E_i.E_i = -1 \) and \( E_i.K = -1 \) (see Exercise 9.3), so the results follow. Finally, \( C_{\overline{k}} \) is a disjoint union of copies of \( \mathbb{P}^1_{\overline{k}} \), so \( C \) is geometrically reduced.

\[ (v) \Rightarrow (iv) \]: We have \(-n < 0\).

\[ (iv) \Rightarrow (i) \]: See the proof of [Mor82, Theorem 2.7]. \( \square \)

**Corollary 9.3.4.** Let \( X \) be a nice surface over a field \( k \). Every \((-1)\)-curve on \( X_{\overline{k}} \) is definable over \( k_s \), i.e., is the base extension of a \((-1)\)-curve on \( X_{k_s} \) with constant field \( k_s \).

**Proof.** We may assume that \( k \) is separably closed. Let \( D \) be a \((-1)\)-curve on \( X_{\overline{k}} \). Let \( C \) be its image under \( X_{\overline{k}} \to X_{k_s} \). As divisors on \( X_{\overline{k}} \), we have \( C_{\overline{k}} = qD \) for some \( q \geq 1 \). Thus \( C.C < 0 \) and \( C.K < 0 \). By \( (iv) \Rightarrow (v) \) in Theorem 9.3.3, \( C \) is a \((-1)\)-curve with constant field \( k_s \), and \( C \) is geometrically reduced, so \( C_{\overline{k}} = D \). \( \square \)

For more general contractibility criteria, including the case of blowing down entire configurations of curves at once, see [Art62, Theorems 2.3, 2.7, and 2.9], [Art66, Corollary 7], and [Lip69, Theorem 27.1].

**9.3.1.5. Minimal surfaces.**

**Definition 9.3.5.** Let \( X \) be a regular surface. Call \( X \) relatively minimal if every proper birational morphism from \( X \) to another regular surface is an isomorphism. If in addition, every birational map from a regular surface \( Y \) to \( X \) is a morphism, call \( X \) minimal.

**Proposition 9.3.6.** A regular surface \( X \) is relatively minimal if and only if it does not contain a curve \( C \) satisfying one of the equivalent conditions of Theorem 9.3.3. In particular, a nice surface \( X \) over a field \( k \) is relatively minimal if and only if \( X_{k_s} \) does not contain a \( \text{Gal}(k_s/k) \)-orbit of skew \((-1)\)-curves with constant field \( k_s \).
Corollary 9.3.7. Relative minimality is unchanged by inseparable extension of the base field.

Warning 9.3.8. Relative minimality can be lost under separable extension of the base field. It can happen that $X_{k_s}$ contains $(-1)$-curves but that each such curve intersects one of its other Galois conjugates.

Theorem 9.3.9 (Existence of relatively minimal models). Let $X$ be a nice surface over a field $k$. Then there exists a proper birational morphism from $X$ to some relatively minimal surface.

Proof. If not, then one could iteratively blow down orbits of $(-1)$-curves on $X_{k_s}$ as in Theorem 9.3.3(v) forever. But then one could do the same over $\bar{k}$, which is impossible by the proof of [Har77, Theorem V.5.8]. □

Warning 9.3.10. There can exist more than one relatively minimal surface in a birational equivalence class, as the following example shows.

Example 9.3.11. The obvious isomorphism $\mathbb{A}^1 \times \mathbb{A}^1 \rightarrow \mathbb{A}^2$ defines a birational map $\mathbb{P}^1 \times \mathbb{P}^1 \rightarrow \mathbb{P}^2$ indeterminate only at $P := (\infty, \infty)$. The indeterminacy can be resolved by blowing up $P$ on $\mathbb{P}^1 \times \mathbb{P}^1$ to produce a surface $X$ fitting in a diagram

$$
\begin{array}{c}
\mathbb{P}^1 \times \mathbb{P}^1 \\
X \\
\mathbb{P}^2.
\end{array}
$$

More explicitly, the strict transforms of $\mathbb{P}^1 \times \{\infty\}$ and $\{\infty\} \times \mathbb{P}^1$ are skew $(-1)$-curves in $X$, and blowing them down produces $\mathbb{P}^2$. Both $\mathbb{P}^1 \times \mathbb{P}^1$ and $\mathbb{P}^2$ are relatively minimal, but not minimal.

On the other hand, we have the following.

Proposition 9.3.12 (Uniqueness of minimal models). If $X_1$ and $X_2$ are minimal regular surfaces in the same birational equivalence class, then they are isomorphic.

Proof. The inverse rational maps $X_1 \rightarrow X_2$ and $X_2 \rightarrow X_1$ extend to morphisms whose composition in either order is the identity. □

9.3.1.6. Fibered surfaces. There is a variant of the theory of minimal surfaces in which everything is fibered over a noetherian scheme $S$. To obtain this variant, change “regular surface” to “regular surface equipped with a proper morphism to $S$”, and change “proper
birational morphism” to “proper birational $S$-morphism” everywhere; this also changes the
notions of relatively minimal and minimal. Then in Theorem $9.3.3$ consider only curves $C$
that map to a closed point in $S$.

A key setting is the one in which $S$ is the spectrum of a discrete valuation ring, or more
generally an integral separated Dedekind scheme. If $Z$ is a nice curve of genus $g \geq 1$ (or more
generally, a regular proper integral curve of positive arithmetic genus) over the function field
of such an $S$, then among regular surfaces proper over $S$ with generic fiber $Z$, there exists a
minimal one: this is a consequence of $[\text{Lic68},$ Theorem $4.4]$. It is unique by Proposition $9.3.12$
and is called the minimal regular proper model of $Z$. See also $[\text{Chi86}]$.

9.3.2. Surfaces over algebraically closed fields. 

(Reference: $[\text{Mor82},$ Chapter $2]$)

**Definition** $9.3.13$. Let $X$ be a nice variety over a field. Let $D$ be a divisor on $X$. Then

(i) $D$ is numerically equivalent to $0$ if $D.C = 0$ for all closed integral curves $C$ on $X$.

(ii) $D$ is nef (numerically effective) if $D.C \geq 0$ for all closed integral curves $C$ on $X$.

The same terminology applies to the line bundle associated to $D$.

**Theorem** $9.3.14$ (Minimal models of surfaces). Let $k$ be an algebraically closed field. Let $X$
be a relatively minimal nice surface over $k$, with canonical divisor $K$. Then exactly one of
the following holds:

(i) $X$ is rational or ruled (in which case $\kappa(X) = -\infty$), or

(ii) $K$ is nef (in which case $\kappa(X) \in \{0, 1, 2\}$). In this case, $X$ is minimal.

**Proof.** See $[\text{Mor82},$ Corollary $2.2$ and Lemma $2.4]$.

A more refined classification is possible. For the rest of Section $9.3.2$ we assume that
$k$ is algebraically closed and $X$ is a relatively minimal nice surface over $k$. First, one can
subdivide according to the Kodaira dimension $\kappa := \kappa(X)$:

9.3.2.1. $\kappa = -\infty$. Rational surfaces: The only Hirzebruch surface $F_n$ that contains a
$(-1)$-curve is $F_1$, which is isomorphic to the blow-up of $\mathbb{P}^2$ at a point. Therefore the rational
surfaces

$F_0, \mathbb{P}^2, F_2, F_3, \ldots$

are all relatively minimal. One can show that every rational relatively minimal surface is
isomorphic to one of these.

**Example** $9.3.15$. We have $F_0 \simeq \mathbb{P}^1 \times \mathbb{P}^1$.

Ruled surfaces: Given a nice curve $C$ and a rank 2 vector bundle $E$ on $C$, the ruled
surface $\mathbb{P}E \to C$ is relatively minimal. Every ruled relatively minimal surface is isomorphic
to one of these.
9.3.2.2. $\kappa = 0$. The minimal surfaces of Kodaira dimension 0 are the abelian surfaces (2-dimensional abelian varieties), K3 surfaces (nice surfaces $X$ with $H^1(X, \mathcal{O}_X) = 0$ and $K = 0$), and quotients of these by a finite group scheme acting freely. A quotient that one obtains that is not an abelian surface or a K3 surface is of one of two types:

- a bielliptic surface: see Definition 8.6.2
- an Enriques surface: quotient of a K3 surface by a group scheme of order 2.

Example 9.3.16. If $G$ is a finite subgroup scheme of an abelian surface $A$ acting by translation on $A$, then $A/G$ is another abelian surface, with an isogeny $A \to A/G$.

Example 9.3.17 (Bielliptic surface). Let $E_1$ and $E_2$ be elliptic curves. Let $t \in E_1(k)$ be of order exactly 2. Let $G = \mathbb{Z}/2\mathbb{Z}$ act on $E_1 \times E_2$ by the action of $G$. Then $X$ is a bielliptic surface. If $X$ were an abelian surface, then the morphism $E_1 \times E_2 \to X$ would be a homomorphism up to translation, so its geometric fibers, the $G$-orbits in $(E_1 \times E_2)(k)$, would all be cosets of one subgroup, but they are not. If $X$ were a K3 surface, it would be algebraically simply connected, but $X$ has $E_1 \times E_2$ as a nontrivial connected finite étale cover.

9.3.2.3. $\kappa = 1$. All surfaces with $\kappa = 1$ are elliptic surfaces, surfaces fibered over a curve $C$ such that all but finitely many fibers are of genus 1, except that if $k$ is of characteristic 2 or 3, there are also quasi-elliptic surfaces, which are fibered into singular curves of arithmetic genus 1. But not all elliptic (or quasi-elliptic) surfaces $X$ have $\kappa = 1$; in general all one can say is $\kappa \in \{-\infty, 0, 1\}$. If the base curve $C$ is of genus at least 2, then $\kappa = 1$ is guaranteed, but if $C$ has genus 0 or 1, then one needs to know more about $X$ to determine $\kappa$.

9.3.2.4. $\kappa = 2$. These are, by definition, surfaces of general type. As a warmup, recall that curves of general type can be classified by their genus $g \in \{2, 3, \ldots\}$, and for each $g$, there is a quasi-projective variety $M_g$ whose $k$-points correspond to the isomorphism classes of genus $g$ curves. There is an analogue for surfaces, in which $g$ is replaced by a pair of integers $(e, K^2)$. Here $e$ is the topological Euler characteristic, defined by

$$e := \sum_{i=0}^{4} (-1)^i \dim H^i_{\text{Betti}}(X, \mathbb{Q})$$

if $k = \mathbb{C}$, or by

$$e := \sum_{i=0}^{4} (-1)^i \dim H^i_{\text{et}}(X, \mathbb{Q}_\ell)$$

if $k$ is an arbitrary algebraically closed field, where $\ell$ is a prime chosen so that $\ell \neq \text{char } k$. And $K^2$ is the self-intersection of a canonical divisor. It is not known what the range of possibilities for $(e, K^2)$ is, but for fixed $(e, K^2)$, the general type minimal surfaces over $\mathbb{C}$ are parametrized by a coarse moduli space that is a quasi-projective variety [Gie77].

249
Definition 9.3.18. Let \( k \) be an algebraically closed field. A nice \( k \)-variety \( X \) of arbitrary dimension is called a **minimal model** if \( K \) is nef. When \( \dim X = 2 \), this coincides with the notion of minimal surface given in Definition 9.3.5, because of Theorem 9.3.14 and the multiple examples of relatively minimal rational and ruled surfaces.

9.3.3. Surfaces over arbitrary fields.

(Reference: [Mor82, Chapter 2, Section 3])

Definition 9.3.19. Let \( X \) be a nice surface over a field \( k \). The group \( \text{Num} X \) is the quotient of \( \text{Pic} X \) by the subgroup of classes of line bundles numerically equivalent to 0. We have \( \text{Num} X \cong \mathbb{Z}^\rho \) for some \( \rho \geq 1 \) called the **Picard number** of \( X \).

\[ \text{Warning 9.3.20.} \] The Picard number is unchanged by inseparable extension of the base field, but it can grow under separable extension. For example, let \( X = \text{Res}_{\mathbb{C}/\mathbb{R}} \mathbb{P}^1 \). Then \( X_C \cong \mathbb{P}^1_C \times \mathbb{P}^1_C \), so \( \text{Pic} X_C \cong \mathbb{Z}^2 \), but complex conjugation interchanges the coordinates, so by Exercise 6.10b \( \text{Pic} X \) is isomorphic to the diagonal copy of \( \mathbb{Z} \) in \( \mathbb{Z}^2 \). Thus \( \rho(X) = 1 \) and \( \rho(X_C) = 2 \).

The following builds on the work of many people, including Castelnuovo, Enriques, Manin, Iskovskikh, and Mori.

Theorem 9.3.21. Let \( k \) be a field. Let \( X \) be a nice \( k \)-surface, and let \( K \) be a canonical divisor. Then at least one of the following properties holds:

(i) \( X \) is not relatively minimal (see Proposition 9.3.6).

(ii) \( \rho = 1 \) and \( -K \) is ample.

(iii) \( \rho = 2 \) and \( X \) is a conic bundle over a nice \( k \)-curve \( Y \) such that for every \( y \in Y \), the fiber \( X_y \) is isomorphic to an irreducible and geometrically reduced \( k(y) \)-curve of degree 2 in \( \mathbb{P}^2_{k(y)} \) (i.e., each geometric fiber is either a smooth conic, or a union of two intersecting lines defined over a separable quadratic extension, each a Galois conjugate of the other).

(iv) \( K \) is nef.

Moreover, these four classes of varieties are pairwise disjoint, except that some surfaces satisfy both (i) and (iii).

Proof. See [Mor82, Theorem 2.7]. For the classification of surfaces satisfying both (i) and (iii), see [Isk79, Theorem 4].

Corollary 9.3.22.

(a) A rational surface over \( k \) is birational (over \( k \)) to either a del Pezzo surface (see Section 9.4) or a conic bundle over a conic.

(b) A ruled surface over \( k \) is birational to a conic bundle over a nice \( k \)-curve.
Remark 9.3.23. The arithmetic of del Pezzo surfaces will be discussed in detail in Section 9.4. For the arithmetic of conic bundles, see Chapter 7.

Corollary 9.3.24. Let $k$ be a separably closed field.
(a) The relatively minimal rational surfaces over $k$ are $\mathbb{P}^2$ and the Hirzebruch surfaces $F_n$ for $n \in \{0\} \cup \{2, 3, \ldots\}$.
(b) The relatively minimal ruled surfaces over $k$ with base of positive genus are the surfaces $\mathbb{P}E \to Y$ where $Y$ is a nice $k$-curve of positive genus and $E$ is a rank 2 vector bundle on $Y$.

Proof. In Theorem 9.3.21, we are in case (ii) or (iii). If (ii), then $X_k \cong \mathbb{P}^2$, so $X \cong \mathbb{P}^2$ by Remark 4.5.9.
If (iii), then the conic bundle $X$ corresponds to an element of $H^1(Y, \text{PGL}_2) \hookrightarrow H^2(Y, \mathbb{G}_m) = \text{Br} Y$, but the latter is trivial by Theorem 6.9.7. Thus $X \cong \mathbb{P}E$ for some rank 2 vector bundle $E$ on $Y$. Finally, if $Y$ itself is a conic, then $Y \cong \mathbb{P}^1$ (Remark 4.5.9 again), and the classification of vector bundles on $\mathbb{P}^1$ shows that $E \cong \mathcal{O} \oplus \mathcal{O}(n)$ for some $n \geq 0$. Finally, $\mathbb{P}E$ is relatively minimal if and only if $(\mathbb{P}E)_K$ is relatively minimal, which holds if and only if $n \neq 1$. □

Proposition 9.3.25 (Wei56). Let $k$ be a finite field $\mathbb{F}_q$. Let $X$ be a nice rational surface over $k$. Then
\[ \#X(k) = q^2 + (\text{tr Frob}_q | \text{Pic} X_k)q + 1, \]
and $X$ has a $k$-point.

Proof. Apply Proposition 9.2.6 to $X_K$, and then use the Lefschetz trace formula to obtain the formula. Since $\text{tr Frob}_q | \text{Pic} X_K \in \mathbb{Z}$, we obtain $\#X(k) \equiv 1 \pmod{q}$, so $X(k) \neq \emptyset$. □

Remark 9.3.26. As mentioned in (3) in Section 1.2.4 the final conclusion of Proposition 9.3.25 generalizes to rationally chain connected nice varieties Esn03, Corollary 1.3.

9.4. Del Pezzo surfaces

(Reference: Kol96, III.3)

Recall from Section 9.2.5 that a Fano variety is a nice variety for which $-K$ (an anticanonical divisor) is ample.

Definition 9.4.1. A del Pezzo surface is a (nice) Fano variety of dimension 2.

Let $X$ be a del Pezzo surface. According to the definition for Fano varieties in Section 9.2.5, the degree of $X$ is the positive integer $d := (-K).(-K) = K.K$. It then turns out that $\dim H^0(X, -K) = d + 1$ [Kol96 Corollary III.2.3.5.2] and $-K$ is very ample when $d \geq 3$ [Kol96 Proposition III.3.4.3]. Thus, if $d \geq 3$, then $|-K|$ embeds $X$ as a degree $d$ surface in $\mathbb{P}^d$. 251
9.4.1. Del Pezzo surfaces over a separably closed field.

**Lemma 9.4.2.** Let $k$ be a separably closed field. Let $X$ be a del Pezzo surface over $k$. If $C$ is a closed integral curve on $X$ with $C.C < 0$, then $C$ is a $(-1)$-curve with constant field $k$.

**Proof.** Since $-K$ is ample, $C.(-K) > 0$. Theorem 9.3.3(iv) implies that $C$ is a $(-1)$-curve with constant field $k$. □

**Definition 9.4.3.** Let $0 \leq r \leq 8$. Points $P_1, \ldots, P_r \in \mathbb{P}^2(k)$ are in *general position* if they are distinct and *none* of the following hold:

(i) Three of the $P_i$ lie on a line.

(ii) Six of the $P_i$ lie on a conic.

(iii) Eight of the $P_i$ lie on a singular cubic, with one of these eight points at the singularity.

**Theorem 9.4.4** (Classification of del Pezzo surfaces). Let $k$ be a separably closed field. Let $X$ be a del Pezzo surface over $k$. Then exactly one of the following holds:

- $X \simeq \mathbb{P}^1 \times \mathbb{P}^1$; then deg $X = 8$.
- There exists $r$ with $0 \leq r \leq 8$ such that $X$ is the blow-up of $\mathbb{P}^2$ at $r$ $k$-points in general position; then deg $X = 9 - r \in \{1, 2, \ldots, 9\}$.

**Proof.** Let $X \to Y$ be a proper birational morphism to a relatively minimal surface $Y$. By Corollary 9.3.24, $Y \simeq \mathbb{P}^2$ or $Y \simeq F_n$ for some $n \in \{0\} \cup \mathbb{Z}_{\geq 2}$. A section of $F_n \to \mathbb{P}^1$ has self-intersection $-n$ ([Har77 Proposition V.2.9]), and its strict transform in $X$ would have self-intersection at least as negative, which contradicts Lemma 9.4.2 if $n \geq 2$. Thus $Y \simeq \mathbb{P}^2$ or $Y \simeq \mathbb{P}^1 \times \mathbb{P}^1$. By Theorem 9.3.1(b), $X$ is obtained from $Y$ by iteratively blowing up $k$-points. The blow-up of $\mathbb{P}^1 \times \mathbb{P}^1$ at a $k$-point is isomorphic to the blow-up of $\mathbb{P}^2$ at two $k$-points (Example 9.3.11), so we need only consider blow-ups of $\mathbb{P}^2$. If we ever blow up a point on an exceptional curve from a previous blow-up, the strict transform $C$ of that exceptional curve in $X$ would satisfy $C.C < -1$, contradicting Lemma 9.4.2. Thus $X$ is the blow-up of $\mathbb{P}^2$ at a finite subset $\{P_1, \ldots, P_r\}$ of $X(k)$. Since $-K$ is ample, $0 < (-K).(-K) = K.K = 9 - r$ (the last equality follows from [Har77 Proposition V.3.3]), so $r \leq 8$. If three of the $P_i$ were on a line, the strict transform $C$ of that line would satisfy $C.C \leq 1 - 3 \leq -2$, contradicting Lemma 9.4.2. The other restrictions on the $P_i$ are similarly derived; see [Dem80 Théorème 1(i)⇒(iii)]. □

**Remark 9.4.5.** If $X$ is as in Theorem 9.4.4 then Pic $X \simeq \mathbb{Z}^{10-d}$: this is true when $X$ is $\mathbb{P}^2$ or $\mathbb{P}^1 \times \mathbb{P}^1$, and blowing up a $k$-point adds a new factor of $\mathbb{Z}$ [Har77 Proposition V.3.2]. One can also describe the canonical class and the intersection pairing on Pic $X$ explicitly with respect to a suitable basis [Man86 Theorem 23.8].

**Remark 9.4.6.** If $r \geq 9$ and $X$ is the blow-up of $\mathbb{P}^2$ at any $r$ points, then $K.K = 9 - r \leq 0$, so $X$ can not be a del Pezzo surface. This shows that the property of being a del Pezzo surface is not invariant under birational maps.
Proposition 9.4.7 (Exceptional curves on a del Pezzo surface). Let \( k \) be a separably closed field. Let \( X \to \mathbb{P}^2 \) be the blow-up of points \( x_1, \ldots, x_r \) in general position, where \( 0 \leq r \leq 8 \). Then the exceptional curves are the fibers above the \( x_i \) together with the strict transforms of the following curves in \( \mathbb{P}^2 \):

(i) a line through 2 of the \( x_i \),
(ii) a conic through 5 of the \( x_i \),
(iii) a cubic passing through 7 of the \( x_i \) such that one of them is a double point (on the cubic),
(iv) a quartic passing through 8 of the \( x_i \) such that three of them are double points,
(v) a quintic passing through 8 of the \( x_i \) such that six of them are double points, and one of them is a triple point.

Proof. See [Man86] Theorem 26.2. \( \square \)

9.4.2. Del Pezzo surfaces over an arbitrary field. The proof of the following will be scattered over the next few subsections within Section 9.4.

Theorem 9.4.8. Let \( k \) be a field. Let \( X \) be a del Pezzo surface over \( k \) of degree \( d \geq 5 \).

(i) If \( d = 7 \) or 5, then \( X \) has a \( k \)-point.
(ii) If \( \dim k \leq 1 \), then \( X \) has a \( k \)-point.
(iii) If \( X \) has a \( k \)-point, then \( X \) is birational to \( \mathbb{P}^2_k \).
(iv) If \( X \) has a \( k \)-point and \( k \) is infinite, then \( X(k) \) is Zariski dense in \( X \).
(v) The homomorphism \( \text{Br} k \to \text{Br} X \) is surjective.
(vi) If \( k \) is a global field, then \( X \) satisfies the local-global principle.
(vii) If \( k \) is a global field, then \( X \) satisfies weak approximation.

Part (iii) implies (iv). To prove (v), check that for every possible \( \mathfrak{G}_k \)-action on \( \text{Pic} X_k_s \cong \mathbb{Z}^{10-d} \) respecting the intersection pairing, \( H^1(\mathfrak{G}_k, \text{Pic} X_k_s) = 0 \); then use Corollaries 6.7.8 and 6.9.11. Parts (vi) and (iii) imply (vii).

Remark 9.4.9. In the case where \( k \) is finite, Proposition 9.3.25 proves (ii) even without the restriction \( d \geq 5 \).

Remark 9.4.10. When \( d \leq 4 \), most parts of Theorem 9.4.8 can fail. Part (i) holds for \( d = 1 \) but can fail for \( d = 2, 3, 4 \). Part (iii) can fail for \( d = 2, 3, 4 \) [CTM04]. The birational invariant \( H^1(\mathfrak{G}_k, \text{Pic} X_k_s) \) (see Exercise 9.5) is 0 for \( \mathbb{P}^2_k \), but can be nonzero for a degree \( d \) del Pezzo surface over a global field if \( d \leq 4 \); thus (iii) can fail for each \( d \leq 4 \). For such an example, Corollaries 6.7.8 and 6.9.11 shows that \( \text{Br} k \to \text{Br} X \) will fail to be surjective; that is, (v) fails. This means that there is potentially a Brauer–Manin obstruction to the
local-global principle and/or weak approximation, and in fact (vi) can fail for \( d = 2, 3, 4 \) and (vii) can fail for \( d = 1, 2, 3, 4 \), as will be discussed below.

**Remark 9.4.11 (Unirationality of del Pezzo surfaces).** It may be that every del Pezzo surface over \( k \) with a \( k \)-point is \( k \)-unirational. This has already been proved for all \( d \geq 3 \) [Seg43, Seg51, Man86, Theorems 29.4 and 30.1; Kol02, Theorem 1.1; Pie12, Proposition 5.19; Kne15, Theorem 2.1], and also under additional hypotheses for \( d = 2 \) and \( d = 1 \) [Man86, Theorems 29.4; STVA14, Theorems 1.1 and 3.2; FvL16, Theorem 1.1; KM16, Corollary 38]. For each surface for which this holds, part (iv) of Theorem 9.4.8 holds too.

**9.4.3. Degree 9.** Then \( X_k \simeq \mathbb{P}^2_k \), so \( X \) is a Severi–Brauer surface. In particular:
- If \( X \) has a \( k \)-point, then \( X \simeq \mathbb{P}^2_k \) (Proposition 4.5.10).
- If \( \dim k \leq 1 \), then \( X \simeq \mathbb{P}^2_k \).
- If \( k \) is a global field, then \( X \) satisfies the local-global principle (Theorem 4.5.11).

**9.4.4. Degree 8.**

**Proposition 9.4.12.** Let \( X \) be a degree 8 del Pezzo surface over a field \( k \). Then exactly one of the following holds:
1. There is a degree 2 étale extension \( L/k \) and a nice conic \( C \) over \( L \) such that \( X \) is isomorphic to the restriction of scalars \( \text{Res}_{L/k} C \). (In the split case \( L = k \times k \), this means simply that \( X \) is a product of two nice conics over \( k \).)
2. \( X \) is the blow-up of \( \mathbb{P}^2_k \) at a \( k \)-point.

**Proof.** By Theorem 9.4.4 either \( X_k \simeq (\mathbb{P}^1 \times \mathbb{P}^1)_k \) or \( X_k \) is the blow-up of \( \mathbb{P}^2_k \) at a \( k \)-point.

(1) Suppose that \( X_k \simeq (\mathbb{P}^1 \times \mathbb{P}^1)_k \); i.e., \( X \) is a twist of \( \mathbb{P}^1 \times \mathbb{P}^1 \). To understand the twists, we need to compute \( \text{Aut}((\mathbb{P}^1 \times \mathbb{P}^1)_k) \). First, \( \text{Aut} \mathbb{P}^1_k \simeq \text{PGL}_2(k) \) (see Har77, Example II.7.1.1). Let \( A \leq \text{Aut}((\mathbb{P}^1 \times \mathbb{P}^1)_k) \) be the subgroup generated by the action of \( \text{PGL}_2(k) \) on each factor and the involution that interchanges the two factors. Let \( S \) and \( I \) be the kernel and image of the homomorphism

\[
\text{Aut}((\mathbb{P}^1 \times \mathbb{P}^1)_k) \rightarrow \text{Aut}((\mathbb{P}^1 \times \mathbb{P}^1)_k)
\]

describing the action of automorphisms on the Picard group, which is \( \mathbb{Z} \times \mathbb{Z} \) (see Har77, Example II.6.6.1 and Corollary II.6.16]). We have a commutative diagram

\[
\begin{array}{ccccccccc}
1 & \rightarrow & \text{PGL}_2(k) \times \text{PGL}_2(k) & \rightarrow & A & \rightarrow & \mathbb{Z}/2\mathbb{Z} & \rightarrow & 1 \\
\downarrow & & \downarrow & & \downarrow & & \downarrow & & \\
1 & \rightarrow & S & \rightarrow & \text{Aut}((\mathbb{P}^1 \times \mathbb{P}^1)_k) & \rightarrow & I & \rightarrow & 1
\end{array}
\]
with exact rows. Any automorphism in $S$ induces linear automorphisms of the spaces of global sections of $\mathcal{O}(1, 0)$ and $\mathcal{O}(0, 1)$, and hence is given by an element of $\text{PGL}_2(k_s) \times \text{PGL}_2(k_s)$. In other words, the left vertical homomorphism is an isomorphism. On the other hand, an automorphism of $(\mathbb{P}^1 \times \mathbb{P}^1)_{k_s}$ acts on the Picard group $\mathbb{Z} \times \mathbb{Z}$ so as to preserve the ample cone, which is the first quadrant, so it can only be the identity or the coordinate-interchanging involution of $\mathbb{Z} \times \mathbb{Z}$. In other words, the right vertical homomorphism is an isomorphism. Thus the middle vertical homomorphism is an isomorphism too.

Taking cohomology of either of the now-identified rows of (9.4.13) yields a map of pointed sets

$$H^1(k, \text{Aut}((\mathbb{P}^1 \times \mathbb{P}^1)_{k_s})) \longrightarrow H^1(k, \mathbb{Z}/2\mathbb{Z}).$$

An element of the latter corresponds to a degree 2 étale extension $L/k$, and its preimage in $H^1(k, \text{Aut}((\mathbb{P}^1 \times \mathbb{P}^1)_{k_s}))$ is in bijection with

$$H^1(k, \text{the } L/k\text{-twist of } \text{PGL}_2 \times \text{PGL}_2) \simeq H^1(L, \text{PGL}_2),$$

the isomorphism arising from a nonabelian analogue of Shapiro’s lemma. The latter set $H^1(L, \text{PGL}_2)$ parametrizes twists of $\mathbb{P}^1$ over $L$, i.e., conics over $L$. Thus twists of $\mathbb{P}^1 \times \mathbb{P}^1$ are parametrized by pairs $(L, C)$ where $L$ is a degree 2 étale extension $L/k$ and $C$ is a nice conic over $L$. By writing out explicit 1-cocycles, one can verify that the twist corresponding to $(L, C)$ is the restriction of scalars $\text{Res}_{L/k} C$.

(2) There is a unique exceptional curve on $X_{k_s}$. It must be Galois invariant, so it descends to a genus 0 curve $E$ over $k$. Blow down $E$ to get a morphism $X \rightarrow Y$, where $Y$ is a Severi–Brauer surface over $k$. The image of $E$ is a $k$-point on $Y$, so $Y \simeq \mathbb{P}^2_k$. Thus $X$ is the blow-up of $\mathbb{P}^2_k$ at a $k$-point. □

**Corollary 9.4.14.** If $\dim k \leq 1$, then any degree 8 del Pezzo surface $X$ over $k$ has a $k$-point.

**Proof.** It suffices to consider Case [1] of Proposition 9.4.12. Since $\dim k \leq 1$, we have $\text{Br} L = 0$. Since $C$ is a 1-dimensional Severi–Brauer variety over $L$, it has an $L$-point. Finally, $X(k) = C(L)$. □

**Corollary 9.4.15.** Let $X$ be a degree 8 del Pezzo surface over a field $k$. If $X$ has a $k$-point, then $X$ is birational to $\mathbb{P}^2_k$.

**Proof.** In Case [2] of Proposition 9.4.12, $X$ is a blow-up of $\mathbb{P}^2_k$, and hence birational to $\mathbb{P}^2_k$. In Case [1], $X$ has the form $\text{Res}_{L/k} C$; if $X$ has a $k$-point, then $C$ has an $L$-point, so $C \simeq \mathbb{P}^1_L$, which is birational to $\mathbb{A}^1_L$, so $X$ is birational to $\text{Res}_{L/k} \mathbb{A}^1_L \simeq \mathbb{A}^2_k$, which is birational to $\mathbb{P}^2_k$. □
Corollary 9.4.16. A degree 8 del Pezzo surface over a global field $k$ satisfies the local-global principle.

Proof. If $X = \text{Res}_{L/k} C$, apply the local-global principle to $C$ over $L$. If $X$ is the blow-up of $\mathbb{P}^2_k$ at a $k$-point, then $X$ has a $k$-point already. \qed

9.4.5. Degree 7.

Proposition 9.4.17. A degree 7 del Pezzo surface $X$ is $\mathbb{P}^2_k$ blown up at either two $k$-points or at a closed point whose residue field is separable of degree 2 over $k$.

Proof. There are three exceptional curves on $X_k$, arranged in a chain, say $E_1, E_2, E_3$ in order. The middle one $E_2$ is Galois-stable, so $E_2$ descends to a nice genus 0 curve over $k$. Blowing down $E_2$ yields a nice surface $Y$ with a $k$-point. Blowing down $E_1$ and $E_3$ together instead yields a Severi–Brauer variety $Z$ over $k$. Since $Z$ is birational to $Y$, it has a $k$-point too, so $Z \simeq \mathbb{P}^2_k$. The image of $E_1 \cup E_3$ in $Z \simeq \mathbb{P}^2_k$ is what must be blown up to recover $X$. \qed

9.4.6. Degree 6.

Lemma 9.4.18. Let $X$ be a degree 6 del Pezzo surface over a field $k$. If there exist separable extensions $K$ and $L$ with $[K : k] = 2$ and $[L : k] = 3$ such that $X$ has a $K$-point and an $L$-point, then $X$ has a $k$-point.

Proof. Consider the anticanonical embedding $X \subseteq \mathbb{P}^6$. If the $K$-point or $L$-point is defined over $k$, we are done. Otherwise the conjugates of the two points give 5 geometric points on $X$. If these 5 points are sufficiently generic on $X$, then the 4-dimensional linear subspace of $\mathbb{P}^6$ passing through them intersects $X$ in a 0-cycle of degree 6, of which 5 points are accounted for, and the remaining point is $G_k$-stable, hence a $k$-point. One can remove the genericity hypothesis by invoking the Lang–Nishimura theorem (Theorem 3.6.11): the construction above defines a rational map $\text{Sym}^2 X \times \text{Sym}^3 X \to X$, and the hypothesis supplies a $k$-point on the smooth source, so the target has a $k$-point. \qed

There are six exceptional curves on $X_k$, forming a hexagon. Label them $E_1, \ldots, E_6$ in order around the hexagon.

Proposition 9.4.19. Let $X$ be a degree 6 del Pezzo surface over a field $k$. If either $\dim k \leq 1$, or $k$ is a global field and $X(A) \neq \emptyset$, then $X$ has a $k$-point.

Proof. (This is based on [CT72].) Since the action of $G_k$ on $\{E_1, \ldots, E_6\}$ respects intersections, it preserves the partition $\{\{E_1, E_3, E_5\}, \{E_2, E_4, E_6\}\}$. The stabilizer in $G_k$ of $\{E_1, E_3, E_5\}$ is $G_K$ for some separable extension $K$ of degree 1 or 2. Blowing down $E_1, E_3, E_5$ simultaneously on $X_K$ yields a degree 9 del Pezzo surface $Y$. If $\dim k \leq 1$, then $\text{Br} K = 0$, \end{quote}
so $Y \cong \mathbb{P}^2_K$, so $Y$ has a $K$-point. If $k$ is a global field and $X(A) \neq \emptyset$, then $X(A_K) \neq \emptyset$, so $Y(A_K) \neq \emptyset$, so $Y \cong \mathbb{P}^2_K$ by Theorem 4.5.11 (the local-global principle for Severi–Brauer varieties). In either case, $Y$ has a $K$-point, and $X$ is birational to $Y$, so $X$ has a $K$-point.

The same argument using the partition $\{\{E_1, E_4\}, \{E_2, E_5\}, \{E_3, E_6\}\}$ shows that $X$ has an $L$-point for some separable extension $L$ of degree 1 or 3. If either $K$ or $L$ has degree 1, then $X$ has a $k$-point already. Otherwise Lemma 9.4.18 shows that $X$ has a $k$-point. \qed

**Sketch of alternative proof.** Let $U = X - \bigcup_{i=1}^6 E_i$. Then $U_{k_s}$ is $\mathbb{P}^2_{k_s}$ with 3 lines deleted; in other words $U_{k_s} \cong \mathbb{G}^2_m$. One can prove that in general, if $U$ is a variety over a field $k$, and $U_{k_s} \cong \mathbb{G}^n_m$ for some $n \in \mathbb{N}$, then $U$ is a torsor under a torus $T$. If $\dim k \leq 1$, then Theorem 5.12.19(b) shows that $U$ has a $k$-point. Now suppose that $k$ is a global field and $X(A) \neq \emptyset$. For every $v$, Proposition 3.5.74 shows that $X(k_v)$ is Zariski dense in $X$, so $U$ has a $k_v$-point. By Theorem 5.12.32, $U$ has a $k$-point. Hence $X$ has a $k$-point. \qed

**Proposition 9.4.20.** Let $X$ be a degree 6 del Pezzo surface over a field $k$. If $X$ has a $k$-point, then $X$ is birational to $\mathbb{P}^2_k$.

**Proof.** Let $x \in X(k)$.

*Case 1. The point $x$ lies on a unique exceptional curve $E_i$. Then $E_i$ is defined over $k$ and may be blown down, so we reduce to the case of a degree 7 del Pezzo surface.*

*Case 2. The point $x$ lies on the intersection of two exceptional curves.* Suppose that $x \in E_1 \cap E_2$. Then $E_3 \cup E_6$ is $G_k$-stable. Blowing down $E_3$ and $E_6$ simultaneously, we reduce to the case of a degree 8 del Pezzo surface.

*Case 3. The point $x$ does not lie on any exceptional curve.* Make the variety more complicated by blowing up $x$! This yields a degree 5 del Pezzo surface $Y$. Let $D$ be the exceptional divisor for this blow-up. Let $P$ be the dual graph of the 10 exceptional curves, so $P$ has one vertex for each exceptional curve, and one edge for each intersecting pair of exceptional curves. Then $P$ turns out to be the Petersen graph; this shows that there are three exceptional curves on $Y$ meeting $D$, and they are disjoint. Blowing them down let us reduce to the case of a degree 8 del Pezzo surface. \qed

**9.4.7. Degree 5.** Recall the fine moduli space $M_{0,5}$ of Example 2.3.9.

**Lemma 9.4.21.** Let $\mathcal{X}$ be the blow-up of $\mathbb{P}^2$ at the points $(1 : 0 : 0)$, $(0 : 1 : 0)$, $(0 : 0 : 1)$, and $(1 : 1 : 1)$. Then there is an open immersion $M_{0,5} \hookrightarrow \mathcal{X}$, and the $S_5$-action on $M_{0,5}$ extends to an $S_5$-action on $\mathcal{X}$. Moreover, $S_5 \to \text{Aut} \mathcal{X}$ is an isomorphism.

**Proof.** Let $\mathcal{X}'$ be the complement in $\mathcal{X}$ of the 10 exceptional curves, so $\mathcal{X}'$ is the complement in $\mathbb{P}^2$ of the $\binom{4}{2}$ lines through the four blown up points. Then $\mathcal{X}'$ and $M_{0,5}$ are the same open subvariety of $\mathbb{A}^2$! By symmetry, the transposition $(0, 1, \infty, x, y) \mapsto (0, 1, \infty, y, x)$
of $M_{0,5}$ extends to an automorphism of $X$. A calculation shows that the 5-cycle

$$(0, 1, \infty, x, y) \mapsto (y, 0, 1, \infty, x) \sim \left(0, 1, \infty, \frac{1}{y}, \frac{x-y}{y(x-1)}\right)$$

also extends. These generate $S_5$, so $S_5$ acts faithfully on $X$. The dual graph of the set of the exceptional curves is the Petersen graph $P$. We have

(9.4.22) \hspace{1cm} S_5 \hookrightarrow \text{Aut} X \twoheadrightarrow \text{Aut} P \cong S_5.

The homomorphism $\text{Aut} X \to \text{Aut} P$ is injective since an automorphism preserving each of the 10 exceptional curves would act on the blow-down $\mathbb{P}^2$ and would fix the four blown up points, forcing it to be the identity. Thus all the homomorphisms in (9.4.22) are isomorphisms. \hfill \Box

Remark 9.4.23. One can show that $X \supset X'$ is isomorphic to the compactification $\overline{M}_{0,5} \supset M_{0,5}$ of Example 2.3.12. This explains why the $S_5$-action on $M_{0,5}$ extends to $X$.

Lemma 9.4.24. Every degree 5 del Pezzo surface over a field $k$ is dominated by the Grassmannian $\text{Gr}(2, 5)$.

Proof. Let $X$ be the degree 5 del Pezzo surface in Lemma 9.4.21. The group $S_5$ acts on $k^5$ by permuting the coordinates, so it acts on the Grassmannian $\text{Gr}(2, 5)$ defined in Example 9.2.3. Given a general point $[W] \in \text{Gr}(2, 5)$, so $W$ is a 2-dimensional subspace of $k^5$, the intersections of $W$ with the five coordinate hyperplanes are five distinct lines in $W$, and projectivizing yields a point of $M_{0,5}$. This defines the first of the two $S_5$-equivariant rational maps

(9.4.25) \hspace{1cm} \text{Gr}(2, 5) \dashrightarrow M_{0,5} \hookrightarrow X,

and the second map is the open immersion of Lemma 9.4.21. The first map is dominant since given five distinct points in $\mathbb{P}^1$, or equivalently five distinct lines in a 2-dimensional space $W$, one can choose linear functionals $\lambda_1, \ldots, \lambda_5: W \to k$ cutting out these lines, and the image of $(\lambda_1, \ldots, \lambda_5): W \to k^5$ represents a preimage in $\text{Gr}(2, 5)$.

We now twist. Over a separably closed field, there is only one degree 5 del Pezzo surface: see Exercise 9.7. Thus, over $k$, any other one is a twist $X$ of $X$ by a cocycle $\xi$ representing a class in $H^1(k, \text{Aut} X_k) = H^1(k, S_5)$. Twist $k^5$ and (9.4.25) by $\xi$ to obtain a degree 5 étale $k$-algebra $L$ and

(9.4.26) \hspace{1cm} \text{Gr}(2, L) \dashrightarrow M_{0,5}^{(L)} \hookrightarrow X,

where $M_{0,5}^{(L)}$ is as in Example 2.3.11. In $\text{Gr}(2, L)$, the space $L$ is just another 5-dimensional vector space, so $\text{Gr}(2, L) \cong \text{Gr}(2, 5)$. Thus $\text{Gr}(2, 5)$ dominates $X$. \hfill \Box
Remark 9.4.27. Let $X$ be a degree 5 del Pezzo surface. Let $X' \subset X$ be the complement of the 10 exceptional curves. The proof of Lemma 9.4.24 shows that $X' \subset X$ is isomorphic to $M^{(L)}_{0,5} \subset \overline{M}^{(L)}_{0,5}$ for some degree 5 étale $k$-algebra $L$, where $\overline{M}^{(L)}_{0,5}$ is as in 2.3.12.

Corollary 9.4.28. Every degree 5 del Pezzo surface has a $k$-point.

Proof. Combine Lemma 9.4.24 with the Lang–Nishimura theorem (Theorem 3.6.11).

There are many other proofs of Corollary 9.4.28; see [Enr97] (not quite complete), [SD72], [SB92], [Sko93], [Kol96] Exercise III.3.13, and [Has09] Exercise 3.1.4. The proof we gave is closest to that in [Sko93].

Lemma 9.4.24 implies that a degree 5 del Pezzo surface over $k$ is $k$-unirational, but even more is true:

Theorem 9.4.29. Every degree 5 del Pezzo surface over a field $k$ is birational to $\mathbb{P}^2_k$.

Proof. Let $X$ be the del Pezzo surface. Let $X' \subset X$ be the complement of the exceptional curves in $X$.

First suppose that $X'$ has a $k$-point $x$. Then the blow-up of $X$ at $x$ is a degree 4 del Pezzo surface $Y$. There are 16 exceptional curves on $Y$ (over $k$): the strict transforms of the 10 exceptional curves on $X$, the preimage of $x$, and 5 more. Moreover, those last 5 curves are skew, as can be checked over $\overline{k}$: if $Y$ is the blow-up of $\mathbb{P}^2$ at points $x_1, \ldots, x_5$ in general position, and $X$ is the blow-up of $\mathbb{P}^2$ at $x_1, \ldots, x_4$, then the 5 curves are the strict transforms of the conic through $x_1, \ldots, x_5$ and of the four lines connecting each of $x_1, \ldots, x_4$ to $x_5$. Blowing down this $\mathcal{G}$-stable set of 5 skew lines on $Y$ yields a degree 9 del Pezzo surface $Z$ with a $k$-point, so $Z \simeq \mathbb{P}^2_k$.

Now suppose that $X'$ has no $k$-points. The pair $X' \subset X$ is isomorphic to $M^{(L)}_{0,5} \subset \overline{M}^{(L)}_{0,5}$ for some degree 5 étale $k$-algebra $L$. Then $M^{(L)}_{0,5}$ has no $k$-point, so there is no closed immersion $\text{Spec } L \hookrightarrow \mathbb{P}^1_k$. Counting the closed points on $\mathbb{P}^1_k$ with each residue field shows this is possible only in these cases:

(i) $L = k^5$ with $k = \mathbb{F}_2$ or $k = \mathbb{F}_3$; or
(ii) $L = \mathbb{F}_2 \times \mathbb{F}_4 \times \mathbb{F}_4$ with $k = \mathbb{F}_2$.

In Case (i), $X$ is the blow-up of $\mathbb{P}^2_k$ at four $k$-points, so $X$ is birational to $\mathbb{P}^2_k$. In Case (ii), $L \simeq L_3 \times L_2$ for étale algebras $L_3$ of degree 3 and $L_2$ of degree 2. Fix one closed immersion $\iota: \text{Spec } L_3 \to \mathbb{P}^1_k$. Then each $(\text{Aut } \mathbb{P}^1)$-orbit of closed immersions $\text{Spec } L \to \mathbb{P}^1_k$ contains a unique representative whose restriction to $\text{Spec } L_3$ is $\iota$, so $X'$ is isomorphic to the space of closed immersions $\text{Spec } L_2 \to U := \mathbb{P}^1 - \iota(\text{Spec } L_3)$. Thus we have birational equivalences

$$X \sim X' \sim \text{Res}_{L_2/k} U \sim \text{Res}_{L_2/k} \mathbb{A}^1_k \simeq \mathbb{A}^2_k \sim \mathbb{P}^2_k.$$
9.4.8. Degree 4. These $X$ are smooth intersections of two quadrics in $\mathbb{P}^4$ [Kol96, Theorem III.3.5.4]. If $k$ is a global field, then the local-global principle can fail (Exercise 8.3), and weak approximation can fail even if $X$ has a $k$-point [CTS77, III, Exemple (a)].

9.4.9. Degree 3. These are nice cubic surfaces in $\mathbb{P}^3$ [Kol96, Theorem III.3.5.3]. Mordell [Mor49] conjectured that nice cubic surfaces over $\mathbb{Q}$ satisfy the local-global principle, but this turned out to be false [SD62, Section 2]. Selmer [Sel53] proved that diagonal cubic surfaces $ax^3 + by^3 + cz^3 + dw^3 = 0$ in $\mathbb{P}^3_\mathbb{Q}$ for nonzero integers $a, b, c, d$ satisfy the local-global principle if $ab = cd$ or $|abcd| \leq 500$, but later Cassels and Guy [CG66] discovered that the surface

$$5x^3 + 9y^3 + 10z^3 + 12w^3 = 0$$

over $\mathbb{Q}$ violates the local-global principle. Also, weak approximation can fail even if $X$ is minimal and has a $k$-point [SD62, Section 3] (we ask for $X$ to be minimal since otherwise one could simply blow up a $k$-point on a degree 4 counterexample to weak approximation). See [CTKS87] for many more counterexamples.

9.4.10. Degree 2. The anticanonical map is a degree 2 morphism $X \to \mathbb{P}^2$ ramified along a nice curve of degree 4 in $\mathbb{P}^2$ [Kol96, Theorem III.3.5.2]. In other words, $X$ is of degree 4 in a weighted projective space $\mathbb{P}(1,1,2)$. If $k$ is a global field, then $X$ need not satisfy the local-global principle: Kresch and Tschinkel [KT04] give many counterexamples, including the surface over $\mathbb{Q}$ defined by the weighted homogeneous equation

$$w^2 = -6x^4 - 3y^4 + 2z^4.$$

Colliot-Thélène observed that one can obtain a counterexample also by replacing $z^2$ by $z^4$ in Iskovskikh’s surface of Section 8.2.5; this results in the surface

$$y^2 = -z^4 + (3w^2 - x^2)(x^2 - 2w^2)$$

over $\mathbb{Q}$.

Weak approximation can fail too, even if $X$ is minimal and has a $k$-point [KT04].

Remark 9.4.30. So far, every time a del Pezzo surface has been found to violate the local-global principle, the violation has been explained by the Brauer–Manin obstruction, as predicted by Conjecture 9.2.27.

9.4.11. Degree 1. Then $X$ is of degree 6 in a weighted projective space $\mathbb{P}(1,1,2,3)$ [Kol96, Theorem III.3.5.1]. The common zero locus of any basis $s_1, s_2$ of the 2-dimensional space $H^0(X, -K)$ is independent of the choice of basis, and consists of a single degree 1 point since $(-K).(-K) = 1$. In other words, the intersection of any two distinct divisors in $|-K|$ is a canonical $k$-point! Thus $X(k) \neq \emptyset$. 

260
In particular, the local-global principle holds trivially. On the other hand, there can be a Brauer–Manin obstruction to weak approximation, even if $X$ is minimal [VA08, Proposition 7.1].

9.4.12. Summary. The results on the arithmetic of del Pezzo surfaces are summarized in the following table, whose entries answer the following questions about a del Pezzo surface of specified degree over a field $k$:

- **$k$-point**: Must the surface have a $k$-point?
- **$k$-rational†**: If the surface has a $k$-point, must it be birational to $\mathbb{P}^2_k$?
- **$k$-unirational†**: If the surface has a $k$-point, must it be dominated by $\mathbb{P}^2_k$?
- **local-global**: If $k$ is a global field, must the surface satisfy the local-global principle?
- **weak approximation**: If $k$ is a global field, must the surface satisfy weak approximation?

<table>
<thead>
<tr>
<th>Degree</th>
<th>$k$-point</th>
<th>$k$-rational†</th>
<th>$k$-unirational†</th>
<th>local-global</th>
<th>weak approximation</th>
</tr>
</thead>
<tbody>
<tr>
<td>9</td>
<td>NO</td>
<td>YES</td>
<td>YES</td>
<td>YES</td>
<td>YES</td>
</tr>
<tr>
<td>8</td>
<td>NO</td>
<td>YES</td>
<td>YES</td>
<td>YES</td>
<td>YES</td>
</tr>
<tr>
<td>7</td>
<td>YES</td>
<td>YES</td>
<td>YES</td>
<td>YES</td>
<td>YES</td>
</tr>
<tr>
<td>6</td>
<td>NO</td>
<td>YES</td>
<td>YES</td>
<td>YES</td>
<td>YES</td>
</tr>
<tr>
<td>5</td>
<td>YES</td>
<td>YES</td>
<td>YES</td>
<td>YES</td>
<td>YES</td>
</tr>
<tr>
<td>4</td>
<td>NO</td>
<td>NO</td>
<td>YES</td>
<td>NO</td>
<td>NO</td>
</tr>
<tr>
<td>3</td>
<td>NO</td>
<td>NO</td>
<td>YES</td>
<td>NO</td>
<td>NO</td>
</tr>
<tr>
<td>2</td>
<td>NO</td>
<td>NO</td>
<td>?</td>
<td>NO</td>
<td>NO</td>
</tr>
<tr>
<td>1</td>
<td>YES</td>
<td>NO</td>
<td>?</td>
<td>YES</td>
<td>NO</td>
</tr>
</tbody>
</table>

The daggers † in certain column headings serve as a warning that those columns presume the existence of a $k$-point.

9.5. Rational points on varieties of general type

9.5.1. Curves of genus > 1 over number fields.

(References: [HS00, BG06])

Let $X$ be a nice curve over a field $K$. In Section 2.6.4.2 we stated the following result, conjectured by Mordell in 1922 (for $K = \mathbb{Q}$) [Mor22] and proved by Faltings in 1983.

**Theorem 9.5.1 (Fal83).** Let $X$ be a nice curve of genus > 1 over a number field $K$. Then $X(K)$ is finite.

We will not give a proof, since the known proofs are very complicated. Faltings’s proof uses an idea of Parshin to reduce the problem to proving a conjecture of Shafarevich that for
a fixed number field $K$, a fixed finite set of places $S$ of $K$, and a fixed $d \geq 0$, there are at most finitely many isomorphism classes of $d$-dimensional abelian varieties over $K$ with good reduction outside $S$. Vojta [Voj91] gave a different proof of Theorem 9.5.1 based on diophantine approximation, and later Bombieri [Bom90] gave a more elementary version of Vojta’s proof; Bombieri’s proof is presented also in [HS00].

**Remark 9.5.2.** All known proofs of Theorem 2.6.8 are ineffective. In other words, it is not known whether there exists a Turing machine that takes as input a number field $K$ and equations for a nice $K$-curve $X$ of genus $> 1$, and outputs the list of $K$-points on $X$. See [Poo02] for more about this problem.

### 9.5.2. Curves of genus $> 1$ over function fields.

(References: [Sam66], [Vol97])

The analogue of Theorem 9.5.1 over global function fields can fail because of Frobenius morphisms, as the following two examples show.

**Example 9.5.3.** Let $X_0$ be a nice curve of genus $> 1$ over a finite field $\mathbb{F}_q$. Let $K = k(X_0)$. Let $X = (X_0)_K$. By Proposition 3.6.5(b), $X(K) = \text{Hom}_{\mathbb{F}_q}(X_0, X_0)$, which is infinite since it contains the $q^n$-power Frobenius morphism for every $n \geq 0$.

**Example 9.5.4.** Let $q$ be an odd prime power. Let $K = \mathbb{F}_q(t)$. Let $f \in \mathbb{F}_q[x]$ be a separable polynomial of degree $\geq 5$. Let $X$ be the nice $K$-curve birational to $f(t)y^2 = f(x)$, so $X$ has genus $> 1$. Then $(t^{q^n}, f(t)^{(q^n-1)/2}) \in X(K)$ for every $n \geq 0$, so $X(K)$ is infinite.

This example can be explained using the nice curve $Y$ defined by $y^2 = f(x)$: under the isomorphism $X_{K(f(t)^{1/2})} \to Y_{K(f(t)^{1/2})}$ sending $(x, y)$ to $(x, f(t)^{1/2}y)$, the points above correspond to $(t^{q^n}, f(t)^{q^n/2})$, which are as constructed in Example 9.5.3.

If we consider function fields over *infinite* constant fields, then the analogue of Theorem 9.5.1 can fail even in characteristic 0:

**Example 9.5.5.** Let $K = \mathbb{C}(t)$. Let $X_0$ be a curve over $\mathbb{C}$. Let $X = (X_0)_K$. Then $X(K)$ is infinite since it contains $X_0(\mathbb{C})$.

Nevertheless, there are positive results. To state them, we introduce a few definitions.

**Definition 9.5.6.** A function field with field of constants $k$ is $K := k(V)$ where $V$ is an integral $k$-variety and $k$ is algebraically closed in $K$.

**Remark 9.5.7.** By Proposition 2.2.22(b), the requirement that $k$ be algebraically closed in $K$ is automatically satisfied if $V$ is geometrically integral.

**Definition 9.5.8.** Let $K$ be a function field with field of constants $k$. Let $X$ be a $K$-variety.
(i) Call $X$ **constant** or **split** if $X = Y_K$ for some $k$-variety $Y$.

(ii) Call $X$ **isotrivial** if there exists a finite extension $K' \supset K$ such that $X_{K'}$ is constant (with respect to the constant field of $K'$).

**Example 9.5.9.** The curves in Examples 9.5.3 and 9.5.5 are constant. The curve in Example 9.5.4 is isotrivial, but not constant.

**Theorem 9.5.10.** Let $K$ be a function field with field of constants $k$. Let $X$ be a regular, projective, geometrically integral $K$-curve of genus $> 1$ such that $X(K)$ is infinite. If $\text{char} \; k = 0$, then $X$ is constant. If $\text{char} \; k = p$, then $X$ is isotrivial. Moreover, $X$ is nice, so $g(X_K) = g(X)$.

**Proof.** By induction on $\text{tr} \; \deg(K/k)$, we may reduce to the case $\text{tr} \; \deg(K/k) = 1$. For $\text{char} \; k = 0$, the first complete proof appeared in [Gra65] (see also [Man63], which was corrected in [Col90]). For $\text{char} \; k = p$, we may assume that $k$ is algebraically closed; then [Sam66, Théorème 4] proves the result when $g(X_K) > 1$, and in particular when $g(X_K) = g(X)$ since we assumed $g(X) > 1$. If $g(X_K) < g(X)$, then $X(K)$ is finite by [Vol91] Theorem 3]. Finally, by Theorem 2.5.1, the curve $X$ is nice if and only if $g(X_K) = g(X)$.

See [Miw69] for more detailed results.

**9.5.3. Higher-dimensional varieties.**

(Reference: [Lan91])

**Conjecture 9.5.11 (Bombieri, Lang independently).** Let $k$ be a number field. Let $X$ be a geometrically integral $k$-variety of general type with $\dim X > 0$. Then $X(k)$ is not Zariski dense in $X$.

There are various stronger forms proposed by Lang, discussed in [Lan91 I,§3]. Here is one of them:

**Conjecture 9.5.12 (Lang).** Let $k$ be a number field. Let $X$ be a geometrically integral $k$-variety of general type with $\dim X > 0$. Then there exists a closed subvariety $S \subseteq X$ such that $(X - S)(L)$ is finite for all finite extensions $L \supseteq k$.

In fact, Lang predicts what $S$ should be [Lan91 I,§3].

Faltings simplified and generalized Vojta’s methods to prove that Conjectures 9.5.11 and 9.5.12 are true when $X$ is a subvariety of an abelian variety [Fal91].

**Exercises**

9.1. Given a field $k$, describe all nice $k$-varieties that are simultaneously Fano and of general type.
Let $X$ be a nice surface over a field $k$. Let $C \subset X$ be a curve. Show that $C$ is a $(-1)$-curve with constant field $k$ on $X$ if and only if $C_{k}$ is a $(-1)$-curve on $X_{k}$.

Let $X$ be a nice surface over a field $k$. Let $K$ be a canonical divisor on $X$. Let $C \subset X$ be a curve. Without using Theorem 9.3.3, show that $C$ is a $(-1)$-curve on $X$ with constant field $k$ if and only if $C.C = -1$ and $C.K = -1$.

Let $X$ be a nice surface over an algebraically closed field $k$. For a coherent sheaf $\mathcal{F}$ on $X$ and for any $i \geq 0$, define $h^i(\mathcal{F}) := \dim_k H^i(X, \mathcal{F})$ and the Euler characteristic $\chi(\mathcal{F}) := \sum_{i \geq 0} (-1)^i h^i(\mathcal{F})$. Let $C \subset X$ be a curve. Without using Theorem 9.3.3, show that $C$ is a $(-1)$-curve if and only if $\chi(\mathcal{O}_C) > 0$ and $C.C = -h^0(\mathcal{O}_C)$.

Let $X$ be a nice surface over a field $k$. Let $P$ be a closed point of $X$. Let $L = k(P)$; suppose that $L$ is separable over $k$. Let $Y$ be the blow-up of $X$ at $P$. Let $Z[\mathfrak{S}_k/\mathfrak{S}_L]$ be the permutation module associated to $L/k$.

(a) Prove that $\text{Pic} Y_{k_s} \simeq \text{Pic} X_{k_s} \oplus Z[\mathfrak{S}_k/\mathfrak{S}_L]$.

(b) Prove that the natural homomorphism $H^1(\mathfrak{S}_k, \text{Pic} X_{k_s}) \to H^1(\mathfrak{S}_k, \text{Pic} Y_{k_s})$ is an isomorphism.

(c) Deduce that $H^1(\mathfrak{S}_k, \text{Pic} X_{k_s})$ is a birational invariant of a nice surface $X$ over a perfect field $k$.

Let $X \subseteq \mathbb{P}^n_k$ be a degree 3 hypersurface over a field $k$ for some $n \geq 2$.

(a) Let $L$ be a degree 2 separable field extension of $k$. Prove that if $X$ has an $L$-point, then $X$ has a $k$-point.

(b) Do the same without the separability hypothesis.

(Cassels and Swinnerton-Dyer conjectured that the same holds for an extension $L$ of $k$ of any degree $d$ not divisible by 3, but this is unknown even in the case $\dim X = 2$, $k = \mathbb{Q}$, $d = 4$. See [Cor76].)

Let $k$ be a field.

(a) Prove that for $0 \leq r \leq 4$, the group $\text{PGL}_3(k) = \text{Aut} \mathbb{P}^2_k$ acts transitively on the set of $r$-tuples of points in $\mathbb{P}^2(k)$ in general position.

(b) Fix a separably closed field $k$. For $5 \leq d \leq 9$, determine the number of isomorphism types of degree $d$ del Pezzo surfaces over $k$.

Let $k$ be a finite field. Prove that there are exactly seven isomorphism types of degree 5 del Pezzo surfaces over $k$. 

264
APPENDIX A

Universes

(Reference: [SGA 4i I.Appendice])

The plan is to assume the existence of a very large set, called a universe, such that almost all the constructions we need can be carried out within it. Those constructions that cannot be carried out within it can be carried out in a larger universe.

According to [SGA 4i I.Appendice], the theory of universes comes from “the secret papers of N. Bourbaki”. According to [SGA 1 VI, §1], the details will be given in a book in preparation by Chevalley and Gabriel to appear in the year 3000.

A.1. Definition of universe

Everything is a set. In particular, elements of a set are themselves sets. Given a set $x$, let $\mathcal{P}(x)$ be the set of all subsets of $x$.

**Definition A.1.1.** ([SGA 4i I.Appendice, Définition 1]) A universe is a set $\mathcal{U}$ satisfying the following conditions:

(U.I) If $y \in \mathcal{U}$ and $x \in y$, then $x \in \mathcal{U}$.

(U.II) If $x, y \in \mathcal{U}$, then $\{x, y\} \in \mathcal{U}$.

(U.III) If $x \in \mathcal{U}$, then $\mathcal{P}(x) \in \mathcal{U}$.

(U.IV) If $I \in \mathcal{U}$, and $(x_i)_{i \in I}$ is a collection of elements of $\mathcal{U}$, then the union $\bigcup_{i \in I} x_i$ is an element of $\mathcal{U}$.

A universe $\mathcal{U}$ is not a “set of all sets”. In particular, a universe cannot be a member of itself: see Exercise A.2

A.2. The universe axiom

To the usual ZFC axioms of set theory (the Zermelo-Frenkel axioms with the axiom of choice), one adds the universe axiom ([SGA 4i I.Appendice.§4])

Every set is an element of some universe.

\[\text{In [SGA 4i I.Appendice.§4] one finds an additional axiom (UB) that is present only because Bourbaki’s axioms for set theory are different from the usual ZFC axioms. Bourbaki’s set theory includes a global choice operator } \tau: \text{ for any 1-variable predicate } P(x), \text{ the expression } \tau_x P(x) \text{ represents an element } y \text{ such that } P(y) \text{ is true, if such a } y \text{ exists. Axiom (UB) says that for any 1-variable predicate } P(x) \text{ and any universe } \mathcal{U}, \text{ if there exists } y \in \mathcal{U} \text{ such that } P(y) \text{ is true, then } \tau_x P(x) \text{ is an element of } \mathcal{U}. \text{ So axiom (UB) says that the elements produced by the global choice operator lie in a given universe whenever possible.} \]
Suppose that ZFC is consistent. Then it turns out that the negation of the universe axiom is consistent with ZFC: given a model of ZFC, one can build another model of ZFC in which the universe axiom fails. But it is not known whether the universe axiom itself is consistent with ZFC.

The universe axiom is so convenient that we are going to assume it despite its uncertain status relative to ZFC.

Remark A.2.1. The original proof of Fermat’s last theorem made use of constructions relying on the universe axiom! But the proof can probably be redone without this axiom: see Section A.5.

A.3. Strongly inaccessible cardinals

Definition A.3.1. A cardinal $\kappa$ is strongly inaccessible if

1. For every $\lambda < \kappa$, we have $2^\lambda < \kappa$.
2. If $(\lambda_i)_{i \in I}$ is a family of cardinals indexed by a set $I$ of cardinality strictly less than $\kappa$, and $\lambda_i < \kappa$ for all $i \in I$, then $\sum_{i \in I} \lambda_i < \kappa$.

The two smallest strongly inaccessible cardinals are 0 and $\aleph_0$. By $[1]$, any other strongly inaccessible cardinal $\kappa$ must be larger than all of

$$\beth_0 := \aleph_0$$

$$\beth_1 := 2^{\aleph_0}$$

$$\beth_2 := 2^{2^{\aleph_0}}$$

$$\vdots$$

By [2], $\kappa$ must also be larger than the supremum $\beth_\omega$ of all these. Transfinite induction continues this sequence of cardinals by defining $\beth_\alpha$ for any ordinal $\alpha$. Then $\kappa$ must be larger than $\beth_\omega$, $\beth_\omega^\omega$, $\ldots$, and even $\beth_{\omega_1}$, where $\omega_1$ is the first uncountable ordinal. Identify each cardinal with the first ordinal of its cardinality. Then $\omega_1 \leq 2^{\aleph_0} = \beth_1$, so $\beth_{\omega_1} \leq \beth_2$. But $\kappa$ is also larger than $\beth_{\omega_1}$, $\beth_{\omega_1^{\omega_1}}$, and so on.

Theorem A.3.2. Within ZFC, the universe axiom is equivalent to the following “large cardinal axiom”:

For every cardinal, there is a strictly larger strongly inaccessible cardinal.

Proof. One direction is easy, because if $\mathcal{U}$ is a universe, then $\sup\{\#x : x \in \mathcal{U}\}$ is a strongly inaccessible cardinal. For the other direction, see [SGA 4] I.Appendice.§5, which constructs a universe from a strongly inaccessible cardinal. $\square$
A.4. Universes and categories

We now assume that an uncountable universe $U$ has been fixed.

Recall that everything is a set. For instance, an ordered pair $(x, y)$ is $\{x, \{y\}\}$. A group is a 4-tuple $(G, m, i, e)$ such that various conditions hold. Even a scheme can be described as a set.

**Definition A.4.1.** A **small category** is a category in which the collection of objects is a set (instead of a class).

We want all our categories to be small categories. Thus for example, **Sets** will denote not the category of all sets, but the category of sets that are elements of $U$. Similarly, **Groups** will be the category of groups that are elements of $U$, and so on.

For categories such as these two, the set of objects is a subset of $U$ having the same cardinality as $U$, which implies that the set of objects cannot be an element of $U$. This creates a minor problem: the collection of all functors $\textit{Schemes}^{\text{opp}} \to \textit{Sets}$, say, is a set of cardinality larger than that of $U$! The category of such functors is still a small category, but it lives in a larger universe $U'$.

A.5. Avoiding universes

Suppose that we want to prove theorems that are not conditional on the universe axiom. Then we cannot define the category **Schemes** as the set of schemes that are elements of a particular universe $U$. Instead we choose a category of schemes that is closed under various operations, and work within that category $\text{[SP Tag 020S Tag 03XB]}$. Ideally, we should then show that our choice did not matter for our particular objects of study; see $\text{[SP Tag 00VY]}$ for an example of this.

**Exercises**

A.1. Classify all finite universes.

A.2. Let $U$ be a universe. Prove that $U \not\in U$.

A.3. Let $P_0 = \emptyset$. For $n \in \mathbb{N}$, inductively define $P_{n+1} := \mathcal{P}(P_n)$. Let $U = \bigcup_{n \in \mathbb{N}} P_n$. Prove that $U$ is a universe.
APPENDIX B

Other kinds of fields

In Section 1.1, we introduced some of the most important fields for number theory, namely local and global fields. Here we discuss some other fields that arise in nature.

B.1. Higher-dimensional local fields

Higher-dimensional local fields are defined recursively as follows. A 0-dimensional local field is a finite field. For $n \geq 1$, an $n$-dimensional local field is a field complete with respect to a discrete valuation whose residue field is an $(n - 1)$-dimensional local field. Local class field theory can be generalized to these fields, and there is also a generalization of global class field theory to finitely generated fields $\text{Kat79}, \text{Kat80}, \text{Kat82}, \text{KS86}$. These generalizations involve $K$-theory.

Example B.1.1. The field $\mathbb{Q}_p((t))$ is a 2-dimensional local field.

Warning B.1.2. An $n$-dimensional local field for $n \neq 1$ is not a local field in the sense of Section 1.1.2. In the rest of this book, we use the term “local field” as in Section 1.1.2.

B.2. Formally real and real closed fields

(Reference: Chapter 11 of $\text{Jac89}$)

Definition B.2.1. A field $k$ is formally real if it satisfies one of the following equivalent conditions:

(i) $k$ admits a total ordering compatible with the addition and multiplication.

(ii) $-1$ is not a sum of squares in $k$.

The implication (ii) $\Rightarrow$ (i) is not obvious. Its proof uses Zorn’s lemma to find a maximal subgroup $P$ of $k^\times$ that is closed under addition and contains $k^{\times 2}$ but not $-1$. Then $P$ turns out to be the set of positive elements for an ordering on $k$. See Theorem 11.1 of $\text{Jac89}$ for details.

Definition B.2.2. A field $k$ is real closed if it satisfies one of the following equivalent conditions:

(i) $-1 \notin k^{\times 2}$, and $k(\sqrt{-1})$ is algebraically closed.

(ii) $1 < [\overline{k} : k] < \infty$. 

268
(iii) \( k \) is an ordered field such that every positive element has a square root and every odd
degree polynomial in \( k[x] \) has a zero.
(iv) \( k \) is a formally real field with no nontrivial formally real algebraic extension.

The equivalence of these conditions is not obvious. For the proof, see Theorems 11.2, 11.3,
and 11.14 in \cite{Jac89}. The entire theory is due to Artin and Schreier.

The field \( \mathbb{Q} \) is formally real but not real closed. The field \( \mathbb{R} \) is real closed, as is the subfield
of real numbers that are algebraic over \( \mathbb{Q} \). Every formally real field has an algebraic extension
that is real closed.

\section*{B.3. Henselian fields}

(Reference: \cite[Section 2.3]{Ray70a})

Complete discrete valuation rings are not the only rings satisfying Hensel’s lemma.

**Definition B.3.1.** Let \( R \) be a local ring, and let \( k \) be its residue field. The ring \( R \) is
called henselian if one of the following equivalent conditions holds:

1. Every finite \( R \)-algebra is a product of local rings.
2. Hensel’s lemma for lifting roots: If \( f \in R[x] \) is a monic polynomial whose reduction
\( \bar{f} \in k[x] \) has a simple zero \( \bar{a} \in k \), then there exists a zero \( a \in R \) of \( f \) reducing to \( \bar{a} \).
3. Hensel’s lemma for lifting factorizations: If \( f \in R[x] \) is a monic polynomial, any factor-
ization of its reduction \( \bar{f} = \bar{g}\bar{h} \) into relatively prime monic polynomials \( \bar{g}, \bar{h} \in k[x] \) lifts to
a factorization \( f = gh \) into monic polynomials \( g, h \in R[x] \).

(For the equivalence, see \cite[I.§1.5 and VII.§3.3]{Ray70a}.)

**Definition B.3.2.** A valued field is henselian if its valuation subring is henselian.

**Example B.3.3.** Let \( k = \mathbb{Q}_p \cap \overline{\mathbb{Q}} \), i.e., the set of elements of \( \mathbb{Q}_p \) that are algebraic over \( \mathbb{Q} \).
Restrict the \( p \)-adic valuation on \( \mathbb{Q}_p \) to a valuation on \( k \). Then \( k \) is a noncomplete henselian
field. This field acts in many ways like \( \mathbb{Q}_p \), but is algebraic over \( \mathbb{Q} \), which can be an advantage.

**Definition B.3.4.** A henselian ring (or its fraction field) is called strictly henselian if its
residue field is separably closed.

**Example B.3.5.** The maximal unramified extension \( k^{\text{unr}} \) of a discretely valued field \( k \)
is strictly henselian (cf. \cite[X.§2]{Ray70a}) but usually not complete. For example, if \( k \) is a
nonarchimedean local field, then \( k^{\text{unr}} \) is not complete.

Given a commutative local ring \( R \), its henselization \( R^h \) is a henselian local ring with the
following universal property: every homomorphism from \( R \) to a henselian local ring factors
through \( R^h \). Such a ring \( R^h \) exists: it can be constructed as the direct limit of \( R' \) as \( R' \) ranges
over étale local \( R \)-algebras having the same residue field as \( R \). \cite[VIII, Théorème 1]{Ray70a}.
If $F$ is a valued field, and $R$ is its valuation ring, then one can define the henselization of $F$ by $F^h := \text{Frac}(R^h)$. The field $k$ in Example [B.3.3] is the henselization of $\mathbb{Q}$ with its $p$-adic valuation. One can also define the strict henselization. See [Ray70a, Chapitre VIII] or [BLR90, §2.3, Definitions 6 and 6'] for details.

**B.4. Hilbertian fields**

(References: Chapter 9 of [Ser97], and Chapters 12, 13, and 16 of [FJ08])

Given the polynomial

$$f(t, x) := (t + 5)x^2 + (2t - 3)x + (t^2 - 9) \in \mathbb{Q}[t, x]$$

and the number 4, we can specialize $f$ by evaluating each coefficient at $t = 4$; the result is

$$f(4, x) = 9x^2 + 5x + 7 \in \mathbb{Q}[x].$$

The simplest version of the Hilbert irreducibility theorem states that for every irreducible polynomial $f(t, x) \in \mathbb{Q}[t, x]$, there are infinitely many $a \in \mathbb{Q}$ such that the specialized polynomial $f(a, x) \in \mathbb{Q}[x]$ is irreducible. The definition of hilbertian field is modeled after this property. (For other equivalent definitions, see [Ser97, Chapter 9] and [FJ08, §12.1].)

**Definition B.4.1.** A field $k$ is **hilbertian** if for every finite list of irreducible two-variable polynomials $f_1, \ldots, f_n \in k[t, x]$ with each $f_i$ separable in $x$, there are infinitely many $a \in k$ such that the one-variable polynomials $f_1(a, x), \ldots, f_n(a, x) \in k[x]$ are simultaneously irreducible.

Global fields are hilbertian [FJ08, 13.4.2]. If $K$ is a finitely generated transcendental extension of any field $k$, then $K$ is hilbertian [FJ08, 13.4.2]. Finite fields, local fields, and separably closed fields are not hilbertian, as will be shown in the exercises.

**B.5. Pseudo-algebraically closed fields**

(Reference: [FJ08, Chapter 11])

These are studied in model theory.

**Definition B.5.1.** A field $k$ is **pseudo-algebraically closed** (PAC) if every geometrically integral variety over $k$ has a $k$-point. (See Section 2.2.2 for the definition of “geometrically integral variety” and Section 2.3.2 for the definition of “$k$-point”.)

**Remark B.5.2.** Bertini theorems show that every geometrically integral variety of positive dimension over $k$ contains a geometrically integral curve, so Definition 2.5.1 is unchanged if we replace “variety” by “curve”. (Here “curve” means “variety of dimension 1”.)

The following are examples of PAC fields:

(1) separably closed fields,
(2) infinite algebraic extensions of finite fields,
(3) nonprincipal ultraproducts of distinct finite fields (that is, \((\prod_{i=1}^{\infty} k_i) / m\) where the \(k_i\) are finite fields of distinct orders, and \(m\) is a nonprincipal maximal ideal of the ring \(\prod_{i=1}^{\infty} k_i\).)

**Question B.5.3.** ([FJ08 11.5.9(a)]) Is the maximal solvable extension of \(\mathbb{Q}\) a PAC field?

**Exercises**

**B.1.** Let \(k\) be a local field. Let \(n\) be a positive integer such that \(\text{char } k \nmid n\). Prove that \(k^\times/k^\times n\) is finite.

**B.2.** Prove that finite fields are not hilbertian.

**B.3.** Prove that separably closed fields are not hilbertian.

**B.4.** Prove that local fields are not hilbertian.
APPENDIX C

Properties under base extension

C.1. Morphisms

Let “blah” be a property of morphisms of schemes. We can ask the following questions:

**Definition:** Where in EGA (or elsewhere) is it defined?

**Composition:** Is a composition of two blah morphisms blah?

**Base extension:** Let \( f : X \to S \) be a morphism of schemes, and let \( f' : X' \to S' \) be its base extension by a morphism \( S' \to S \). If \( f \) is blah, must \( f' \) be blah?

**fpqc descent:** Let \( f : X \to S \) be a morphism of schemes, and let \( f' : X' \to S' \) be its base extension by an fpqc morphism \( S' \to S \). If \( f' \) is blah, must \( f \) be blah?

**Spreading out:** Does blah spread out in the sense of Theorem 3.2.1(iv)?

Answers are given in Table 1. If a reference is given, the answer is “YES”. In some cases, if the answer is obvious or it follows easily from other entries, we write “YES” or “NO” instead of giving a reference. If you see a superscript such as \(^7\), please read the corresponding caveat below:

1. Our definitions of fppf and fpqc are less restrictive than the standard ones suggested by the acronyms: see Section 3.4.
2. In the fpqc column, the EGA references assume that the base extension is by a faithfully flat and quasi-compact morphism. This implies descent for our more general notion of fpqc morphism, by Lemma C.1.1 below, provided that we know that blah is **local on the base** (in the Zariski topology), i.e., that for any morphism \( f : X \to S \) and any Zariski open covering \( \{S_i\} \) of \( S \), the morphism \( f \) is blah if and only if \( f|_{f^{-1}S_i} : f^{-1}S_i \to S_i \) is blah for all \( i \). Conversely, if blah satisfies fpqc descent and is stable under base extension by open immersions, then blah is local on the base.

   Lemma C.1.1 below says roughly that the “open covering” given by an fpqc morphism can be “refined” to another fpqc morphism consisting of a faithfully flat quasi-compact morphism followed by a Zariski open covering morphism.

3. In the rows labelled geom. connected, geom. integral, geom. irreducible, geom. reduced, we are considering a morphism of finite presentation whose fibers have the specified property. The first and third properties for morphisms are called connected and irreducible in [EGA IV] 4.5.5].
4. The morphisms

\[ \text{Spec } k[x, x^{-1}] \amalg \text{Spec } k[x]/(x) \to \text{Spec } k[x] \to \text{Spec } k \]

have geometrically integral fibers, but the unique fiber of the composition is not even connected. On the other hand, see [EGA IV, 4.5.7] for some positive results.

5. The morphisms

\[ \text{Spec } k[x]/(x^2) \to \text{Spec } k[x] \to \text{Spec } k \]

have geometrically reduced (and even geometrically integral) fibers, but their composition does not.

6. The property of being an immersion satisfies fppf descent, but it is not known whether it satisfies fpqc descent.

7. A composition of projective morphisms \( X \to Y \to Z \) is projective if \( Z \) is quasi-compact or the topological space underlying \( Z \) is noetherian.

8. A composition of quasi-projective morphisms \( X \to Y \to Z \) is quasi-projective if \( Z \) is quasi-compact.

9. Projective and quasi-projective do not satisfy fpqc descent, because they are not even local on the base in the Zariski topology: see [Har77, Exercise II.7.13] for a counterexample.

10. To generalize the spreading out properties for projective and quasi-projective morphisms beyond Theorem 3.2.1 to the setting of more general limits, one should work over a quasi-separated base.

11. To generalize the spreading out properties for étale, faithfully flat, flat, fppf, smooth, and G-unramified morphisms beyond Theorem 3.2.1 to the setting of more general limits, one should work over a quasi-compact base.

12. What is called G-unramified here is called unramified in [EGA IV, 17.3.1]. See Warning 3.5.32.

Lemma C.1.1. Any fpqc morphism of schemes \( f : X \to Y \) fits into a commutative diagram
in which $Y' \to Y$ and $X' \to X$ are Zariski open covering morphisms, $X'' \to X'$ is an open immersion, and $X'' \to Y'$ is faithfully flat and quasi-compact. (In particular, $X'' \to Y$ is fpqc.)

Proof. Let $\{Y_i\}$ be an affine open cover of $Y$. Let $Y' = \bigsqcup Y_i$. Let $X' = \bigsqcup f^{-1}Y_i$. By definition of fpqc, for each $i$ there is a quasi-compact open subscheme $U_i$ of $f^{-1}Y_i$ with $f(U_i) = Y_i$. Let $X''$ be the open subscheme $\bigsqcup U_i$ of $X'$. Then $X'' \to Y'$ is faithfully flat and quasi-compact, because each morphism $f|_{U_i} : U_i \to Y_i$ is so. \qed

274
<table>
<thead>
<tr>
<th>Property</th>
<th>Definition</th>
<th>Composition</th>
<th>Base extension</th>
<th>fpqc descent</th>
<th>Spreading out</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>affine</strong></td>
<td>EGA II</td>
<td>EGA II</td>
<td>EGA II</td>
<td>EGA IV_3</td>
<td>EGA IV_3</td>
</tr>
<tr>
<td><strong>bijection</strong></td>
<td>YES</td>
<td>YES</td>
<td>EGA II</td>
<td>EGA IV_2</td>
<td>EGA IV_2</td>
</tr>
<tr>
<td><strong>closed</strong></td>
<td>EGA I</td>
<td>EGA I</td>
<td>NO</td>
<td>EGA IV_2</td>
<td>NO</td>
</tr>
<tr>
<td><strong>closed immersion</strong></td>
<td>EGA I</td>
<td>EGA I</td>
<td>EGA I</td>
<td>EGA IV_2</td>
<td>EGA IV_2</td>
</tr>
<tr>
<td><strong>dominant</strong></td>
<td>EGA I</td>
<td>EGA I</td>
<td>NO</td>
<td>EGA IV_2</td>
<td>NO</td>
</tr>
<tr>
<td><strong>étale</strong></td>
<td>EGA IV_1</td>
<td>EGA IV_1</td>
<td>EGA IV_1</td>
<td>EGA IV_2</td>
<td>EGA IV_2</td>
</tr>
<tr>
<td><strong>faithfully flat</strong></td>
<td>YES</td>
<td>YES</td>
<td>EGA IV_1</td>
<td>EGA IV_2</td>
<td>EGA IV_2</td>
</tr>
<tr>
<td><strong>finite</strong></td>
<td>EGA II</td>
<td>EGA II</td>
<td>EGA II</td>
<td>EGA IV_2</td>
<td>EGA IV_2</td>
</tr>
<tr>
<td><strong>finite presentation</strong></td>
<td>EGA IV_1</td>
<td>EGA IV_1</td>
<td>EGA IV_1</td>
<td>EGA IV_2</td>
<td>EGA IV_2</td>
</tr>
<tr>
<td><strong>finite type</strong></td>
<td>EGA I</td>
<td>EGA I</td>
<td>EGA I</td>
<td>EGA IV_2</td>
<td>EGA IV_2</td>
</tr>
<tr>
<td><strong>flat</strong></td>
<td>EGA I</td>
<td>EGA IV_2</td>
<td>EGA IV_2</td>
<td>EGA IV_2</td>
<td>EGA IV_2</td>
</tr>
<tr>
<td><strong>formally étale</strong></td>
<td>EGA IV_1</td>
<td>EGA IV_1</td>
<td>EGA IV_1</td>
<td>EGA IV_2</td>
<td>EGA IV_2</td>
</tr>
<tr>
<td><strong>formally smooth</strong></td>
<td>EGA IV_1</td>
<td>EGA IV_1</td>
<td>EGA IV_1</td>
<td>EGA IV_2</td>
<td>EGA IV_2</td>
</tr>
<tr>
<td><strong>formally unram.</strong></td>
<td>EGA IV_1</td>
<td>EGA IV_1</td>
<td>EGA IV_1</td>
<td>EGA IV_2</td>
<td>EGA IV_2</td>
</tr>
<tr>
<td><strong>fpqc</strong></td>
<td>Vis05 2.34</td>
<td>Vis05 2.35</td>
<td>Vis05 2.35</td>
<td>EGA IV_2</td>
<td>EGA IV_2</td>
</tr>
<tr>
<td><strong>fpqc</strong></td>
<td>Vis05 2.34</td>
<td>Vis05 2.35</td>
<td>Vis05 2.35</td>
<td>EGA IV_2</td>
<td>EGA IV_2</td>
</tr>
<tr>
<td><strong>geom. connected</strong></td>
<td>EGA IV_1</td>
<td>EGA IV_1</td>
<td>EGA IV_1</td>
<td>EGA IV_2</td>
<td>EGA IV_2</td>
</tr>
<tr>
<td><strong>geom. integral</strong></td>
<td>EGA IV_1</td>
<td>EGA IV_1</td>
<td>EGA IV_1</td>
<td>EGA IV_2</td>
<td>EGA IV_2</td>
</tr>
<tr>
<td><strong>geom. irreducible</strong></td>
<td>EGA IV_1</td>
<td>EGA IV_1</td>
<td>EGA IV_1</td>
<td>EGA IV_2</td>
<td>EGA IV_2</td>
</tr>
<tr>
<td><strong>geom. reduced</strong></td>
<td>EGA IV_1</td>
<td>EGA IV_1</td>
<td>EGA IV_1</td>
<td>EGA IV_2</td>
<td>EGA IV_2</td>
</tr>
<tr>
<td><strong>homeomorphism</strong></td>
<td>YES</td>
<td>YES</td>
<td>EGA IV_1</td>
<td>EGA IV_2</td>
<td>EGA IV_2</td>
</tr>
<tr>
<td><strong>immersion</strong></td>
<td>EGA I</td>
<td>EGA I</td>
<td>EGA I</td>
<td>EGA IV_2</td>
<td>EGA IV_2</td>
</tr>
<tr>
<td><strong>injective</strong></td>
<td>EGA I</td>
<td>EGA I</td>
<td>EGA I</td>
<td>EGA IV_2</td>
<td>EGA IV_2</td>
</tr>
<tr>
<td><strong>isomorphism</strong></td>
<td>EGA I</td>
<td>EGA I</td>
<td>EGA I</td>
<td>EGA IV_2</td>
<td>EGA IV_2</td>
</tr>
<tr>
<td><strong>loc. immersion</strong></td>
<td>EGA I</td>
<td>EGA I</td>
<td>EGA I</td>
<td>EGA IV_2</td>
<td>EGA IV_2</td>
</tr>
<tr>
<td><strong>loc. isomorphism</strong></td>
<td>EGA I</td>
<td>EGA I</td>
<td>EGA I</td>
<td>EGA IV_2</td>
<td>EGA IV_2</td>
</tr>
<tr>
<td><strong>loc. of finite pres.</strong></td>
<td>EGA IV_1</td>
<td>EGA IV_1</td>
<td>EGA IV_1</td>
<td>EGA IV_2</td>
<td>EGA IV_2</td>
</tr>
<tr>
<td><strong>loc. of finite type</strong></td>
<td>EGA I</td>
<td>EGA I</td>
<td>EGA I</td>
<td>EGA IV_2</td>
<td>EGA IV_2</td>
</tr>
<tr>
<td><strong>monomorphism</strong></td>
<td>EGA I</td>
<td>EGA I</td>
<td>EGA I</td>
<td>EGA IV_2</td>
<td>EGA IV_2</td>
</tr>
<tr>
<td><strong>open</strong></td>
<td>EGA I</td>
<td>EGA I</td>
<td>EGA I</td>
<td>EGA IV_2</td>
<td>EGA IV_2</td>
</tr>
<tr>
<td><strong>open immersion</strong></td>
<td>EGA I</td>
<td>EGA I</td>
<td>EGA I</td>
<td>EGA IV_2</td>
<td>EGA IV_2</td>
</tr>
<tr>
<td><strong>projective</strong></td>
<td>EGA II</td>
<td>EGA II</td>
<td>EGA II</td>
<td>EGA IV_2</td>
<td>EGA IV_2</td>
</tr>
<tr>
<td><strong>proper</strong></td>
<td>EGA II</td>
<td>EGA II</td>
<td>EGA II</td>
<td>EGA IV_2</td>
<td>EGA IV_2</td>
</tr>
<tr>
<td><strong>quasi-affine</strong></td>
<td>EGA II</td>
<td>EGA II</td>
<td>EGA II</td>
<td>EGA IV_2</td>
<td>EGA IV_2</td>
</tr>
<tr>
<td><strong>quasi-compact</strong></td>
<td>EGA I</td>
<td>EGA I</td>
<td>EGA I</td>
<td>EGA IV_2</td>
<td>EGA IV_2</td>
</tr>
<tr>
<td><strong>quasi-finite</strong></td>
<td>EGA II</td>
<td>EGA II</td>
<td>EGA II</td>
<td>EGA IV_2</td>
<td>EGA IV_2</td>
</tr>
<tr>
<td><strong>quasi-projective</strong></td>
<td>EGA II</td>
<td>EGA II</td>
<td>EGA II</td>
<td>EGA IV_2</td>
<td>EGA IV_2</td>
</tr>
<tr>
<td><strong>quasi-separated</strong></td>
<td>EGA IV_1</td>
<td>EGA IV_1</td>
<td>EGA IV_1</td>
<td>EGA IV_2</td>
<td>EGA IV_2</td>
</tr>
<tr>
<td><strong>radical</strong></td>
<td>EGA I</td>
<td>EGA I</td>
<td>EGA I</td>
<td>EGA IV_2</td>
<td>EGA IV_2</td>
</tr>
<tr>
<td><strong>sch.-th. dominant</strong></td>
<td>YES</td>
<td>YES</td>
<td>EGA IV_1</td>
<td>EGA IV_2</td>
<td>EGA IV_2</td>
</tr>
<tr>
<td><strong>separated</strong></td>
<td>EGA I</td>
<td>EGA I</td>
<td>EGA I</td>
<td>EGA IV_2</td>
<td>EGA IV_2</td>
</tr>
<tr>
<td><strong>smooth</strong></td>
<td>EGA IV_1</td>
<td>EGA IV_1</td>
<td>EGA IV_1</td>
<td>EGA IV_2</td>
<td>EGA IV_2</td>
</tr>
<tr>
<td><strong>surjective</strong></td>
<td>EGA I</td>
<td>EGA I</td>
<td>EGA I</td>
<td>EGA IV_2</td>
<td>EGA IV_2</td>
</tr>
<tr>
<td><strong>univ. bicommutative</strong></td>
<td>EGA IV_2</td>
<td>EGA IV_2</td>
<td>EGA IV_2</td>
<td>EGA IV_2</td>
<td>EGA IV_2</td>
</tr>
<tr>
<td><strong>univ. closed</strong></td>
<td>EGA II</td>
<td>EGA II</td>
<td>EGA II</td>
<td>EGA IV_2</td>
<td>EGA IV_2</td>
</tr>
<tr>
<td><strong>univ. homeom.</strong></td>
<td>EGA II</td>
<td>EGA II</td>
<td>EGA II</td>
<td>EGA IV_2</td>
<td>EGA IV_2</td>
</tr>
<tr>
<td><strong>univ. open</strong></td>
<td>EGA II</td>
<td>EGA II</td>
<td>EGA II</td>
<td>EGA IV_2</td>
<td>EGA IV_2</td>
</tr>
<tr>
<td><strong>unramified</strong></td>
<td>SP Tag 02G</td>
<td>SP Tag 02G</td>
<td>SP Tag 02G</td>
<td>EGA IV_2</td>
<td>EGA IV_2</td>
</tr>
<tr>
<td><strong>G-unramified</strong></td>
<td>EGA IV_1</td>
<td>EGA IV_1</td>
<td>EGA IV_1</td>
<td>EGA IV_2</td>
<td>EGA IV_2</td>
</tr>
</tbody>
</table>

Table 1. Properties of morphisms
Please contact the author if you can fill in some of the blanks in Table 1.

### C.2. Varieties

<table>
<thead>
<tr>
<th>blah</th>
<th>Definition</th>
<th>Base extension</th>
<th>Descent</th>
</tr>
</thead>
<tbody>
<tr>
<td>connected</td>
<td>EGA I 2.1.8</td>
<td>NO</td>
<td>YES</td>
</tr>
<tr>
<td>loc. integral</td>
<td>EGA I 2.1.8</td>
<td>NO</td>
<td>YES</td>
</tr>
<tr>
<td>integral</td>
<td>EGA I 2.1.8</td>
<td>NO</td>
<td>YES</td>
</tr>
<tr>
<td>irreducible</td>
<td>EGA I 2.1.8</td>
<td>NO</td>
<td>YES</td>
</tr>
<tr>
<td>reduced</td>
<td>EGA I 0:4.1.4</td>
<td>NO</td>
<td>YES</td>
</tr>
<tr>
<td>regular</td>
<td>EGA I 0:4.1.4</td>
<td>NO</td>
<td>EGA IV 2, 6.5.2(i)</td>
</tr>
</tbody>
</table>

**Table 2. Properties of varieties**

Each YES under “Descent” denotes the easy fact that if $X$ is a $k$-variety and $L \supseteq k$ is a field extension such that the $L$-variety $X_L$ has the property, then $X$ has the property too.

### C.3. Algebraic groups

Let “blah” be a property of an algebraic group $G$ over a field $k$. We can ask the following questions:

**Base extension:** If $G$ is blah, and $L \supseteq k$ is a field extension, must $G_L$ be blah?

**Subgroup:** If $G$ is blah, must every closed subgroup scheme of $G$ be blah?

**Quotient:** If $G$ is blah and $H \leq G$ is a closed normal subgroup scheme, must $G/H$ be blah?

**Extension:** If $1 \to A \to B \to C \to 1$ is an exact sequence of algebraic groups, and $A$ and $C$ are blah, must $B$ be blah?

**Descent:** If $L \supseteq k$ is a field extension and $G_L$ is blah, must $G$ be blah?

Answers are given in Table 3; we omit the answers for “Descent” since they are “YES” for every property listed. If a reference is given, the answer is “YES”. In some cases, if the answer is obvious or it follows easily from other entries, we write “YES” or “NO” instead of giving a reference. If you see a superscript such as 7, please read the corresponding comment below:

1. The answer is “YES” if the extension $B$ is commutative or $C$ is connected. But in general the answer is “NO”: if char $k \neq 2$, then the group $G$ in Exercise 5.1 is an extension of groups of multiplicative type, but is not itself of multiplicative type.

2. Let $k = \mathbb{F}_p(t)$ and $L = \mathbb{F}_p(t^{1/p})$. If $G$ is the subgroup $x^p - ty^p = 0$ in $G_2^2$ over $k$, then $G$ is reduced, but $G_L$ is not.

3. If $G$ is as in 2, then $G \times G$ is not reduced.

4. The conjugation action of $\text{PGL}_2$ on the space $M_2$ of $2 \times 2$ matrices gives an injective homomorphism $\text{PGL}_2 \to \text{GL}_4$ whose image is contained in $\text{SL}_4$ (because $\text{PGL}_2$ is simple).
5. For any $n \geq 2$, the group $\text{SL}_n$ is simply connected, but its quotient $\text{PGL}_n \simeq \text{SL}_n / \mu_n$ is not.

<table>
<thead>
<tr>
<th>blah</th>
<th>Base extension</th>
<th>Subgroup</th>
<th>Quotient</th>
<th>Extension</th>
</tr>
</thead>
<tbody>
<tr>
<td>abelian variety</td>
<td>YES</td>
<td>YES</td>
<td>YES</td>
<td>YES</td>
</tr>
<tr>
<td>adjoint</td>
<td>YES</td>
<td>NO</td>
<td>YES</td>
<td>YES</td>
</tr>
<tr>
<td>affine</td>
<td><strong>EGA II</strong> 1.6.2(iii)]</td>
<td>YES</td>
<td><strong>SGA 3</strong> 11.7</td>
<td>Proposition 5.2.7(b)</td>
</tr>
<tr>
<td>connected = geom. connected</td>
<td>YES</td>
<td>NO</td>
<td>YES</td>
<td>YES</td>
</tr>
<tr>
<td>finite</td>
<td><strong>EGA II</strong> 6.1.5(iii)]</td>
<td>YES</td>
<td><strong>SGA 3</strong> 9.2(xii)]</td>
<td>Proposition 5.2.7(b)</td>
</tr>
<tr>
<td>(finite) étale = unramified</td>
<td><strong>EGA IV</strong> 17.3.3(ii)]</td>
<td>YES</td>
<td><strong>SGA 3</strong> 9.2(xii)]</td>
<td>Proposition 5.2.7(b)</td>
</tr>
<tr>
<td>multiplicative type</td>
<td>YES</td>
<td><strong>SGA 3</strong> IX 8.1</td>
<td><strong>SGA 3</strong> IX 8.1</td>
<td>YES</td>
</tr>
<tr>
<td>proper</td>
<td><strong>EGA II</strong> 5.4.2(iii)]</td>
<td>YES</td>
<td>YES</td>
<td>Proposition 5.2.7(b)</td>
</tr>
<tr>
<td>reduced</td>
<td>NO(3)</td>
<td>NO</td>
<td><strong>SGA 3</strong> 9.2(ix)]</td>
<td>NO(3)</td>
</tr>
<tr>
<td>reductive</td>
<td>YES</td>
<td>NO</td>
<td>YES</td>
<td>YES</td>
</tr>
<tr>
<td>semisimple</td>
<td>YES</td>
<td>NO</td>
<td>YES</td>
<td>YES</td>
</tr>
<tr>
<td>solvable</td>
<td>YES</td>
<td>YES</td>
<td>YES</td>
<td>YES</td>
</tr>
<tr>
<td>simply connected</td>
<td>YES</td>
<td>NO(3)</td>
<td>NO(3)</td>
<td>NO(3)</td>
</tr>
<tr>
<td>smooth = geom. reduced</td>
<td><strong>EGA IV</strong> 17.3.3(iii)]</td>
<td>NO</td>
<td><strong>SGA 3</strong> 9.2(xii)]</td>
<td>Proposition 5.2.7(b)</td>
</tr>
<tr>
<td>torus</td>
<td>YES</td>
<td>YES</td>
<td>YES</td>
<td>YES</td>
</tr>
<tr>
<td>unipotent</td>
<td>YES</td>
<td>YES</td>
<td>YES</td>
<td>YES</td>
</tr>
</tbody>
</table>

**TABLE 3. Properties of algebraic groups**

The answers are the same for fppf group schemes over a field, and in this setting, one can add a row for “finite type” with all answers being YES.
Bibliography


[Ax65] James Ax, *A field of cohomological dimension 1 which is not C_1*, Bull. Amer. Math. Soc. 71 (1965), 717. MR0199177 (33 #7326)


[BLR90] Siegfried Bosch, Werner Lütkebohmert, and Michel Raynaud, *Néron models*, Ergebnisse der Mathematik und ihrer Grenzgebiete (3) [Results in Mathematics and Related Areas (3)], vol. 21, Springer-Verlag, Berlin, 1990. MR1045822 (91i:14034)

[92] 279
Har77 Robin Hartshorne, Algebraic geometry, Springer-Verlag, New York, 1977. Graduate Texts in Mathematics, No. 52. MR0463157 (57 #3116)


Hig51 Graham Higman, A finitely generated infinite simple group, J. London Math. Soc. 26 (1951), 61–64. MR0038348 (12,390c)


IM71 V. A. Iskovskikh and Ju. I. Manin, Three-dimensional quartics and counterexamples to the Lüroth problem, Mat. Sb. (N.S.) 86(128) (1971), 140–166 (Russian). MR0291172 (45 #266)


[Kat01] Nicholas M. Katz, Sums of Betti numbers in arbitrary characteristic, Finite Fields Appl. 7 (2001), no. 1, 29–44. Dedicated to Professor Chao Ko on the occasion of his 90th birthday. MR1803934 (2002d:14028)


[Knu83] Finn F. Knudsen, The projectivity of the moduli space of stable curves. III. The line bundles on $M_{g,n}$, and a proof of the projectivity of $\overline{M}_{g,n}$ in characteristic $0$, Math. Scand. 52 (1983), no. 2, 200–212. MR702954


287


[Lan56] Serge Lang, **Algebraic groups over finite fields**, Amer. J. Math. 78 (1956), 555–563. MR0086367 (19,174a)


[Lew52] D. J. Lewis, **Cubic homogeneous polynomials over p-adic number fields**, Ann. of Math. (2) 56 (1952), 473–478. MR0049947 (14,251g)


Index

abelian scheme, 132 133 166
abelian variety, 83 103 127 135 135 137 141 145 147 187 194 202 203 206 221 222 249 262 263 277
adèle ring, 2 46 47 49 52 88 89 139 208
adjoint algebraic group, 125 126 126 138 277
affine algebraic group, 116 135 137
affine morphism, 93
Albanese torsor, 141 149
Albanese variety, 130 131 141 141 149 166
algebraic cycle, 199 200
algebraic group, 111 106 150
quasi-projectivity of, 115
algebraic space, 36 81 82 167
almost simple algebraic group, 126 126 127 139
\(\alpha_p\), 110 118 147 149 187
\(\alpha\)-twisted sheaf, 176
Amitsur’s conjecture, 102
anti-affine algebraic group, 137
Azumaya algebra, 15 14 28 99 101 173 172 175 187 213 216
base extension, 30 34 38 44 45 90 94 103 113 272 277
Betti number, 188 189 192 193 195 195 199
bielliptic surface, 228
birational automorphism group, 85 242
birational invariant, 86 182 233 236 241 243 252 253 264
birational map, 85 101 102 105 182 219 236 238 247
factorization of, 245
birational morphism, 172 244 248 252
factorization of, viii 244
Birch and Swinnerton-Dyer conjecture, 103 134 202 203
Bombieri–Lang conjecture, 263
Borel–Serre theorem
  global, 146 169
  local, 145 170 221
Brauer evaluation, 209 211 212 214 233
Brauer group, 1 18 14 28 99 102 105 151 152 172 174 170 176
  algebraic part of, 179 184
  Azumaya, 174 174 176 182
  birational invariance of, 182
  cohomological, 172 172 173
  counterexamples, 172 176 181 182 187
  of a \(C_1\) field, 22 181
  of a complete intersection, 232
  of a curve, 183 187
  of a del Pezzo surface, 233 253
  of a discrete valuation ring, 180 183 187 210
  of a finite field, 23 149 183
  of a function field, 23 25 28 182
  of a global field, 20 24 100
  of a Laurent series field, 181
  of a limit, 27 160 173
  of a local field, 20 23
  of a maximal abelian extension, 28
  of a perfect field, 28
  of a projective space, 184
  of a proper \(Z\)-scheme, 183
  of a quadric, 185 187
  of a quadric bundle, 185 186
  of a rational variety, 184
  of a regular integral scheme, 172 181 182
  of a ring of \(S\)-integers, 183 187
of a singular variety, 176, 187
of a surface over a finite field, 183, 202, 203
of an adèle ring, 209
spreading out, 173, 210
Brauer set, 209, 210, 226
Brauer–Manin obstruction, 210, 216, 225
effectivity of, 216
for a rationally connected variety, 243
insufficiency of, 227–232
to weak approximation, 212, 215, 233, 261

$C_1$ field, 3, 7, 11, 22, 23, 26, 181
$C_r$ field, 3, 11, 7
counterexamples, 6, 23, 26
examples, 5, 6
for non-integral $r$, 6, 25
transition theorems for, 4, 5, 26
$C'_r$ field, 7, 26
canonical ring, 235
Čech cohomology, 145, 146, 158, 162, 163, 165, 167, 170, 171, 219
center
of a group scheme, 114
of a reductive group, 123
of a semisimple group, 123
central isogeny, 124, 125
centralizer of a subgroup scheme, 114
Chabauty’s method, 218
character group, 120, 120, 122, 148, 149
Châtelet surface, 213, 215, 228
Chevalley–Warning theorem, 5, 23, 26
Chow group, 200, 201
class field theory, 25, 180, 268
classification of surfaces, 244, 251
closed point, 42, 42, 44, 50, 56, 190
cocharacter group, 148
Cohen structure theorem, 78
cohomological dimension, 11, 11, 11, 14, 22, 23, 27, 28
examples, 14
of a global field, 14, 180
of a local field, 14
strict, 12, 11, 14, 180
transition theorems for, 12, 14
cohomology with compact support, 199, 201, 204
commutator subgroup of an algebraic group, 122
comparison of Azumaya and cohomological Brauer groups, 172, 174, 176
comparison of Brauer–Manin and descent obstructions, 225, 226
comparison of étale and fppf cohomologies, 170, 172
comparison of étale and Galois cohomologies, 151, 161, 162
comparison of étale and singular cohomologies, 171, 172, 193, 199
comparison of étale and topological fundamental groups, 72
comparison of étale and Zariski cohomologies, 170, 176
comparison of étale-Brauer and descent obstructions, 227
complete intersection, 232, 260
complex analytic space, 46, 63, 69, 72
complex manifold, 63, 64, 151
component group of an algebraic group, 135, 221
composition series, 113, 117, 118
conic, 187, 212, 252, 255, 259
conic bundle, 88, 213, 215, 250, 251
connected component of a group scheme, 111, 115, 136, 136, 168
constant field
of a (−1) curve, 244
of a function field, 34
constructible scheme, 62
contracted product, 143, 167
contractible curve on a surface, 244, 245, 246
Cremona group, 85
curve, 30, 43, 45, 244
cohomology of a, 152, 187, 189
of genus 0, 99, 105, 256
of genus 1, 141, 145, 218, 233, 234
of genus > 1, 147, 261, 263
cycle class homomorphism, 201, 199, 203
cyclic algebra, 21, 20, 25, 27, 28, 174
cyclotomic character, 195
Dedekind domain, 57, 58, 60, 83, 89
Dedekind scheme, 57, 57, 59, 83, 132, 248
degree of a closed point, 43
degree of a Fano variety, 241, 251
degree of a morphism, 85, 87
del Pezzo surface, 251, 250–261
  of degree 1, 254, 260–261
  of degree 2, 254, 260
  of degree 3, 260
  of degree 4, 233, 259, 260
  of degree 5, 257, 257, 259, 264
  of degree 6, 256, 257
  of degree 7, 256, 257
  of degree 8, 254, 256, 257
  of degree 9, 254, 256
Demyanenko–Manin method, 218
descent
fpqc, 90, 105, 113, 156
  for algebraic groups, 115, 276
  for properties of morphisms, 91, 104, 164, 170, 179
  186, 272, 273, 275
  for quasi-coherent sheaves, 92, 157, 171, 174
  200
  for schemes, 93, 157, 166, 168, 200
Galois, 9, 10, 19, 50, 94, 97, 122, 166
  generalizations of Fermat’s method of infinite descent, 209, 216, 225, 233
  descent datum, 92
  descent obstruction, 225, 224, 227
  insufficiency of, 228, 232
dimension, 60
  dimension ≤ 1, 22, 23, 28, 144, 253, 257
diophantine approximation, 262
discrete valuation ring or field, 81, 164, 170, 179
  186, 272, 273, 275
flat module, 59, 59–60
flat morphism, 60, 275
formally real field, 6, 13, 268, 269
formally smooth morphism, 76, 275
fpfp cohomology, 19, 99, 143, 146, 160, 184
fpfp morphism, 61, 88, 89, 91, 154, 272, 275
fpqc morphism, 62, 88, 89, 91, 154, 272, 275
  that is not fpfp, 89
free rational curve, 239
Frobenius automorphism, 134, 144, 196, 197
Frobenius morphism, 86, 87, 192, 204, 262
  of a group scheme, 110, 114, 115, 123, 140, 144
<table>
<thead>
<tr>
<th>Term</th>
<th>Pages</th>
</tr>
</thead>
<tbody>
<tr>
<td>function field of a variety</td>
<td>32, 32, 34, 84, 85</td>
</tr>
<tr>
<td>functor of points</td>
<td>35, 35, 36, 52, 82, 83</td>
</tr>
<tr>
<td>is a sheaf</td>
<td>157</td>
</tr>
<tr>
<td>of a group scheme</td>
<td>108, 110, 112, 128, 129</td>
</tr>
<tr>
<td>fundamental group</td>
<td>71, 72, 71, 73, 232</td>
</tr>
<tr>
<td>of a normal scheme</td>
<td>75</td>
</tr>
<tr>
<td>variety with prescribed</td>
<td></td>
</tr>
<tr>
<td>G-unramified morphism</td>
<td>69, 69, 77, 275</td>
</tr>
<tr>
<td>GAGA</td>
<td>46</td>
</tr>
<tr>
<td>Galois cohomology</td>
<td>10, 11, 18, 19, 21, 22, 26, 151</td>
</tr>
<tr>
<td>Galois étale algebra</td>
<td>8</td>
</tr>
<tr>
<td>Galois theory</td>
<td>7, 11</td>
</tr>
<tr>
<td>gamma function</td>
<td>190</td>
</tr>
<tr>
<td>general type</td>
<td>236, 249</td>
</tr>
<tr>
<td>genus</td>
<td>44</td>
</tr>
<tr>
<td>change under field extension</td>
<td>44, 45</td>
</tr>
<tr>
<td>geometric point</td>
<td>72</td>
</tr>
<tr>
<td>geometrically connected variety</td>
<td>31, 31, 41, 49, 78</td>
</tr>
<tr>
<td></td>
<td>79, 112, 128, 130, 144, 275</td>
</tr>
<tr>
<td>geometrically integral variety</td>
<td>2, 31, 32, 33, 37, 41</td>
</tr>
<tr>
<td></td>
<td>42, 44, 45, 50, 62, 75, 76, 78, 89, 104, 128</td>
</tr>
<tr>
<td></td>
<td>130, 141, 149, 180, 185, 187, 203, 204, 212</td>
</tr>
<tr>
<td></td>
<td>223, 224, 229, 231, 230, 241, 262, 263, 270</td>
</tr>
<tr>
<td></td>
<td>273, 275</td>
</tr>
<tr>
<td>geometrically irreducible variety</td>
<td>31, 31, 33, 41, 76</td>
</tr>
<tr>
<td></td>
<td>112, 188, 192, 203, 203, 206, 275</td>
</tr>
<tr>
<td>geometrically reduced variety</td>
<td>31, 31, 41, 42</td>
</tr>
<tr>
<td></td>
<td>49, 78, 79, 114, 129, 246, 250, 273, 275</td>
</tr>
<tr>
<td>geometrically regular variety</td>
<td>31, 31, 32, 34, 49</td>
</tr>
<tr>
<td></td>
<td>64, 66, 68, 78</td>
</tr>
<tr>
<td>global field</td>
<td>8, 2, 24, 25, 47, 50, 133, 135</td>
</tr>
<tr>
<td></td>
<td>138, 139, 146, 147, 203, 204, 208, 234, 253, 263</td>
</tr>
<tr>
<td>global function field</td>
<td>2, 47, 158, 146, 147, 202, 203</td>
</tr>
<tr>
<td></td>
<td>202, 203</td>
</tr>
<tr>
<td>good reduction</td>
<td>81, 81, 82, 89, 132, 133</td>
</tr>
<tr>
<td>Grassmannian</td>
<td>237, 258</td>
</tr>
<tr>
<td>Greenberg transform</td>
<td>104, 104</td>
</tr>
<tr>
<td>Grothendieck topology</td>
<td>153, 152, 155</td>
</tr>
<tr>
<td>group object</td>
<td>107</td>
</tr>
<tr>
<td>group scheme</td>
<td>10, 83, 107, 106, 111, 158</td>
</tr>
<tr>
<td>additive</td>
<td>109, 109, 110, 117, 119, 138, 147, 149</td>
</tr>
<tr>
<td></td>
<td>158, 276</td>
</tr>
<tr>
<td>constant</td>
<td>109, 118, 119, 141</td>
</tr>
<tr>
<td>finite étale</td>
<td>135, 136</td>
</tr>
<tr>
<td>fppf</td>
<td>110, 110, 115</td>
</tr>
<tr>
<td>multiplicative</td>
<td>109, 109, 110, 119, 121, 123, 132</td>
</tr>
<tr>
<td></td>
<td>147, 148, 158, 165, 170, 171, 186</td>
</tr>
<tr>
<td>of multiplicative type</td>
<td>121</td>
</tr>
<tr>
<td>of order $p$</td>
<td>147</td>
</tr>
<tr>
<td>over the ring of dual numbers</td>
<td>116</td>
</tr>
<tr>
<td>Grunwald–Wang theorem</td>
<td>25</td>
</tr>
<tr>
<td>Hasse–Weil bound</td>
<td>143, 189, 233</td>
</tr>
<tr>
<td>height of a rational point</td>
<td>48, 134</td>
</tr>
<tr>
<td>Hensel’s lemma</td>
<td>77, 169, 204, 214, 223, 269</td>
</tr>
<tr>
<td>henselian local ring or field</td>
<td>6, 183, 211, 269, 270</td>
</tr>
<tr>
<td>Hermite’s finiteness theorem</td>
<td>viii, 170</td>
</tr>
<tr>
<td>Hilbert irreducibility theorem</td>
<td>270</td>
</tr>
<tr>
<td>Hilbert’s tenth problem</td>
<td>40, 47</td>
</tr>
<tr>
<td>Hilbert’s theorem 90</td>
<td>10, 11, 19, 26, 171, 180</td>
</tr>
<tr>
<td>hibertian field</td>
<td>270, 271</td>
</tr>
<tr>
<td>Hirzebruch surface</td>
<td>237, 248, 251</td>
</tr>
<tr>
<td>Hodge conjecture</td>
<td>201, 202, 243</td>
</tr>
<tr>
<td>Hodge structure</td>
<td>148</td>
</tr>
<tr>
<td>homogeneous space</td>
<td>viii, 112, 115, 140, 141, 149</td>
</tr>
<tr>
<td>Hopf algebra</td>
<td>107</td>
</tr>
<tr>
<td>hyperbolic variety</td>
<td>232</td>
</tr>
<tr>
<td>hyperelliptic or superelliptic curve</td>
<td>104</td>
</tr>
<tr>
<td>hypersurface</td>
<td>6, 185, 192, 232, 241, 243, 264</td>
</tr>
<tr>
<td>imperfect field</td>
<td>25, 31, 45, 62, 67, 78, 79, 105</td>
</tr>
<tr>
<td></td>
<td>180, 182, 186</td>
</tr>
<tr>
<td>group scheme over an</td>
<td>137, 138, 147</td>
</tr>
<tr>
<td>index of an Azumaya algebra</td>
<td>20, 23, 25</td>
</tr>
<tr>
<td>induced module</td>
<td>12</td>
</tr>
<tr>
<td>infinitesimal lifting property</td>
<td>76, 76, 78</td>
</tr>
<tr>
<td>inflation-restriction sequence</td>
<td>19, 170, 179</td>
</tr>
<tr>
<td>inner twist</td>
<td>139, 143, 146, 167</td>
</tr>
<tr>
<td>integral scheme</td>
<td>29</td>
</tr>
<tr>
<td>intermediate Jacobian</td>
<td>242</td>
</tr>
<tr>
<td>isogeny between connected algebraic groups</td>
<td>124</td>
</tr>
<tr>
<td>isotrivial variety</td>
<td>263</td>
</tr>
<tr>
<td>Jacobian variety</td>
<td>128, 128, 130, 141, 145, 203, 218</td>
</tr>
<tr>
<td>jet</td>
<td>77</td>
</tr>
</tbody>
</table>
jet space, 104
K3 surface, 48, 81, 249
Kodaira dimension, 235, 237, 248, 249
Krasner’s lemma, 80, 81, 221, 223
Kronecker–Weber theorem, 7
L-function, 134, 135, 235, 237–249
Lang’s conjecture for a hyperbolic variety, 232
Lang–Nishimura theorem, viii, 85–86, 89, 99, 256
Lang–Weil theorem, 203, 206
Laurent series, ix, 1, 6, 28, 36, 85, 86, 181, 268
Lefschetz trace formula for a non-proper variety, 199, 204
in étale cohomology, 196, 198, 251
in topology, 192, 193
linear recursive sequence, 206
local coordinates, 64, 73, 78
local field, 1, 2, 6, 14, 20, 23, 25, 40, 46, 79, 81
145, 146, 183, 204, 205, 211, 220, 221, 269, 271
higher-dimensional, 268
local-global principle, 48, 208, 210, 212, 214, 216
225, 228, 256
for a Châtelet surface, 215
for a del Pezzo surface, 253, 254, 256, 260, 261
for a hypersurface, 232
for a rationally connected variety, 213
for a Severi–Brauer variety, 100, 254, 257
for a torsor, 146, 147
locally integral scheme, 58
locally of finite presentation morphism, 52, 53, 61
275
maximal abelian extension, 7, 28
maximal unramified extension, 6, 70, 181, 269
Merkurjev–Suslin theorem, 23
Minchev’s theorem on strong approximation, viii
223, 224
minimal regular proper model, 82, 83, 133, 248
minimal surface, 246, 246, 248, 250
moduli space, 36, 38, 237
coarse, 37, 38, 50, 249
fine, 36, 38, 50
of curves, 37
of curves with marked points, 37, 38, 257, 259
Mordell–Weil theorem, 134, 222
μ_n, 110, 111, 118, 121, 123, 126, 147, 148
174, 176, 186, 187, 193, 200
nef, 248, 248, 250
Néron model, 82, 83
of an abelian variety, 132
of an elliptic curve, 133
nice variety, 78
noetherian hypothesis, 51, 52, 55, 273
norm form, 3, 22, 26
normalizer of a subgroup scheme, 114
number field, 2, 6, 20, 27, 48, 138, 139, 146, 147
168, 170, 180, 204, 215, 221, 223, 227, 232
234, 243, 261, 263
numerical equivalence, 248, 250
opposite category, ix
order of a group scheme, 109
PAC field, 7, 270, 271
perfect closure, 1, 25
period of an Azumaya algebra, 20, 23, 25
Picard number, 250
Picard scheme, 129, 130
Picard variety, 130, 131
Poincaré duality
for a non-proper variety, 199, 201
in ℓ-adic cohomology, 196
in topology, 194
polynomial ring, ix, 51
potential density, 48
power series ring, 28, 78, 85, 86, 89, 181
presheaf, 155
primary extension of fields, 33, 34, 41, 186
pseudo-morphism, 84
pseudo-reductive algebraic group, 137, 145, 149
pseudo-semisimple algebraic group, 137
purity conjecture, 181
quadric, 185
quadric bundle, 185, 228, 231
quasi-affine morphism, 93, 93, 94, 97, 275
<table>
<thead>
<tr>
<th>Term</th>
<th>Page(s)</th>
</tr>
</thead>
<tbody>
<tr>
<td>quasi-compact morphism or scheme</td>
<td>52, 275</td>
</tr>
<tr>
<td>quasi-separated morphism or scheme</td>
<td>52, 275</td>
</tr>
<tr>
<td>quaternion algebra</td>
<td>16, 17, 20, 22, 27, 28, 213</td>
</tr>
<tr>
<td>quotient of group schemes</td>
<td>110–111, 112–114, 276</td>
</tr>
<tr>
<td>radical of an algebraic group</td>
<td>122–123, 136, 137</td>
</tr>
<tr>
<td>rational equivalence</td>
<td>200, 201</td>
</tr>
<tr>
<td>rational function field</td>
<td>1x, 4, 4, 24, 26, 28, 105</td>
</tr>
<tr>
<td>rational map</td>
<td>83–86, 89, 100, 102, 132, 184, 235, 239, 256</td>
</tr>
<tr>
<td>rational surface</td>
<td>237, 239, 256</td>
</tr>
<tr>
<td>cohomology of a</td>
<td>238</td>
</tr>
<tr>
<td>number of points on a</td>
<td>251</td>
</tr>
<tr>
<td>rational variety</td>
<td>45, 63, 99, 121, 148, 184, 237</td>
</tr>
<tr>
<td>in a family</td>
<td>237, 238, 242, 243, 243</td>
</tr>
<tr>
<td>rationally chain connected variety</td>
<td>0, 240, 243</td>
</tr>
<tr>
<td>rationally connected variety</td>
<td>238, 239, 241</td>
</tr>
<tr>
<td>real approximation theorem</td>
<td>138, 149</td>
</tr>
<tr>
<td>real closed field</td>
<td>268, 269</td>
</tr>
<tr>
<td>reduced norm</td>
<td>17, 27</td>
</tr>
<tr>
<td>reduced subscheme of a group scheme</td>
<td>149</td>
</tr>
<tr>
<td>reduced trace</td>
<td>17, 27</td>
</tr>
<tr>
<td>reductive algebraic group</td>
<td>123, 124, 127, 136, 143, 277</td>
</tr>
<tr>
<td>regular scheme</td>
<td>31, 32, 34, 43, 45, 49, 58, 62, 62, 63, 66, 67, 73, 82, 84, 89, 133, 172, 176</td>
</tr>
<tr>
<td>relative dimension</td>
<td>61, 65, 66, 70, 73</td>
</tr>
<tr>
<td>relative Picard functor</td>
<td>129, 130</td>
</tr>
<tr>
<td>representable functor</td>
<td>36, 36, 38, 46, 49, 50, 52</td>
</tr>
<tr>
<td>residue homomorphism</td>
<td>170, 180, 182, 185, 187</td>
</tr>
<tr>
<td>resolution of singularities</td>
<td>32, 82, 236</td>
</tr>
<tr>
<td>restricted product</td>
<td>1x, 2, 4, 49</td>
</tr>
<tr>
<td>restriction of scalars</td>
<td>102, 104, 105, 120, 127, 148</td>
</tr>
<tr>
<td>inseparable</td>
<td>105</td>
</tr>
<tr>
<td>Riemann existence theorem</td>
<td>72, 72</td>
</tr>
<tr>
<td>Riemann hypothesis</td>
<td>190</td>
</tr>
<tr>
<td>for a curve over a finite field</td>
<td>192</td>
</tr>
<tr>
<td>for a variety over a finite field</td>
<td>188, 192, 192</td>
</tr>
<tr>
<td>Riemann–Roch theorem</td>
<td>44, 45, 50, 145, 236, 236, 237, 238, 239, 243</td>
</tr>
<tr>
<td>ruled surface</td>
<td>248, 250, 251</td>
</tr>
<tr>
<td>ruled variety</td>
<td>238, 239, 243</td>
</tr>
<tr>
<td>scheme-theoretically dominant</td>
<td>40, 50</td>
</tr>
<tr>
<td>scheme-valued points</td>
<td>35, 34, 42</td>
</tr>
<tr>
<td>Shafarevich's hypothesis</td>
<td>215</td>
</tr>
<tr>
<td>Shafarevich group</td>
<td>221</td>
</tr>
<tr>
<td>Selmer set</td>
<td>221, 222, 224</td>
</tr>
<tr>
<td>set theory</td>
<td>15, 16, 153, 158, 159, 159, 225, 237</td>
</tr>
<tr>
<td>Shafarevich conjecture</td>
<td>261</td>
</tr>
<tr>
<td>Shafarevich–Tate group</td>
<td>134, 202, 203</td>
</tr>
<tr>
<td>Shapiro's lemma</td>
<td>12, 13, 185, 255</td>
</tr>
<tr>
<td>sheaf</td>
<td>156, 155, 159</td>
</tr>
<tr>
<td>sheafification</td>
<td>112, 129, 158, 159, 159</td>
</tr>
<tr>
<td>sieve</td>
<td>153</td>
</tr>
<tr>
<td>simply connected algebraic group</td>
<td>viii, 124</td>
</tr>
<tr>
<td>simply connected scheme</td>
<td>124, 127, 138, 139, 145, 147, 277</td>
</tr>
<tr>
<td>simply connected scheme</td>
<td>124, 127, 138, 139, 145, 147, 277</td>
</tr>
<tr>
<td>singular cohomology</td>
<td>151, 152, 189, 192, 194, 199</td>
</tr>
<tr>
<td>site</td>
<td>153, 155</td>
</tr>
<tr>
<td>Skolem–Mahler–Lech theorem</td>
<td>207</td>
</tr>
<tr>
<td>Skolem–Noether theorem</td>
<td>16</td>
</tr>
<tr>
<td>small category</td>
<td>267</td>
</tr>
<tr>
<td>smooth group scheme</td>
<td>83, 111, 114, 115, 133</td>
</tr>
<tr>
<td>smooth locus</td>
<td>66, 78, 83, 113, 133, 204, 223</td>
</tr>
<tr>
<td>smooth morphism</td>
<td>65, 68, 76, 62, 83, 275</td>
</tr>
<tr>
<td>smooth vs. regular</td>
<td>62, 63, 66, 67</td>
</tr>
<tr>
<td>solvable algebraic group</td>
<td>122, 122, 123, 136, 277</td>
</tr>
</tbody>
</table>
specialization. 55, 56, 118, 199, 270
spectral sequence, 176, 180
Hochschild–Serre, 118, 178, 199, 270
of Čech cohomology, 163
spreading out, 53, 210
of Čech cohomology, 163
stably birational varieties, 102, 105
stably rational variety, 237, 242
stack, 37
standard étale morphism, 70, 79
strictly henselian local ring or field, 269
strong approximation, viii, 49, 89, 223–224
in an algebraic group, 139
strongly inaccessible cardinal, 266
Tate class, 202
Tate conjecture, 202, 203
Tate module, 134, 194
Tate twist, 195, 196
of an elliptic curve, 104
of \( G_a \), 117
unirational variety, 237, 238, 243, 254, 259, 261
that is not rational, 242–243
uniruled variety, 238, 239, 242
universe, 8
unramified cohomology class, 168
unramified cohomology group of a function field, 243
unramified morphism, 68–69
unramified torsor, 168
valuative criterion for properness, 58–59
vectorial group, 117
very free rational curve, 239
weak approximation, 48, 49, 50, 89, 209, 212, 215
weak Lefschetz theorem, 232
weak Mordell–Weil theorem, 134
Wedderburn’s theorem on finite division rings, 23
Weil conjectures, 188
Wedderburn’s theorem on semisimple algebras, 15
Weierstrass model, 105
Weil conjectures, 188, 191
Witt vector, 104, 118
Yoneda’s lemma, 36, 82, 83
Zariski open covering morphism, 62, 88, 89
Zariski’s main theorem, 71, 74
zeta function, 189, 192
convergence of, 191
Dedekind, 191
of a scheme of finite type over a finite field, 191
of a scheme of finite type over \( \mathbb{Z} \), 190
Riemann, 189–190

Tate class, 202
Tate module, 134, 194
Tate twist, 195, 196
operations on a, 142–143
over a finite field, 144–145
over a local field, 145
under a torus, 141, 149–152
under \( \alpha_p \), 187
under \( \mu_n \), 174
Torsor, 108, 139–140, 139, 141–147
over a finite field, 144
over a local field, 145
under a torus, 141, 149–152
under \( \alpha_p \), 187
Torsor sheaf, 165, 165
Torsor, 120, 119, 123–127
rationality of a, 121
Transcendence degree, 14
Transcendence basis, 14
Transcendence degree, 15
Tsen’s theorem, 5, 23
Twist, 15, 149, 138–143
of an elliptic curve, 104
of \( G_a \), 117
Unipotent group, 117
Unipotent radical, 122