Lectures on rational points on curves

March 5, 2006 version

Bjorn Poonen

Department of Mathematics, University of California, Berkeley, CA 94720-3840, USA

E-mail address: `poonen@math.berkeley.edu`

URL: `http://math.berkeley.edu/~poonen`

This research was supported by NSF grant DMS-0301280 and the Miller Institute for Basic Research in Science.

Contents

CHAPTER 0

Introduction

The main goal of these notes is to explain how to answer questions like “What are the rational number solutions to $x^4 + y^4 = 17$?”

☡ WARNING 0.0.1. These notes are not yet finished, and what is written is only a first draft. Read them at your own risk! If you see ♣♣♣ Bjorn: [], that means that it hasn't been written or fixed up yet.

0.1. Notation

Let $\operatorname{char} k$ denote the characteristic of a field k. By a global field k, we mean a number field (finite extension of $\mathbb{Q}$) or a global function field (finite extension of $\mathbb{F}_q(t)$ for some finite field $\mathbb{F}_q$). A local field is the completion k_v of a global field k with respect to some place v.

CHAPTER 1

Varieties over perfect fields

Let k be a perfect field. Fix an algebraic closure $\overline{k}$. Let $G = G_k$ be the profinite group $\operatorname{Gal}(\overline{k}/k)$.

Remark 1.0.1. Much of what we say remains true for imperfect fields k if we replace $\overline{k}$ by a separable closure k^{s} of k and define $G_k = \operatorname{Gal}(k^{\mathrm{s}}/k)$. At various points in these notes, we will indicate how things are different over imperfect fields.

We will keep our terminology compatible with the language of schemes, even though we try to keep the exposition down-to-earth whenever possible. Our exposition in this chapter is intended not as a thorough introduction to algebraic geometry, but rather as a review, with particular attention to issues that arise when working over perfect fields that are not algebraically closed.

Definition 1.0.2. Officially, a k-variety is a separated scheme X of finite type over k. Do not worry if you do not know what this means: for most of our purposes, it is enough to know its set $X(L)$ of L-rational points for each field extension $L \supseteq k$, and this set can be defined in down-to-earth terms. For most of these notes, it will be OK to think of a k-variety as the set $X(\overline{k})$ in some ambient affine or projective space.

Warning 1.0.3. Our varieties need not be irreducible or reduced: see Section 1.4.

1.1. Affine varieties

If $n \in \mathbb{Z}_{\geq 0}$, define n-dimensional affine space over k as

$$\mathbb{A}^n = \mathbb{A}^n_k := \operatorname{Spec} k[t_1, \ldots, t_n].$$

If you do not know what Spec means, just remember that $\mathbb{A}^n(L) = L^n$ for each field extension $L \supseteq k$, or even for any k-algebra L.

Definition 1.1.1. An affine k-variety is a subscheme $X = \operatorname{Spec} k[t_1, \ldots, t_n]/I \subseteq \mathbb{A}^n_k$ for some $n \in \mathbb{Z}_{\geq 0}$ and some ideal $I \subseteq k[t_1, \ldots, t_n]$. Affine k-varieties are also called closed k-subvarieties of $\mathbb{A}^n$. Concretely, if $\vec{f} = (f_1, \ldots, f_m)$ is a sequence of generators of the ideal I, and L is any k-algebra, then

$$X(L) = \{\, \vec{a} \in L^n : \vec{f}(\vec{a}) = 0 \,\}.$$

The k-algebra $k[t_1, \ldots, t_n]/I$ is called the affine coordinate ring of X.

Two affine varieties in $\mathbb{A}^n_k$ are considered the same if they are defined using the same k, the same n, and the same ideal I of $k[t_1, \ldots, t_n]$. We will sometimes use variable names other than $t_1, \ldots, t_n$.

EXAMPLES 1.1.2.

(1) Let X be the $\mathbb{R}$-variety $x^2 + y^2 = -1$ in $\mathbb{A}^2_{\mathbb{R}}$; i.e. $X = \operatorname{Spec} \mathbb{R}[x, y]/(x^2 + y^2 + 1)$. Let Y be the $\mathbb{R}$-variety $1 = 0$ in $\mathbb{A}^2_{\mathbb{R}}$. Then $X(\mathbb{R}) = Y(\mathbb{R})$, but X and Y are not the same since the ideals $(x^2 + y^2 + 1)$ and (1) of $\mathbb{R}[x, y]$ are not the same. Another way to see that X and Y are different is to observe that $X(\mathbb{C})$ is nonempty, while $Y(\mathbb{C})$ is empty.

(2) Let X be as above, and let Z be the $\mathbb{C}$-variety $x^2 + y^2 = -1$ in $\mathbb{A}^2_{\mathbb{C}}$. Then X and Z are different. A variety always comes equipped with a ground field. But see Section 1.3.

(3) Let S be the $\mathbb{C}$-variety $\operatorname{Spec} \mathbb{C}[x]/(x^2)$ in $\mathbb{A}^1_{\mathbb{C}}$, and let T be the $\mathbb{C}$-variety $\operatorname{Spec} \mathbb{C}[x]/(x)$ in $\mathbb{A}^1_{\mathbb{C}}$. Then S and T are different, since the ideals (x^2) and (x) of $\mathbb{C}[x]$ are different, even though $S(L) = T(L)$ for every field extension $L \supseteq \mathbb{C}$. We can see the difference by taking $L = k[\epsilon]/(\epsilon^2)$.

Suppose X and X' are two affine k-varieties in $\mathbb{A}^n$. It follows from the Nullstellensatz that $X(\overline{k}) = X'(\overline{k})$ if and only if the corresponding ideals of $k[t_1, \ldots, t_n]$ have the same radical. If one is willing to restrict attention to affine varieties X defined by radical ideals, and one does not care about preserving the field k as part of the data defining X, then one can use the subset $X(\overline{k})$ of $\overline{k}^n$ as a stand-in for X. Thus we have some reconciliation with the elementary approach to algebraic geometry in which affine varieties are defined as subsets of $\overline{k}^n$.

DEFINITION 1.1.3. A hypersurface in $\mathbb{A}^n$ is a closed subvariety defined by a single nonzero polynomial.

DEFINITION 1.1.4. An affine variety is reduced if its defining ideal I is radical, or equivalently if its affine coordinate ring is reduced, meaning that it has no nonzero nilpotent elements.

1.2. Projective varieties

1.2.1. Definition of projective varieties. If $n \in \mathbb{Z}_{\geq 0}$, define n-dimensional projective space over k as

$$\mathbb{P}^n = \mathbb{P}^n_k := \operatorname{Proj} k[t_0, \dots, t_n],$$

where $k[t_0, \dots, t_n]$ has the grading in which $\deg t_i = 1$ for all i. If you do not know what Proj means, just remember that for each field extension $L \supseteq k$,

$$\mathbb{P}^n(L) = \frac{L^{n+1} - \{\vec{0}\}}{L^\times}, \tag{1.2.1}$$

where $\vec{0} = (0, \dots, 0) \in L^{n+1}$ and $\lambda \in L^\times$ acts on $(a_0, \dots, a_n) \in L^{n+1} - \{\vec{0}\}$ by mapping it to $(\lambda a_0, \dots, \lambda a_n)$. If $(a_0, \dots, a_n) \in L^{n+1} - \{\vec{0}\}$, let $(a_0 : \dots : a_n)$ be the corresponding point of $\mathbb{P}^n(L)$.

WARNING 1.2.2. Whereas $\mathbb{A}^n(L) = L^n$ was valid for any k-algebra L, (1.2.1) should be used only for fields L. The right way to define $\mathbb{P}^n(L)$ for a k-algebra L is as the set of morphisms of k-schemes $\operatorname{Spec} L \to \mathbb{P}^n_k$, but then (1.2.1) may be wrong if L is not a field.

DEFINITION 1.2.3. A projective k-variety is a subscheme $X = \operatorname{Proj} k[t_0, \dots, t_n]/I \subseteq \mathbb{P}^n_k$ for some $n \in \mathbb{Z}_{\geq 0}$ and some homogeneous ideal $I \subseteq k[t_0, \dots, t_n]$. Projective k-varieties are also called closed k-subvarieties of $\mathbb{P}^n$. Concretely, if $\vec{f} = (f_1, \dots, f_m)$ is a sequence of homogeneous polynomials generating the ideal I, and $L \supseteq k$ is any field extension, then

$$X(L) = \frac{\{\, \vec{a} \in L^{n+1} - \{\vec{0}\} : \vec{f}(\vec{a}) = 0 \,\}}{L^\times}.$$

DEFINITION 1.2.4. For any k-variety X and any field extension $L \supseteq k$, an element of $X(L)$ is called an L-rational point, or simply an L-point.

DEFINITION 1.2.5. A hypersurface in $\mathbb{P}^n$ is a closed subvariety defined by a single nonzero homogeneous polynomial. The degree of the hypersurface is the degree of the polynomial.

REMARK 1.2.6. More generally, one could define the notion of quasi-projective variety: a variety of the form $X - Y$ where X and Y are projective varieties with $Y \subseteq X \subseteq \mathbb{P}^n$.

1.2.2. Affine patches. Let H_i be the hyperplane $x_i = 0$ in $\mathbb{P}^n$; i.e., $\operatorname{Proj} k[t_0, \dots, t_n]/(t_i)$. We have an isomorphism

$$\begin{aligned} \phi_i \colon \mathbb{A}^n &\to \mathbb{P}^n - H_i \\ (a_0, \dots, a_{i-1}, a_{i+1}, \dots, a_n) &\mapsto (a_0 : \dots : a_{i-1} : 1 : a_{i+1} : \dots : a_n). \end{aligned}$$

The $\phi_i(\mathbb{A}^n)$ form the standard open covering of $\mathbb{P}^n$ by $n+1$ affine spaces: one says that "$\mathbb{P}^n$ is obtained by glueing $n+1$ copies of $\mathbb{A}^n$." Similarly any projective k-variety $X \subseteq \mathbb{P}^n$ has an open covering by $n+1$ affine varieties of the form $X_i := X \cap \phi_i(\mathbb{A}^n) \subseteq \phi_i(\mathbb{A}^n) \simeq \mathbb{A}^n$. These X_i are the standard affine patches of X.

Definition 1.2.7. A projective variety is reduced if and only if all its affine patches are reduced.

If X and Y are reduced subvarieties of $\mathbb{A}^n$ or $\mathbb{P}^n$, the notation $X \subseteq Y$ means that $X(L) \subseteq Y(L)$ for all field extensions L of k. (In fact, it suffices to check the condition for $L = \overline{k}$.)

1.2.3. Projective closure. Fix $i \in \{0, \ldots, n\}$, and identify $\mathbb{A}^n$ with $\phi_i(\mathbb{A}^n) \subseteq \mathbb{P}^n$. Given a reduced closed k-subvariety $X_0 \subseteq \mathbb{A}^n$, the projective closure of X_0 is the smallest projective variety X in $\mathbb{P}^n$ containing X_0.

We have maps in both directions

$$\{\text{closed } k\text{-subvarieties of } \mathbb{A}^n\} \leftrightarrows \{\text{closed } k\text{-subvarieties of } \mathbb{P}^n\}:$$

namely an X_0 on the left is mapped to its projective closure on the right, and an X on the right is mapped to the i-th affine patch.

☡ Warning 1.2.8. These maps are not quite inverses to each other.

Nevertheless, they do give, for instance, a bijection between the closed integral hypersurfaces in $\mathbb{A}^n$ and the closed integral hypersurfaces in $\mathbb{P}^n$ other than the hyperplane H_0. This bijection and its inverse can be described explicitly in terms of the defining polynomials, namely by homogenization and dehomogenization.

Example 1.2.9. The projective variety

$$X\colon y^2 z = x^3 + 17z^3,$$

in $\mathbb{P}^2_{\mathbb{Q}}$ is the projective closure of its affine patch

$$X_0\colon y^2 = x^3 + 17$$

in $\mathbb{A}^2_{\mathbb{Q}}$ defined by deleting the hyperplane $z = 0$ in $\mathbb{P}^2_{\mathbb{Q}}$.

☡ Warning 1.2.10. For affine varieties defined by more than one equation, one cannot always compute projective closures by blithely homogenizing a set of defining equations.

1.3. Base extension

Let X be a k-variety and let $L \supseteq k$ be an extension of fields. The base extension of X to L is the fiber product

$$X_L = X \underset{k}{\times} L := X \underset{\operatorname{Spec} k}{\times} \operatorname{Spec} L$$

viewed as an L-variety. If

$$X = \operatorname{Spec} A = \operatorname{Spec} \frac{k[t_1, \ldots, t_n]}{(f_1, \ldots, f_m)},$$

then

$$X_L = \operatorname{Spec} A \underset{k}{\otimes} L = \operatorname{Spec} \frac{L[t_1, \ldots, t_n]}{(f_1, \ldots, f_m)}.$$

A similar statement holds for projective varieties. In concrete terms, X_L is defined by the same polynomial equations as X, but the coefficients of these equations are considered to be elements of L.

We will use the abbreviation $\overline{X} = X_{\overline{k}}$.

Definition 1.3.1. Suppose that *blah* is an adjective applicable to k-varieties for any k. One says that a k-variety X is geometrically blah (or absolutely blah) if and only if the $\overline{k}$-variety $\overline{X}$ is blah.

For instance, given a (not necessarily reduced) k-variety X, one can ask whether it is geometrically reduced. Actually, it turns out that the property of being reduced is preserved by base extension to a finite separable extension $L \supseteq k$, so if one is working over a perfect field k, the notions of reduced and geometrically reduced coincide.

Remark 1.3.2. Given a finite extension of fields $L \supseteq k$, there is also an operation called restriction of scalars or Weil restriction that takes a quasi-projective L-variety X and returns a k-variety $\mathscr{X}$ such that $\mathscr{X}(k)$ is naturally in bijection with $X(L)$. ♣♣♣ Bjorn: [Add reference to Néron Models book.]

1.4. Irreducibility

Definition 1.4.1. A k-variety X is irreducible if X is nonempty and it is impossible to write $X = Y_1 \cup Y_2$ where $Y_1, Y_2 \subsetneq X$ are closed k-subvarieties.

One can show that for a reduced finitely generated k-algebra A, the affine k-variety $\operatorname{Spec} A$ is irreducible if and only if A is an integral domain.

Definition 1.4.2. A variety is called integral if it is reduced and irreducible.

Example 1.4.3. Let X be the affine curve $x^2 - 2y^2 = 0$ in $\mathbb{A}^2_{\mathbb{Q}}$. Using properties of the unique factorization domains $\mathbb{Q}[x, y]$ and $\overline{\mathbb{Q}}[x, y]$, one can show that the $\mathbb{Q}$-variety X is integral, while the $\overline{\mathbb{Q}}$-variety $\overline{X}$ is not irreducible. In particular, X is not geometrically irreducible. This example shows that "irreducible" and "geometrically irreducible" are different notions, even over perfect fields. (One can show, however, that they coincide over separably closed fields.)

Definition 1.4.4. Let X be an integral k-variety.

- If X is affine, say $X = \operatorname{Spec} A$, define $\mathbf{k}(X) := \operatorname{Frac}(A)$.
- If X is projective, then any *nonempty* standard affine patch $X \cap \mathbb{A}^n$ is an integral affine variety, and we define $\mathbf{k}(X) := \mathbf{k}(X \cap \mathbb{A}^n)$, which turns out to be independent of the chosen patch.

In both cases, $\mathbf{k}(X)$ is called the function field of X.

Remark 1.4.5. One can also define the function field of a non-reduced irreducible variety by replacing $\operatorname{Frac}(A)$ by $\operatorname{Frac}(A/\sqrt{0})$, where $\sqrt{0}$ is the nilradical of A.

Remark 1.4.6. One can show that, for an irreducible k-variety X,

$$X \text{ is geometrically irreducible} \iff \{\, \alpha \in \mathbf{k}(X) : \alpha \text{ is algebraic over } k \,\} = k.$$

Remark 1.4.7. In Remark 1.4.6 one should replace "algebraic" by "separably algebraic" to get a statement that holds even when k is not perfect.

Definition 1.4.8. Elements of $\mathbf{k}(X)$ are called rational functions on X.

Definition 1.4.9. Suppose $f \in \mathbf{k}(X)$ and $P \in X(\overline{k})$.

- If $X = \operatorname{Spec} A$, then f is defined at P if and only if f can be written as g/h with $g, h \in A$ and $h(P) \neq 0$.
- If X is projective, then f is defined at P if and only if f restricted to some affine patch containing P is defined at P.

1.5. Morphisms and rational maps

1.5.1. Morphisms.

Definition 1.5.1. For those who know what a morphism of schemes is, a morphism of k-varieties $X \to Y$ is a morphism of schemes $X \to Y$ such that

$$\begin{tikzcd}
X \arrow[rr] \arrow[dr] & & Y \arrow[dl] \\
& \operatorname{Spec} k &
\end{tikzcd}$$

commutes.

For alternative, more elementary definitions of morphism, see [Har77, §I.3] or our Section 1.5.3. A morphism of k-varieties is called also a k-morphism.

We get a category

$$\{k\text{-varieties, } k\text{-morphisms}\},$$

and hence can define endomorphism, isomorphism, automorphism, etc.

1.5.2. Rational maps.

Definition 1.5.2. Let X be an integral k-variety, and let Y be any k-variety. A rational map $X \dashrightarrow Y$ is an equivalence class of morphisms $U \to Y$ with U a nonempty open subscheme of X, where two morphisms $U \to Y$ and $U' \to Y$ are considered equivalent if their restriction to $U \cap U'$ agree.

Definition 1.5.3. A rational map $\phi\colon X \to Y$ is dominant if for any representative $U \to Y$, the image is not contained in any closed subset $Y' \subsetneq Y$ (concretely, there should not be any closed subvariety Y' of Y with $Y'(\overline{k}) \subsetneq Y(\overline{k})$ such that the set-theoretic image of $U(\overline{k}) \to Y(\overline{k})$ is contained in $Y'(\overline{k})$).

One can show that there is an equivalence of categories

$$\left\{ \begin{array}{c} \text{integral } k\text{-varieties,} \\ \text{dominant rational maps} \end{array} \right\} \longleftrightarrow \left\{ \begin{array}{c} \text{finitely generated field extensions of } k, \\ k\text{-algebra homomorphisms} \end{array} \right\}^{\mathrm{op}} \tag{1.5.4}$$

taking a variety to its function field. The $^{\mathrm{op}}$ indicates the category with the direction of arrows reversed: if $\pi\colon X \dashrightarrow Y$ is a rational map, we get a k-algebra homomorphism $\mathbf{k}(Y) \to \mathbf{k}(X)$ sending a rational function f on Y to the composition $f \circ \pi$.

Definition 1.5.5. Let X and Y be integral k-varieties. A birational map $X \dashrightarrow Y$ is an "isomorphism" in the category on the left in (1.5.4): in other words, it is a dominant rational map $f\colon X \dashrightarrow Y$ such that there exists a dominant rational $g\colon Y \dashrightarrow X$ such that $f \circ g$ agrees with the identity of Y where defined, and $g \circ f$ agrees with the identity of X where defined.

Definition 1.5.6. Integral k-varieties X and Y are called birational if and only if there exists a birational map between them. Equivalently, X and Y are birational if and only if there is a k-algebra isomorphism $\mathbf{k}(X) \to \mathbf{k}(Y)$.

Warning 1.5.7. By definition, a morphism or rational map between k-varieties is automatically defined over k. A morphism defined by rational functions with coefficients in a field extension $L \supseteq k$ is, in our terminology, a morphism $X_L \to Y_L$.

1.5.3. Explicit rational maps and morphisms. This section shows how to describe rational maps and morphisms concretely. These descriptions could be taken as alternative definitions of the notions.

We build up the description according to the type of the target variety. Let X be an integral k-variety and let $P \in X(\overline{k})$.

Definition 1.5.8.

- A rational map $\phi \colon X \dashrightarrow \mathbb{A}^n_k$ is an n-tuple $(f_1, \ldots, f_n)$ with $f_i \in \mathbf{k}(X)$ for each i. It is defined at P if and only if each f_i is defined at P.
- A rational map $\phi \colon X \dashrightarrow \mathbb{P}^n_k$ is an $(n+1)$-tuple $(f_0, \ldots, f_n)$ with $f_i \in \mathbf{k}(X)$ not all zero, except that for any $g \in \mathbf{k}(X)^\times$, we consider $(gf_0, \ldots, gf_n)$ as defining the same rational map. It is defined at P if and only if there exists $g \in \mathbf{k}(X)^\times$ such that $(gf_0)(P)$, $\ldots$, $(gf_n)(P)$ are all defined and not all zero. In this case and the previous, the image of ϕ is $\{\, \phi(P) : \phi \text{ is defined at } P \,\}$.
- If Y is a k-subvariety of $\mathbb{A}^n_k$ or $\mathbb{P}^n_k$, a rational map $X \dashrightarrow Y$ is a rational map $X \dashrightarrow \mathbb{A}^n_k$ or $X \dashrightarrow \mathbb{P}^n_k$, respectively, such the image is contained in $Y(\overline{k})$.

In terms of this alternative definition of rational map, we can define morphisms as follows:

Definition 1.5.9. Let X be an integral k-variety, and let Y be any affine or projective k-variety. A k-morphism $X \to Y$ is a rational map that is defined at all $P \in X(\overline{k})$.

1.6. Dimension

Definition 1.6.1. The dimension $\dim X$ of a nonempty variety X is the largest $d \in \mathbb{Z}_{\geq 0}$ for which there exists a d-step chain

$$X_0 \subsetneq X_1 \subsetneq \cdots \subsetneq X_d$$

of closed integral subvarieties X_i of X.

Remark 1.6.2. There always is a largest d; i.e., there do not exist arbitrarily long chains in a fixed variety X.

Remark 1.6.3. One usually uses the convention that the empty variety has dimension -1, because one cannot even find an X_0.

One can show the following facts:

- In an irreducible variety, all maximal chains of closed integral subvarieties have the same length. (A chain is maximal if it is impossible to insert any more closed integral subvarieties between varieties in the chain.)
- If X is integral, then $\dim X = \operatorname{trdeg}(\mathbf{k}(X)/k)$, the transcendence degree of $\mathbf{k}(X)$ over k.
- For any k-variety X and field extension $L \supseteq k$, we have $\dim X_L = \dim X$.

♣♣♣ Bjorn: [Add references.]

Definition 1.6.4. If X is an integral k-variety, and Y is a closed subvariety, then the codimension of Y in X is $\dim X - \dim Y$.

1.7. Smooth varieties

Definition 1.7.1.

- Let
$$X = \operatorname{Spec} \frac{k[t_1, \ldots, t_n]}{(f_1, \ldots, f_m)}$$
be an affine variety of dimension d. Let $P \in X(\overline{k})$. Then X is smooth at P if and only if
$$\operatorname{rank} \left(\frac{\partial f_i}{\partial t_j}(P) \right)_{\substack{1 \le i \le m \\ 1 \le j \le n}} = n - d.$$
- For a projective variety X and $P \in X(\overline{k})$, we say that X is smooth at P if and only if some (or equivalently, any) affine patch of X containing P is smooth at P.

We say that X is smooth if X is smooth at every $P \in X(\overline{k})$.

Remark 1.7.2. Suppose we are in the case
$$X = \operatorname{Spec} \frac{k[t_1, \ldots, t_n]}{(f_1, \ldots, f_m)},$$
but instead of assuming $\dim X = d$, we assume that
$$\operatorname{rank} \left(\frac{\partial f_i}{\partial t_j}(P) \right)_{\substack{1 \le i \le m \\ 1 \le j \le n}} = m.$$

Then one can show that X is smooth at P, there is a unique irreducible component of X containing P, and that component has dimension $n - m$.

Remark 1.7.3. One can show that the set of $P \in X(\overline{k})$ such that X is not smooth at P is the set of $\overline{k}$-points of a closed subvariety of X, called the singular locus of X.

Example 1.7.4. If X is a hypersurface $f(t_1, \ldots, t_n) = 0$ in $\mathbb{A}^n$, then the singular locus is defined by

$$\frac{\partial f}{\partial t_1} = \cdots = \frac{\partial f}{\partial t_n} = f = 0.$$

Example 1.7.5. If X is a hypersurface $F(t_0, \ldots, t_n) = 0$ of degree d in $\mathbb{P}^n$, then the singular locus is defined by

$$\frac{\partial F}{\partial t_0} = \cdots = \frac{\partial F}{\partial t_n} = F = 0.$$

If moreover $\operatorname{char} k \nmid d$, then one can omit the condition $F = 0$, because of the Euler relation

$$d \cdot F = \sum_{i=0}^{n} t_i \frac{\partial F}{\partial t_i}.$$

Remark 1.7.6. Smoothness is preserved by base extension.

Remark 1.7.7. One can show that smooth varieties are automatically reduced.

For convenience, we make the following (nonstandard) definition:

Definition 1.7.8. A k-variety X is nice if it is smooth, projective, and geometrically integral.

Because of Remarks 1.7.6 and 1.7.7, the definition of nice is unchanged if we weaken "geometrically integral" to "geometrically irreducible".

Definition 1.7.9. Let k be a field that is complete with respect to a discrete valuation $v \colon k^\times \to \mathbb{Z}$. Let X be a smooth projective variety of dimension d over k. We say that X has good reduction if there exists a smooth model of X over the valuation ring $\mathcal{O} \subseteq k$, i.e., if there exist homogeneous polynomials defining a k-variety isomorphic to X in some $\mathbb{P}^n_k$, such that all the coefficients of these polynomials are in the valuation ring of v and such that reducing all the coefficients modulo the maximal ideal gives equations defining a variety X' that is smooth of dimension d over the residue field.

More generally, suppose k is a field with a discrete valuation v but k is not necessarily complete. (For instance, k might be a number field.) Let k_v be the completion of k at v. Then a smooth projective variety X over k is said to have good reduction at v if the k_v-variety X_{k_v} has good reduction.

WARNING 1.7.10. A very technical point: The existence of a smooth model over the valuation ring of k_v does not imply the existence of a smooth model over the valuation ring of k defined by v.

1.8. Valuations and ramification

1.8.1. Irreducible divisors. Let X be a nice k-variety. (Weaker conditions would suffice, but we do not care, since in our applications we will be able to reduce to the case of nice varieties.)

DEFINITION 1.8.1. An irreducible divisor on X is a closed integral k-subvariety Y of codimension 1 in X.

WARNING 1.8.2. The subvariety Y could become reducible after base extension to $\overline{k}$. For example, if $X = \mathbb{P}^1_{\mathbb{Q}}$ then Y could be the subvariety $x^2 - 2 = 0$ in an affine patch $\mathbb{A}^1_{\mathbb{Q}} \subseteq \mathbb{P}^1_{\mathbb{Q}}$.

1.8.2. Local rings and valuations.

DEFINITION 1.8.3. Suppose Y is an irreducible divisor on a nice k-variety X. The local ring $\mathcal{O}_{X,Y}$ of X along Y (or at Y, in the case where X is a curve and hence $\dim Y = 0$) is the set of $f \in \mathbf{k}(X)$ such that f is defined at some point of $Y(\overline{k})$. In scheme language, this is the stalk of $\mathcal{O}_X$ at the generic point of Y. Hence $\mathcal{O}_{X,Y}$ could be described also as the localization $A_{\mathfrak{p}}$, where A is the affine coordinate ring of an affine patch X_0 of X meeting Y, and $\mathfrak{p}$ is the prime ideal corresponding to the closed integral subvariety $Y \cap X_0$ of X_0.

One can show that $\mathcal{O}_{X,Y}$ is a discrete valuation ring with residue field $\mathbf{k}(Y)$. Let $v_Y \colon \mathbf{k}(X) \to \mathbb{Z} \cup \{\infty\}$ be the valuation. For $f \in \mathbf{k}(X)^\times$, $v_Y(f)$ is called the order of f along Y.

1.8.3. Uniformizers.

DEFINITION 1.8.4. Let $Y \subseteq X$ be as above. An element $t \in \mathbf{k}(X)$ with $v_Y(t) = 1$ is called a uniformizing parameter, or simply a uniformizer.

EXAMPLE 1.8.5. Let C be a nice curve. Let C_0 be an affine patch, defined by $f(x,y) = 0$ in $\mathbb{A}^2$. Suppose $P = (a,b) \in C_0(\overline{k})$. The maximal ideal of $\mathcal{O}_{C,P}$ is generated by $x - a$ and $y - b$, but it must be principal, so in fact one of these generators is redundant. Since C is smooth at P, either $\frac{\partial f}{\partial x}(P) \neq 0$ or $\frac{\partial f}{\partial y}(P) \neq 0$ (possibly both).

We claim that if $\frac{\partial f}{\partial x}(P) \neq 0$, then $y - b \in \mathbf{k}(C)$ is a uniformizer. To prove this, first translate to assume $(a, b) = 0$. Then $f = xg + yh$ for some $g \in k[x, y]$ and $h \in k[y]$ with $g(0, 0) \neq 0$. Now $x = \left(-\frac{h}{g}\right) y \in \mathcal{O}_{C,P} \cdot y$, so the maximal ideal (x, y) of $\mathcal{O}_{C,P}$ is generated by y alone, as desired.

Similarly, if $\frac{\partial f}{\partial y}(P) \neq 0$ then $x - a \in \mathbf{k}(C)$ is a uniformizer.

1.8.4. Ramification. Suppose that $\phi\colon X' \to X$ is a dominant morphism of nice varieties and $\dim X' = \dim X$. Identify $\mathbf{k}(X)$ with a subfield of $\mathbf{k}(X')$. Then $[\mathbf{k}(X') : \mathbf{k}(X)]$ is finite, since $\mathbf{k}(X)$ and $\mathbf{k}(X')$ are finitely generated over k and of the same transcendence degree. Suppose D' is an irreducible divisor of X', and D is an irreducible divisor of X, and $\phi(D') = D$. Then one can show that there exists $e \in \mathbb{Z}_{\geq 1}$ such that $v_{D'}|_{\mathbf{k}(X)^\times} = e v_D$ on $\mathbf{k}(X)^\times$.

Definition 1.8.6. The integer $e = e(D'/D)$ just defined is called the ramification index of ϕ at D'.

Definition 1.8.7. The morphism $X' \to X$ is called unramified at D' if $e(D'/D) = 1$.

1.9. Divisor groups and Picard groups

Let X be a nice k-variety. Our notation for divisor groups and Picard groups will differ from that in [Sil92]: see Warning 1.9.6. Our choice is made so as to be compatible with the standard notation for schemes.

1.9.1. Divisors.

Definition 1.9.1. A divisor on X is a formal sum $D = \sum_Y n_Y Y$ over irreducible divisors Y on X with $n_Y \in \mathbb{Z}$, and $n_Y = 0$ for all but finitely many Y. To match the notation for functions, we define $v_Y(D) := n_Y$. Define

$$\begin{aligned} \operatorname{Div} X &:= \{ \text{ divisors on } X \} \\ &= \text{ the free abelian group on the set of irreducible divisors on } X. \end{aligned}$$

Definition 1.9.2. If $D_1 = \sum n_Y Y$ and $D_2 = \sum m_Y Y$ are in $\operatorname{Div} X$, then $D_1 \geq D_2$ means $n_Y \geq m_Y$ for all Y. A divisor D is effective if $D \geq 0$.

If Y is an irreducible divisor of X, then the irreducible components of $\overline{Y} = Y_{\overline{k}}$ are irreducible divisors of $\overline{X}$, and these components form a single G-orbit in the set of irreducible divisors on $\overline{X}$. In fact, we get a bijection between the set of irreducible divisors on X and the G-orbits in the set of irreducible divisors on $\overline{X}$. Extending by linearity, we get a injective homomorphism

$$\operatorname{Div} X \hookrightarrow \operatorname{Div} \overline{X}$$

sending an irreducible divisor Y to the formal sum of the components of $\overline{Y}$, and the image is

$$(\operatorname{Div} \overline{X})^G := \{\, D \in \operatorname{Div} \overline{X} : {}^{\sigma}D = D \text{ for all } \sigma \in G \,\}.$$

Thus if we had defined $\operatorname{Div} \overline{X}$ first, we could have defined $\operatorname{Div} X$ as $(\operatorname{Div} \overline{X})^G$.

1.9.2. Principal divisors.

Definition 1.9.3. If $f \in \mathbf{k}(X)^\times$, then

$$(f) := \sum_Y v_Y(f) Y$$

is a divisor on X. This divisor is sometimes also written $\operatorname{div} f$. Such divisors are called principal divisors.

The map

$$\begin{aligned} \mathbf{k}(X)^\times &\to \operatorname{Div} X \\ f &\mapsto (f) \end{aligned}$$

is a homomorphism whose kernel is $k^\times$.

Definition 1.9.4. Divisors $D, D' \in \operatorname{Div} X$ are linearly equivalent if and only if $D - D'$ is a principal divisor. In this case we write $D \sim D'$.

If k is algebraically closed, $f \in \mathbf{k}(X)^\times$, and $D = \sum n_P P$ has support disjoint from that of (f), then define

$$f(D) := \prod_P f(P)^{n_P} \in k^\times.$$

Theorem 1.9.5 (Weil reciprocity). *Suppose k is algebraically closed. If $f, g \in \mathbf{k}(X)^\times$ and (f) and (g) have disjoint supports, then*

$$f(\operatorname{div} g) = g(\operatorname{div} f).$$

Proof. ♣♣♣ Bjorn: [See Serre, Algebraic groups and class fields?] □

1.9.3. Picard groups. Define $\operatorname{Pic} X$ as the cokernel of $\mathbf{k}(X)^\times \to \operatorname{Div} X$. We get a commutative diagram

$$\begin{tikzcd}
0 \arrow[r] & k^\times \arrow[r] \arrow[d, hook] & \mathbf{k}(X)^\times \arrow[r] \arrow[d, hook] & \operatorname{Div} X \arrow[r] \arrow[d, hook] & \operatorname{Pic} X \arrow[r] \arrow[d, hook] & 0 \\
0 \arrow[r] & \overline{k}^\times \arrow[r] & \mathbf{k}(\overline{X})^\times \arrow[r] & \operatorname{Div} \overline{X} \arrow[r] & \operatorname{Pic} \overline{X} \arrow[r] & 0.
\end{tikzcd}$$

The only nontrivial statement here is the injectivity of $\operatorname{Pic} X \to \operatorname{Pic} \overline{X}$; this is left as an exercise. The injective homomorphism $\operatorname{Pic} X \to (\operatorname{Pic} \overline{X})^G$ need not be surjective.

WARNING 1.9.6. Here is a dictionary for translating between our notation and that in [Sil92]:

Our notation	Notation in [Sil92]
$\operatorname{Div} X$	$\operatorname{Div}_k(X)$
$\operatorname{Div} \overline{X}$	$\operatorname{Div}(X)$
$\operatorname{Pic} X$	no notation for this
$\operatorname{Pic} \overline{X}$	$\operatorname{Pic}(X)$
$(\operatorname{Pic} \overline{X})^G$	$\operatorname{Pic}_k(X)$

1.10. Twists

"Twists of an object over a field are classified by H^1 of its automorphism group over the algebraic closure." This is not a theorem, because we have not and will not make completely precise what we mean by an object. It is only a vague principle, but nevertheless it holds in many common situations in arithmetic geometry.

We now elaborate a little (but still not being completely precise). Let k be a perfect field. Let V be an object over k, for example a variety equipped with some extra structure defined over k. We assume that the objects form a category, and that there is a notion of base extension: that is, given an object V over k and a field extension $L \supseteq k$, there should be an associated object V_L over L. A *twist* or *k-form* of V is an object W over k such that there exists a (structure-preserving) isomorphism $W_{\overline{k}} \simeq V_{\overline{k}}$ of objects over $\overline{k}$. Then there is an injection

$$\frac{\{\text{twists of } V\}}{k\text{-isomorphism}} \quad \hookrightarrow \quad H^1(k, \operatorname{Aut}(V_{\overline{k}})), \tag{1.10.1}$$

and descent theory proves that it is a bijection for many types of objects. Recall that $H^q(k, \bullet)$ is an abbreviation for the Galois cohomology group (or set) $H^q(\mathrm{Gal}(\overline{k}/k), \bullet)$. The group $\mathrm{Aut}(V_{\overline{k}})$ is the group of automorphisms of $V_{\overline{k}}$ as an object over $\overline{k}$. This automorphism group may be nonabelian, so we may need nonabelian H^1 as defined in [Ser02, I.§5]. In general this H^1 is not a group, but only a pointed set (i.e., a set equipped with a distinguished "zero element").

The injection (1.10.1) is defined as follows. Suppose that W is a twist of V over k. Fix an isomorphism $\phi : W_{\overline{k}} \to V_{\overline{k}}$. Then for $g \in G_k$, we apply g to obtain another isomorphism ${}^g\phi : W_{\overline{k}} \to V_{\overline{k}}$. Then the 1-cocycle $g \mapsto {}^g\phi \circ \phi^{-1} \in \mathrm{Aut}(V_{\overline{k}})$ represents an element of $H^1(k, \mathrm{Aut}(V_{\overline{k}}))$.

Remark 1.10.2. Quasi-projective varieties (without extra structure) are one class of objects for which the injection (1.10.1) is a bijection. ♣♣♣ Bjorn: [Give reference: Néron Models book?]

1.11. Group varieties

Let E be a set with one element. A group is a set G equipped with set maps $m\colon G \times G \to G$ (multiplication), $i\colon G \to G$ (inverse), and $e\colon E \to G$ (identity), satisfying the usual axioms. These axioms can be expressed without referring to elements: for instance, the statement that i gives a left inverse can be expressed as the commutativity of the diagram

$$\begin{tikzcd}
G \arrow[r, "{(i,1)}"] \arrow[dr] & G \times G \arrow[r, "m"] & G. \\
& E \arrow[ur, "e"'] &
\end{tikzcd}$$

If one replaces the category of sets with the category of k-varieties, and E by $\operatorname{Spec} k$ (each E is the terminal object of the corresponding category), one gets the definition of group variety over k.

Remark 1.11.1. Similarly, one could define the notion of group scheme. One could even define a group object in any category $\mathcal{C}$ having a terminal object E: The only difference is that in the general case, one must add axioms saying that the products $G \times G$ and $G \times G \times G$ exist in $\mathcal{C}$, since this is not automatic and one cannot even state the group axioms if the products do not exist.

If G is a group variety over k, then for any field extension $L \supseteq k$ (or even any k-algebra or k-scheme), the set $G(L)$ is a group under the operations given by m, i, e.

Definition 1.11.2. A homomorphism of group varieties $G \to H$ over k is a morphism of k-varieties that respects the m, i, e for G and H.

We get a category of group varieties over k.

Examples 1.11.3.

(i) The additive group variety $\mathbb{G}_a$. The affine line $\mathbb{A}^1$ equipped with the obvious m, i, e is called $\mathbb{G}_a$. For any k-algebra L, the group $\mathbb{G}_a(L)$ is the additive group of L.

(ii) The multiplicative group variety $\mathbb{G}_m$. This is $\mathbb{A}^1 - \{0\}$ with the m, i, e corresponding to multiplication. We could also present $\mathbb{G}_m$ as the affine variety $xy = 1$ in $\mathbb{A}^2$ equipped with $m((x_1, y_1), (x_2, y_2)) = (x_1x_2, y_1y_2)$, and $i((x, y)) = (y, x)$, and $e = (1, 1)$ (i.e., the map sending the point $\operatorname{Spec} k$ to $(1, 1) \in \mathbb{A}^2$). For any k-algebra L, $\mathbb{G}_m(L)$ is the unit group $L^\times$.

(iii) The general linear group variety GL_n. Let (x_{ij}) for $1 \le i, j \le n$ be indeterminates. Let z be an additional indeterminate. These form the coordinates on an affine space $\mathbb{A}^{n^2+1}$. Let GL_n be the variety $\det(x_{ij})z = 1$. The usual formulas for matrix multiplication and inversion make GL_n into a noncommutative group variety of dimension n^2.

(iv) A restriction of scalars. Let R be the variety $\mathbb{A}^2 - \{x^2 - 2y^2 = 0\}$ over $\mathbb{Q}$. (Again, this could be presented as an affine variety, by introducing an extra variable to play the role of $(x^2 - 2y^2)^{-1}$.) Pretending that (x, y) represents $x + y\sqrt{2}$, let us define

$$\begin{aligned} m((x_1, y_1), (x_2, y_2)) &= (x_1x_2 + 2y_1y_2, x_1y_2 + x_2y_1) \\ i((x, y)) &= \left(\frac{x}{x^2 - 2y^2}, -\frac{y}{x^2 - 2y^2}\right) \\ e &= (1, 0). \end{aligned}$$

One can check that R is a 2-dimensional group variety over $\mathbb{Q}$. (In fact one can show that R is the restriction of scalars $\operatorname{Res}_{L/\mathbb{Q}} \mathbb{G}_m$ where $L := \mathbb{Q}(\sqrt{2})$.) Over L we have an isomorphism

$$\begin{aligned} R_L &\to (\mathbb{G}_m \times \mathbb{G}_m)_L \\ (x, y) &\mapsto (x + \sqrt{2}y, x - \sqrt{2}y). \end{aligned}$$

but one can show that R is not isomorphic to $\mathbb{G}_m \times \mathbb{G}_m$ as a group variety over $\mathbb{Q}$.

(v) A "Pell equation torus". There is a homomorphism $\beta\colon R \to \mathbb{G}_m$ sending (x, y) to $x^2 - 2y^2$ (inspired by the norm homomorphism $L^\times \to \mathbb{Q}^\times$). The kernel of β is a group variety G defined by $x^2 - 2y^2 = 1$ and with m, i, e given by the same equations as for R.

Definition 1.11.4. A group variety T over k such that $T_{\overline{k}}$ is isomorphic to $(\mathbb{G}_m^n)_{\overline{k}} = (\mathbb{G}_m \times \cdots \times \mathbb{G}_m)_{\overline{k}}$ for some $n \in \mathbb{Z}_{\geq 0}$ is called a torus. If T is isomorphic to $\mathbb{G}_m^n$ over the ground field k, then T is called a split torus.

1.12. Torsors

1.12.1. An example of a torsor. Let R, β, G be as in the Pell equation torus example. We have an exact sequence

$$1 \to G \to R \xrightarrow{\beta} \mathbb{G}_m \to 1$$

in the sense that the sequence of groups

$$1 \to G(\overline{\mathbb{Q}}) \to R(\overline{\mathbb{Q}}) \xrightarrow{\beta} \mathbb{G}_m(\overline{\mathbb{Q}}) \to 1$$

is exact. Let $X = \beta^{-1}(3)$, which is an affine variety defined by the equation $x^2 - 2y^2 = 3$ in $\mathbb{A}^2_{\mathbb{Q}}$. Then $X(\overline{\mathbb{Q}})$ is a coset of $G(\overline{\mathbb{Q}})$ in $R(\overline{\mathbb{Q}})$. The multiplication $m \colon R \times R \to R$ restricts to a $\mathbb{Q}$-morphism

$$\begin{aligned} X \times G &\to X \\ (x, g) &\mapsto xg := m(x, g) \end{aligned}$$

and this defines an transitive right action of $G(\overline{\mathbb{Q}})$ on $X(\overline{\mathbb{Q}})$ with trivial stabilizers. If we pick $x \in X(\overline{\mathbb{Q}})$, we get an isomorphism of $\overline{\mathbb{Q}}$-varieties

$$\begin{aligned} G_{\overline{\mathbb{Q}}} &\to X_{\overline{\mathbb{Q}}} \\ g &\mapsto xg. \end{aligned}$$

If we could pick $x \in X(\mathbb{Q})$, then we would get an isomorphism of $\mathbb{Q}$-varieties $G \to X$. But applying an algorithm to be discussed in Section 2.7 to the genus-0 curve X shows that $X(\mathbb{Q})$ is empty. (Equivalently, the field $\mathbb{Q}(\sqrt{2})$ has no element of norm 3.) Since $G(\mathbb{Q})$ is nonempty, X is not isomorphic to G.

Here X is an example of a torsor under G. The fact that $X(\mathbb{Q})$ is empty means that X is a nontrivial torsor. In the next section we will give the precise definitions of these terms.

1.12.2. Definition of torsor. Let G be a group variety over k. The notion of group action can be stated in category-theoretic terms; thus we may speak of a k-variety X equipped with a right G-action.

Example 1.12.1. The trivial torsor $\mathbf{G}$ is defined to be the variety G equipped with the right G-action given by the group law $m\colon \mathbf{G} \times G \to \mathbf{G}$.

Proposition 1.12.2. *Let X be a variety with right G-action, which we write as*

$$\begin{aligned} X \times G &\to X \\ (x, g) &\mapsto xg. \end{aligned}$$

Then the following are equivalent:

(1) *X is a twist of $\mathbf{G}$; i.e., $X_{\overline{k}}$ is isomorphic (as variety* equipped with G-action*) to $\mathbf{G}_{\overline{k}}$.*

(2) *X is nonempty (i.e., $X(\overline{k}) \neq \emptyset$), and the morphism*

$$\begin{aligned} X \times G &\to X \times X \\ (x, g) &\mapsto (x, xg) \end{aligned}$$

is an isomorphism of k-varieties.

(3) *(For this condition to be equivalent to the others, we must assume that G is commutative; otherwise it may be strictly stronger.) There is an exact sequence of group schemes*

$$1 \to G \to R \xrightarrow{\beta} \mathbb{Z} \to 1$$

such that X is isomorphic to $\beta^{-1}(1)$ as a variety equipped with G-action.

If any of these conditions is satisfied, X is called a **(right) torsor under** *G (or a* **principal homogeneous space** *of G).*

Remark 1.12.3. In part 3, $\mathbb{Z}$ denotes the constant group scheme, i.e., a disjoint union of copies of $\operatorname{Spec} k$ indexed by integers, equipped with the obvious m, i, e. We must speak of group schemes instead of group varieties, since $\mathbb{Z}$ has infinitely many components. ♣♣♣ Bjorn: [Explain what exact sequence means in this context?]

Sketch of proof of Proposition 1.12.2. Each of the conditions is invariant under algebraic extension of the base field. So we may assume $k = \overline{k}$, in which case the equivalences are almost obvious. □

Warning 1.12.4. Let X be a variety with G-action. If X is a torsor, then the induced action of $G(\overline{k})$ on $X(\overline{k})$ is transitive with trivial stabilizers. But the converse is false: see Exercise 9.

Remark 1.12.5. One can also define torsors over an arbitrary base scheme S in place of $\operatorname{Spec} k$, for instance by generalizing condition 2 of Proposition 1.12.2 appropriately.

1.12.3. Cohomological classification of torsors. Since torsors under G are simply twists of the trivial torsor $\mathbf{G}$, descent theory as in Section 1.10 shows that they are classified up to k-isomorphism by the pointed set $H^1(k, \operatorname{Aut} \mathbf{G}_{\overline{k}})$, where $\operatorname{Aut} \mathbf{G}_{\overline{k}}$ is the group of automorphisms of $G_{\overline{k}}$ that respect the right $G_{\overline{k}}$-action. According to Exercise 10, $\operatorname{Aut} \mathbf{G}_{\overline{k}} = G(\overline{k})$. Thus we have a bijection of pointed sets

$$\frac{\{\text{ torsors under } G\ \}}{k\text{-isomorphism}} \quad \longleftrightarrow \quad H^1(k, G).$$

The "zero element" on each side is described by the following easy result:

Proposition 1.12.6. *The following are equivalent for a torsor X under G:*

(1) *X is isomorphic to the trivial torsor $\mathbf{G}$.*
(2) *$X(k)$ is nonempty.*
(3) *X corresponds to $0 \in H^1(k, A)$.*

Remark 1.12.7. Suppose that G acts freely on a variety R and that a geometric quotient $Q := R/G$ exists (we will not say exactly what this means). ♣♣♣ Bjorn: [Can we clarify this?] Let $\beta \colon R \to R/G = Q$ be the canonical quotient morphism. If $q \in Q(k)$, then $\beta^{-1}(q)$ is a torsor under G. One sometimes says that this torsor is visible in R.

In the special case where

$$1 \to G \to R \xrightarrow{\beta} Q \to 1$$

is an exact sequence of group varieties, the class of the torsor $\beta^{-1}(q)$ equals the image of q under the coboundary map $Q(k) = H^0(k, Q) \to H^1(k, G)$. The torsor in Section 1.12.1 is of this type.

Exercises

1.1. Let X and Y be two closed k-subvarieties in $\mathbb{A}^n_k$. Prove that $X = Y$ as subvarieties of $\mathbb{A}^n_k$ if and only if for every k-algebra R, the subsets $X(R)$ and $Y(R)$ of $\mathbb{A}^n(R) = R^n$ are equal. (Hints: If R is the affine coordinate ring of X, then $X(R)$ has a canonical element. This exercise is very close to Yoneda's lemma.)

1.2. (a) Prove the claims made in Example 1.4.3 for the curve $x^2 - 2y^2 = 0$ in $\mathbb{A}^2_{\mathbb{Q}}$.

(b) Verify Remark 1.4.6 for this curve.

1.3. Let X be an integral k-variety, and let Y be any k-variety. (Though it is not necessary, you may assume that Y is reduced, and that Y is affine or projective, if you want.) Show that the set of rational maps $X \dashrightarrow Y$ is in bijection with $Y(\mathbf{k}(X))$.

1.4. Explain why {integral k-varieties, rational maps} is not a category.

1.5. Give an example of a sequence of polynomials $f_1, \ldots, f_m \in k[t_1, \ldots, t_n]$ such that the projective closure the closed k-subvariety X_0 of $\mathbb{A}^n$ defined by $f_1 = \cdots = f_m = 0$ does not equal the k-subvariety of $\mathbb{P}^n$ defined by the homogenizations of the f_i.

1.6. Use Hilbert's Theorem 90 to prove that the homomorphism $\operatorname{Pic} X \to (\operatorname{Pic} \overline{X})^G$ is injective.

1.7. Show that the "Pell equation torus" G over $\mathbb{Q}$ in Section 1.11 is a torus but not a split torus.

1.8. Let $L \supseteq k$ be a finite Galois extension of fields with Galois group G acting on the left on L. View G as a group variety over k (the disjoint union of $\#G$ copies of the point $\operatorname{Spec} k$, with an obvious group law). View $X := \operatorname{Spec} L$ as a k-variety. Prove that there is a right action of G on X making X a torsor under G.

1.9. Let k be a perfect field of characteristic $p > 0$.

(a) Verify that

$$\begin{aligned} \mathbb{A}^1 \times \mathbb{G}_a &\to \mathbb{A}^1 \\ (x, g) &\mapsto x + g^p. \end{aligned}$$

is an action of $\mathbb{G}_a$ on $\mathbb{A}^1$.

(b) Check that $\mathbb{G}_a(\overline{k})$ acts transitively on $\mathbb{A}^1(\overline{k})$ with trivial stabilizers.

(c) Prove that $\mathbb{A}^1$ with this action is *not* a torsor under $\mathbb{G}_a$.

1.10. Let G be a group variety over a field k. Prove that the group of automorphisms of G as a variety with right G-action equals $G(k)$, acting by *left* translation.

CHAPTER 2

Curves

2.1. Smooth projective models

2.1.1. Curves and function fields. Restricting the equivalence of categories (1.5.4) to 1-dimensional varieties gives an equivalence of categories

(2.1.1)

$$\left\{ \begin{array}{c} \text{integral 1-dimensional } k\text{-varieties,} \\ \text{dominant rational maps} \end{array} \right\} \longleftrightarrow \left\{ \begin{array}{c} \text{f.g. field extensions } K \text{ of } k \text{ with } \operatorname{trdeg}(K/k) = 1 \\ k\text{-algebra homomorphisms} \end{array} \right\}^{\mathrm{op}}.$$

2.1.2. Resolution of singularities. One form of the resolution of singularities conjecture is that every integral k-variety is birational to a smooth projective integral k-variety. So far it has been proved when $\operatorname{char} k = 0$ or the dimension is ≤ 2 [Hir64].

In particular, within the collection of all 1-dimensional integral k-varieties with a given function field (of transcendence degree 1), there exists one that is smooth and projective. Moreover, this smooth projective model is unique up to k-isomorphism.

Thus the category

$$\left\{ \begin{array}{c} \text{smooth projective integral 1-dimensional } k\text{-varieties,} \\ \text{dominant morphisms} \end{array} \right\}$$

is equivalent to the two categories in (2.1.1).

Remark 2.1.2. The uniqueness of the smooth projective model fails in dimension ≥ 2. since given one, one can get other non-isomorphic ones by blowing up a point.

Remark 2.1.3. If we work over an imperfect field k, then "smooth" should be replaced everywhere by the slightly weaker condition "regular".

From now on, a curve is a nice variety of dimension 1, unless otherwise indicated.

2.1.3. Morphisms of curves.

Definition 2.1.4. Let $\pi\colon X \to Y$ be a morphism of curves. We define the degree of π as follows:

- If π is constant (i.e., the image of π is contained in a 0-dimensional subvariety of Y), define $\deg \pi = 0$.
- Otherwise π is dominant, and we identify $\mathbf{k}(Y)$ with a subfield of $\mathbf{k}(X)$. In this case, define $\deg \pi = [\mathbf{k}(X) : \mathbf{k}(Y)]$.

In the non-constant case, we call π separable if and only $\mathbf{k}(X)$ is separable over $\mathbf{k}(Y)$; also, define the separable degree $\deg_s \pi$ and inseparable degree $\deg_i \pi$ in terms of the corresponding notions for the extension $\mathbf{k}(X) \supseteq \mathbf{k}(Y)$.

2.2. Divisor groups and Picard groups of curves

2.2.1. Closed points.

Definition 2.2.1. A closed point P of a k-variety is an integral k-subvariety of dimension 0. The residue field of P is its function field $\mathbf{k}(P)$, which is a finite extension of k. The degree of P is $[\mathbf{k}(P) : k]$.

Remark 2.2.2. One could identify the set of closed points with the set of $\operatorname{Gal}(\overline{k}/k)$-orbits in $X(\overline{k})$.

Example 2.2.3. If $X = \mathbb{A}^1_{\mathbb{Q}} = \operatorname{Spec} \mathbb{Q}[t]$, then $P := \operatorname{Spec} \mathbb{Q}[t]/(t^2 - 2)$ is a closed point of degree 2, with residue field $\mathbb{Q}[t]/(t^2 - 2) \simeq \mathbb{Q}(\sqrt{2})$.

Example 2.2.4. Suppose X is a variety over $k = \overline{k}$. Then a closed point is the same thing as a k-point, the residue field is always k, and the degree is always 1.

Example 2.2.5. Let X be a variety over $\mathbb{F}_q$. Let N_d be the number of closed points of degree d on X, which equals the number of $\operatorname{Gal}(\overline{\mathbb{F}}_q/\mathbb{F}_q)$-orbits of size d in $X(\overline{\mathbb{F}}_q)$. Then $X(\mathbb{F}_{q^n})$ is the union of all orbits of size d over all $d \mid n$, so

$$\#X(\mathbb{F}_{q^n}) = \sum_{d \mid n} d N_d. \tag{2.2.6}$$

2.2.2. Degree of divisors. On a curve C, an irreducible divisor is the same thing as a closed point. Extending the notion of degree linearly gives a homomorphism

$$\begin{aligned} \deg \colon \operatorname{Div} C &\to \mathbb{Z} \\ \sum n_P P &\mapsto \sum n_P (\deg P), \end{aligned}$$

and the kernel is denoted $\operatorname{Div}^0 C$. One can show that every principal divisor has degree 0, so there is an induced homomorphism

$$\deg \colon \operatorname{Pic} C \to \mathbb{Z},$$

and the kernel is denoted $\operatorname{Pic}^0 C$.

WARNING 2.2.7. On a variety X of arbitrary dimension, a finite formal linear combination of closed points is called a zero-cycle. When $\dim X \neq 1$, zero-cycles and divisors are not the same.

2.2.3. Pullback and pushforward of divisors. Suppose $\pi\colon X \to Y$ is a dominant morphism of curves.

For each closed point $P \in Y$, define $\pi^* P := \sum_{Q \in \pi^{-1}(P)} e_Q Q$, where e_Q is the ramification index of Q over P. Extend linearly to define

$$\pi^*\colon \operatorname{Div} Y \to \operatorname{Div} X.$$

For each closed point $Q \in X$, define $\pi_* Q := fP$, where $P = \pi(Q)$ and $f = f(Q/P) := [\mathbf{k}(Q) : \mathbf{k}(P)]$. (If $k = \overline{k}$, then $f = 1$.) Extend linearly to define

$$\pi_*\colon \operatorname{Div} X \to \operatorname{Div} Y.$$

We get commutative diagrams

$$\begin{tikzcd}
\mathbf{k}(X)^\times \arrow[r] & \operatorname{Div} X \\
\mathbf{k}(Y)^\times \arrow[r] \arrow[u, hook, "i"] & \operatorname{Div} Y \arrow[u, "\pi^*"']
\end{tikzcd}
\qquad\qquad
\begin{tikzcd}
\mathbf{k}(X)^\times \arrow[r] \arrow[d, "N"'] & \operatorname{Div} X \arrow[d, "\pi_*"] \\
\mathbf{k}(Y)^\times \arrow[r] & \operatorname{Div} Y
\end{tikzcd}$$

where $i\colon \mathbf{k}(Y) \hookrightarrow \mathbf{k}(X)$ is the inclusion homomorphism induced by π, and $N\colon \mathbf{k}(X) \to \mathbf{k}(Y)$ is the norm map for the finite extension $\mathbf{k}(X) \supseteq \mathbf{k}(Y)$. Hence we get induced homomorphisms

$$\pi^*\colon \operatorname{Pic} Y \to \operatorname{Pic} X, \qquad \pi_*\colon \operatorname{Pic} X \to \operatorname{Pic} Y.$$

2.3. Differentials

2.3.1. Definition of the space of differentials. Let C be a curve over k. Let $\mathcal{K} = \mathbf{k}(C)$. The $\mathcal{K}$-vector space $\Omega_C = \Omega_{\mathcal{K}/k}$ of meromorphic Kähler differentials on C is the quotient of the $\mathcal{K}$-vector space with basis $(dx : x \in \mathcal{K})$ (where dx is a different symbol for each $x \in \mathcal{K}$) modulo the $\mathcal{K}$-vector space of relations spanned by

$$\begin{aligned} d(x_1 + x_2) &= dx_1 + dx_2 \\ d(x_1 x_2) &= x_1 dx_2 + x_2 dx_1 \\ da &= 0 \end{aligned}$$

for all $x_1, x_2 \in \mathcal{K}$ and $a \in k$. For each $x \in \mathcal{K}$, we write dx for its image in Ω_C.

It turns out that Ω_C is a 1-dimensional $\mathcal{K}$-vector space.

Proposition 2.3.1. *For $t \in \mathcal{K}$, the following are equivalent:*

- $dt \neq 0$.
- *dt spans Ω_C as a $\mathcal{K}$-vector space.*
- *$\mathcal{K}$ is a finite separable extension of $k(t)$.*
- $t \notin \begin{cases} k & \text{if } \operatorname{char} k = 0 \\ \mathcal{K}^p & \text{if } \operatorname{char} k = p > 0 \end{cases}$

2.3.2. Divisors of differentials.

Definition 2.3.2. Given a closed point P of C and $\omega \in \Omega_C$, choose a uniformizer t at P. By the above criterion, dt spans Ω_C, so $\omega = f\,dt$ for some $f \in \mathcal{K}$. Define

$$v_P(\omega) := v_P(f) \in \mathbb{Z} \cup \{\infty\}.$$

If $\omega \neq 0$, define the divisor of ω as

$$(\omega) := \sum_{\text{closed } P \in C} v_P(\omega) P \in \operatorname{Div} C.$$

Definition 2.3.3. Say that ω is regular at a closed point $P \in C$ if $v_P(\omega) \geq 0$. Say that ω is regular if it is regular at every closed point $P \in \mathbb{C}$.

Definition 2.3.4. Any divisor of the form (ω) for some $\omega \in \Omega_C$ is called a canonical divisor and denoted K. The corresponding class in $\operatorname{Pic} C$ is independent of the choice of ω, and is called the canonical class.

2.3.3. Pullback of differentials. Let $\pi \colon X \to Y$ be a dominant morphism of k-curves. Identify $\mathbf{k}(Y)$ with a subfield of $\mathbf{k}(X)$. Then there is a homomorphism of $\mathbf{k}(Y)$-vector spaces

$$\pi^* \colon \Omega_Y \to \Omega_X$$

mapping $f\,dx$ for $f, x \in \mathbf{k}(Y)$ to $f\,dx$ with f, x viewed as elements of $\mathbf{k}(X)$. By Proposition 2.3.1, $\pi^* = 0$ if and only if π is not separable.

2.4. The Riemann-Roch theorem

2.4.1. Functions with order conditions.

Definition 2.4.1. For $D \in \operatorname{Div} C$, define a k-vector space

$$L(D) := \{\, f \in \mathbf{k}(C)^\times : (f) + D \geq 0 \,\} \cup \{0\}.$$

This agrees with the space of global sections $\Gamma(C, \mathcal{L}(D))$, where $\mathcal{L}(D)$ is the line sheaf contained in the sheaf of rational functions on C. Also define $\ell(D) := \dim_k L(D)$.

One can show that if $\overline{D}$ denotes the image of D under $\operatorname{Div} C \hookrightarrow \operatorname{Div} \overline{C}$, then the natural map $L(D) \hookrightarrow L(\overline{D})$, where the first space is computed on C and the second on $\overline{C}$, induces an isomorphism $L(D) \otimes_k \overline{k} \to L(\overline{D})$. In particular, $\ell(D) = \ell(\overline{D})$.

Remark 2.4.2. If $D, D' \in \operatorname{Div} C$ and $D' = D + (h)$ for some $h \in \mathbf{k}(C)^\times$, then $L(D') = h^{-1}L(D)$ as a k-subspace in $\mathbf{k}(C)$, so $\ell(D) = \ell(D')$.

Proposition 2.4.3. *If* $\deg D < 0$*, then* $L(D) = \{0\}$ *and* $\ell(D) = 0$*:*

Proof. If $f \in \mathbf{k}(C)^\times$, then $\deg((f)+D) = \deg D < 0$, so $(f)+D \geq 0$ is impossible. □

Definition 2.4.4. The family of linearly equivalent effective divisors $D + (f)$ for $f \in L(D) - \{0\}$ is called the complete linear system $|D|$. The family is parameterized by the points of a projective space of dimension $\ell(D) - 1$, namely the projective space of lines in the vector space $L(D)$.

2.4.2. Genus.

Definition 2.4.5. The genus g of C is $\ell(K)$ where K is any canonical divisor.

The set of possibilities for g is the set of nonnegative integers. Equivalently, g is the dimension of the k-vector space of regular differentials on C.

Remark 2.4.6. Over $k = \mathbb{C}$, one can show that g equals the topological genus (number of holes) of the compact Riemann surface $C(\mathbb{C})$.

2.4.3. The Riemann-Roch theorem and easy corollaries. As usual, let K be a canonical divisor on C.

Theorem 2.4.7 (Riemann-Roch theorem). *For any* $D \in \operatorname{Div} X$*,*

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

Corollary 2.4.8. *For any canonical divisor* K*, we have* $\deg K = 2g - 2$.

Proof. Taking $D = K$ in Theorem 2.4.7 gives

$$g - 1 = \deg K + 1 - g.$$

□

Corollary 2.4.9. *If* $\deg D > 2g - 2$*, then* $\ell(D) = \deg D + 1 - g$.

Proof. We have $\deg(K - D) = 2g - 2 - \deg D < 0$, so by Proposition 2.4.3, $\ell(K - D) = 0$. □

2.4.4. Projective embeddings of curves. If $D \in \operatorname{Div} X$ is such that $L(D) \neq 0$, and $f_0, \ldots, f_n$ is a basis for $L(D)$, one gets a rational map

$$\begin{aligned} X &\to \mathbb{P}^n \\ P &\mapsto (f_0(P) : \cdots : f_n(P)), \end{aligned} \tag{2.4.10}$$

called the rational map associated to $|D|$. (Actually it depends also on the choice of basis of $L(D)$, but changing the basis only composes the rational map with a linear automorphism of $\mathbb{P}^n$.)

PROPOSITION 2.4.11. *Suppose k is algebraically closed. We have $\ell(D-P-Q) = \ell(D) - 2$ for all $P, Q \in X(k)$ if and only if* (2.4.10) *is an* embedding *(a morphism mapping X isomorphically to its image). In this case, the degree of the image as a curve in $\mathbb{P}^n$ equals* $\deg D$.

PROOF. The hypothesis says that (2.4.10) separates points and separates tangent vectors. The hyperplane sections of the image X' correspond to the divisors in $|D|$, so they have degree $\deg D$; i.e., $\deg X' = \deg D$. □

COROLLARY 2.4.12. *Let k be any field. If* $\deg D \geq 2g+1$ *then* (2.4.10) *is an embedding and* $\deg X' = \deg D$. *Moreover, $n = \deg D - g$.*

PROOF. Without loss of generality, we may assume $k = \overline{k}$. By Corollary 2.4.9, $\ell(D) = \deg D + 1 - g$ and $\ell(D-P-Q) = \deg D - 1 - g$ for any $P, Q \in X(k)$. So we may apply Proposition 2.4.11(ii). Finally, $n = \ell(D) - 1 = \deg D - g$. □

DEFINITION 2.4.13. If X is a curve of genus $g \geq 1$, then a canonical divisor K determines a morphism

$$X \to \mathbb{P}^{g-1},$$

called the canonical map.

2.5. The Hurwitz formula

Let $\pi \colon X \to Y$ be a separable morphism of curves.

2.5.1. The ramification divisor.

DEFINITION 2.5.1. The ramification divisor of π is

$$R := (\pi^*\omega) - \pi^*(\omega) \in \operatorname{Div} X,$$

for any nonzero $\omega \in \Omega_Y$.

The separability of π is essential: it makes $\pi^*\omega$ nonzero. For functions (but not necessarily differentials), taking π^* commutes with taking the associated divisor; this implies that R is independent of the choice of ω.

Definition 2.5.2. Say that a morphism $\pi\colon X \to Y$ of k-curves is tamely ramified at a closed point $Q \in X$ if and only if $\operatorname{char} k$ does not divide the ramification index e_Q. Say that π is tamely ramified if it is tamely ramified at every closed point $Q \in X$.

Remark 2.5.3. Let $\pi\colon X \to Y$ be a dominant morphism of k-curves. For every $P \in Y$ we have $\sum_{Q\in\pi^{-1}(Y)} e_Q f_Q = \deg \pi$. In particular, if $\operatorname{char} k = 0$ or $\deg \pi < \operatorname{char} k$, then π is automatically separable and tamely ramified.

Proposition 2.5.4. *Let $\pi\colon X \to Y$ be a separable morphism of curves. Then for each closed point $Q \in X$, we have $v_Q(R) \geq e_Q - 1$, with equality if and only if π is tamely ramified at Q. In particular, if π is tamely ramified, then*

$$\deg R = \sum_{\text{closed } Q \in X} (e_Q - 1) \deg Q.$$

Remark 2.5.5. Suppose k is algebraically closed. In the case where π is separable but not tamely ramified, $v_Q(R)$ can be computed as follows: Let t be a uniformizer at Q on X. Let $f(T) \in \mathbf{k}(Y)[T]$ be the minimal polynomial of t over $\mathbf{k}(Y)$. Then $v_Q(R) = v_Q(f'(t))$, where f' is the derivative of f.

Alternatively, if $G_0 \supseteq G_1 \supseteq \cdots$ are the ramification groups in the lower numbering at Q, then $v_Q(R) = \sum_{i\geq 0}(\#G_i - 1)$. (We have $G_i = \{1\}$ for sufficiently large i, so the sum is finite.) Here G_0 is the inertia group, and G_1 is its Sylow p-subgroup: hence this multiplicity formula is a refinement of the statement that $v_Q(R) \geq e_Q - 1$ with equality if and only if π is tamely ramified at Q.

Example 2.5.6. Let X be the smooth projective model of

$$y^2 + y = x^3$$

over a field k of characteristic 2. Let $\pi\colon X \to \mathbb{P}^1$ be the x-coordinate map, which has degree 2. Our goal is to compute the ramification divisor R of π.

For each $a \in k$, there are two distinct solutions to $y^2 + y = a^3$, because the derivative of the polynomial $y^2 + y - a^3$ in y is nonzero. Hence no affine points occur in R. To see what happens above $\infty \in \mathbb{P}^1$, we make the substitution $x = s^{-1}$, and get $y^2 + y = s^{-3}$. Let v be the valuation at ∞ on $\mathbb{P}^1$, so $v(s) = 1$. Extend v to $\mathbf{k}(X)$. Then $v(y) = -3/2$, so ∞ ramifies. Since $\deg \pi = 2$, there is a unique point $\infty' \in X(k)$ above $\infty \in \mathbb{P}^1(k)$, of ramification index

2. The element $t := s^2 y$ satisfies $v(t) = 1/2$, so t is a uniformizer at ∞' on X. Multiplying both sides of $y^2 + y = s^{-3}$ by s^4 yields

$$t^2 + s^2 t = s$$
$$s^2\, dt = ds.$$

Let v' be the valuation at ∞' on X normalized to take values in $\mathbb{Z}$, so $v' = 2v$. We have $v'(t) = 1$ and $v'(s) = 2$ (the ramification index). Use $\omega = ds$ in the definition of R: we have $v(\omega) = 0$ on $\mathbb{P}^1$ so ∞' does not appear in $\pi^*(\omega)$, but $v'(\pi^*\omega) = v'(ds) = v'(s^2\, dt) = v'(s^2) = 4$ on X. Subtracting gives $v'(R) = 4$. Thus $R = 4\infty'$.

2.5.2. Two versions of the Hurwitz formula.

Theorem 2.5.7 (Hurwitz formula). *For any separable morphism of curves $\pi\colon X \to Y$, we have*

$$2g_X - 2 = (\deg \pi)(2g_Y - 2) + \deg R,$$

where g_X is the genus of X, g_Y is the genus of Y, and R is the ramification divisor of π.

Proof. Choose a nonzero $\omega \in \Omega_Y$, and take degrees on both sides of

$$(\pi^*\omega) = \pi^*(\omega) + R.$$

□

Because genus is unchanged by (separable) field extension, the Hurwitz formula is often applied over an algebraic closure.

Corollary 2.5.8 (simplified Hurwitz formula). *If π is tamely ramified and k is algebraically closed, then*

$$2g_X - 2 = (\deg \pi)(2g_Y - 2) + \sum_{Q \in X(\overline{k})} (e_Q - 1).$$

Proof. Combine Theorem 2.5.7 and Proposition 2.5.4. □

The main application of these formulas is to compute g_X when one knows g_Y. Occasionally one uses them instead to compute g_Y when one knows g_X, especially when Y is defined as the quotient X/H for a finite subgroup $H \leq \operatorname{Aut} X$.

☡ Warning 2.5.9. There is no Hurwitz formula for inseparable morphisms.

2.6. The analogy between number fields and function fields

There is a strong analogy between number fields and function fields. We let k be the constant field in the function field case. As usual, we assume that k is perfect. The analogy is especially good when k is finite.

Number field object	Function field analogue
$\mathbb{Z}$	$k[t]$
$\mathbb{Q}$	$k(t)$
$\mathbb{Q}_p$	$k((t))$
K is a finite extension of $\mathbb{Q}$ (K is a number field)	K is a finite extension of $k(t)$ $\iff$ K f.g. over k with $\operatorname{trdeg}(K/k) = 1$ $\iff$ K is the function field of a k-curve X. We may enlarge k to assume X is nice.
$\operatorname{Spec} \mathcal{O}_K +$ archimedean places	X
place, i.e., absolute value (up to equiv.)	closed point on X, or equivalently $\operatorname{Gal}(\overline{k}/k)$-conjugacy class of points in $X(\overline{k})$
Let S be a nonempty finite set of places containing all archimedean places. Let $\mathcal{O}_{K,S} := \{f \in K : v(f) \ge 0 \text{ for } v \notin S\}$.	
$\operatorname{Spec} \mathcal{O}_{K,S}$	the affine curve $X - S$
The ring $\mathcal{O}_{K.S}$ is a Dedekind domain, and is named as follows:	
ring of S-integers in K	ring of regular functions on $X - S$
The Dirichlet S-unit theorem says:	
$\mathcal{O}_{K,S}^\times \simeq \mathbb{Z}^{\#S-1} \times \frac{\mathbb{Z}}{w\mathbb{Z}}$ where w is the number of roots of 1.	If $k = \mathbb{F}_q$, then $\mathcal{O}_{K,S}^\times \simeq \mathbb{Z}^{\#S-1} \times \frac{\mathbb{Z}}{w\mathbb{Z}}$ where $w = q - 1$ is the number of roots of 1.
fractional ideal $\prod \mathfrak{p}^{n_\mathfrak{p}}$	divisor $\sum n_P P$ on X
Actually one should include archimedean data on the left, to get Arakelov divisors.	
principal ideal (α)	principal divisor (f)
product formula	degree of principal divisor is 0

(continued on next page)

Number field object	Function field analogue
Class groups on the left correspond roughly to Picard groups and Jacobians on the right, provided that one "Arakelov-izes" by adding archimedean information on the left. More precisely, we have:	
	Jacobian variety $J = \operatorname{Jac} X$
Arakelov Picard group $\widehat{\operatorname{Pic}}_K$	$\operatorname{Pic} X$
Arakelov class group $\widehat{\operatorname{Pic}}_K^0$ (compact group)	$J(k) = \operatorname{Pic}^0 X$ if k is finite (compact, since k is finite!)
$0 \to \widehat{\operatorname{Pic}}_K^0 \to \widehat{\operatorname{Pic}}_K \to \mathbb{R} \to 0$	$0 \to \operatorname{Pic}^0 X \to \operatorname{Pic} X \overset{\deg}{\to} \mathbb{Z} \to 0$ (if k is finite)
$\operatorname{Cl}(\mathcal{O}_{K,S})$ (finite abelian group)	$\operatorname{Cl}(\mathcal{O}_{K,S}) \simeq \frac{\operatorname{Pic} X}{\langle \text{classes of } s \in S \rangle}$ (finite if k is)

(continued on next page)

Number field object	Function field analogue
extension of number fields $L \supseteq K$	dominant morphism of curves $\pi \colon Y \to X$
extension of ideals $\mathfrak{a} \mapsto \mathfrak{a}\mathcal{O}_L$ $\mathfrak{p} \mapsto \prod_{\mathfrak{q}\mid\mathfrak{p}} \mathfrak{q}^{e_\mathfrak{q}}$, where $e_\mathfrak{q}$ is the ramification index.	pullback of divisors $\pi^* \colon \operatorname{Div} X \to \operatorname{Div} Y$ In terms of closed points, this is $P \mapsto \sum_{Q \in \pi^{-1}(P)} e_Q Q$, where e_Q is the ramification index.
norm of ideals $\mathfrak{q} \mapsto \mathfrak{p}^f$ where $\mathfrak{p} \subseteq \mathcal{O}_K$ lies under $\mathfrak{q} \subseteq \mathcal{O}_L$, and $f = f(\mathfrak{q}/\mathfrak{p})$ is residue field degree.	pushforward of divisors $\pi_* \colon \operatorname{Div} Y \to \operatorname{Div} X$ If $Q \in Y$ is closed, then $Q \mapsto fP$ where $P = \pi(Q)$, and $f = f(Q/P)$ is residue field degree. If $k = \overline{k}$, then $f = 1$ so $\pi_* Q = \pi(Q)$.
absolute discriminant	q^{g-1}, where $k = \mathbb{F}_q$ and g is the genus of X
different	ramification divisor (assuming π separable)
estimate for number of elements in adelic parallelotopes	Riemann-Roch theorem
Dedekind zeta function $\zeta_K(s) = \zeta_{\operatorname{Spec} \mathcal{O}_K}(s)$ (The analogy is even better if one includes Γ factors for the archimedean places.)	Hasse-Weil zeta function of X over $\mathbb{F}_q$ $\zeta_X(s) = Z_X(q^{-s})$
functional equation for $\zeta_K(s)$, and Generalized Riemann Hypothesis	Weil conjectures (all proven!)

2.7. Genus-0 curves

THEOREM 2.7.1. *Let X be a genus-0 curve.*

(i) *Then X is isomorphic to a* conic*, a smooth plane curve of degree* 2.

(ii) *If moreover X has a k-point, then $X \simeq \mathbb{P}^1_k$.*

(iii) *If k is a global field, then X has a k-point if and only if X has a k_v-point for every place v of k.*

PROOF.

(i) We have $\deg K = 2g - 2 = -2$. Let $D = -K$. Then $\deg D = 2 \geq 2g + 1$, so Proposition 2.4.12 gives an embedding $X \hookrightarrow \mathbb{P}^2$ as a curve of degree $\deg D - g = 2$.

(ii) Let P be the point. Take $D = P$. Then $\deg D = 1 \geq 2g + 1$, so Proposition 2.4.12 gives an embedding $X \hookrightarrow \mathbb{P}^1$ as a curve of degree $\deg D - g = 1$!

(iii) The Hasse-Minkowski theorem for quadratic forms states that a quadratic form (i.e., homogeneous polynomial of degree 2) over a global field k has a nontrivial zero (i.e., other than $\vec{0}$) if and only if it has a nontrivial zero over each k_v. Apply this to the quadratic form in 3 variables defining the conic in (i).

□

For the rest of this section, suppose that $\operatorname{char} k \neq 2$. Then one can perform a linear change of variable (complete the square repeatedly) to show that X is isomorphic to a curve

$$\alpha x^2 + \beta y^2 + \gamma z^2 = 0$$

in $\mathbb{P}^2_k$, and α, β, γ are all nonzero, since otherwise X would not be smooth. We may divide by α to get an equation of the form

$$x^2 - ay^2 - bz^2 = 0,$$

with $a, b \in k^\times$.

In fact, the following are equivalent:

(1) X has a k-point.

(2) The quadratic form $x^2 - ay^2 - bz^2$ has a nontrivial zero over k.

(3) The quaternion algebra over k with basis $1, i, j, ij$ satisfying $i^2 = a$, $j^2 = b$, and $ij = -ji$ is isomorphic to $\mathrm{M}_2(k)$.

DEFINITION 2.7.2. If k_v is a local field of characteristic not 2, and $a, b \in k_v^\times$, one defines the Hilbert symbol $(a, b)_v$ to be $+1$ or -1 according to whether $x^2 - ay^2 - bz^2$ has a nontrivial zero over k_v.

Thus, if k is a global field of characteristic not 2, the curve $x^2-ay^2-bz^2=0$ has a k-point if and only if $(a,b)_v=+1$ for all places v of k. Later on we will explain that $(a,b)_v=+1$ is automatic when v is nonarchimedean of residue characteristic not 2 and $v(a)=v(b)=0$. Thus only finitely many Hilbert symbols need be computed. This gives an effective test for whether a genus-0 curve over a global field k of characteristic not 2 has a k-point.

If $k=\mathbb{Q}$, the hardest part of this test is factoring a and b, which is needed to figure out which v need to be examined. In fact, the general problem of deciding whether a conic over $\mathbb{Q}$ has a $\mathbb{Q}$-point is polynomial-time equivalent to the general problem of factoring integers.

2.8. Hyperelliptic curves

2.8.1. Double covers of $\mathbb{P}^1$. Let $\mathcal{K}$ be a separable degree-2 extension of the rational function field $k(x)$. We want to construct the nice k-curve whose function field is $\mathcal{K}$. The inclusion $k(x)\hookrightarrow K$ corresponds to a dominant morphism $\pi\colon X\to\mathbb{P}^1$, and we will describe X and π by giving an equation for the part of X lying above each of the two copies of $\mathbb{A}^1$ in the standard open covering of $\mathbb{P}^1$. For simplicity, we will assume that $\operatorname{char} k\neq 2$.

Since char $k\neq 2$, we have $\mathcal{K}=k(x)(\sqrt{f})$ for some nonsquare $f\in k(x)^\times$. Since $k[x]$ is a UFD, we may multiply f by a square in $k(x)^\times$ to assume that f is a squarefree polynomial in $k[x]$. Choose $g\in\mathbb{Z}$ so that $\deg f$ is $2g+1$ or $2g+2$. Let X_1 be the affine variety $y^2=f(x)$ in $\mathbb{A}^2_k$, equipped with the projection $\pi_1\colon X_1\to\mathbb{A}^1_k$ onto the x-coordinate.

Remark 2.8.1. Taking the projective closure of X_1 in $\mathbb{P}^2_k$ would give a projective curve, but in general it would fail to be smooth. It turns out that the correct approach is to take the "even-degree homogenization" $F(X,Z):=Z^{2g+2}f(X/Z)$ of f. Then the desired nice model is the curve defined by $Y^2=F(X,Z)$ in a weighted projective plane $\mathbb{P}(1,g+1,1)$ where the variables X,Y,Z have weight $1,g+1,1$, respectively. We will describe this model in more concrete terms below.

Dividing the equation $y^2=f(x)$ by x^{2g+2}, and setting $u=1/x$, $v=y/x^{g+1}$ leads to a birational affine curve X_2 defined by $v^2=f^{\text{rev}}(u)$ in $\mathbb{A}^2_k$, where $f^{\text{rev}}(u)=u^{2g+2}f(1/u)\in k[u]$ is another squarefree polynomial of degree $2g+1$ or $2g+2$. (This X_2 is the curve that would have been obtained as X_1 in the previous paragraph had we started by viewing K as a degree-2 extension of $k(u)=k(1/x)$ instead of $k(x)$.) Equip X_2 with the projection $\pi_2\colon X_2\to\mathbb{A}^1_k$ onto the u-coordinate.

We may glue $\mathbb{A}^1_k=\operatorname{Spec}k[x]$ $\mathbb{A}^1_k=\operatorname{Spec}k[u]$ along the loci where $x\neq 0$ and $u\neq 0$, respectively, using the isomorphism given by $u=1/x$, to get $\mathbb{P}^1_k$. Above this, we may glue X_1 to X_2 along the loci where $x\neq 0$ and $u\neq 0$, respectively, using the isomorphism given by $(u,v) = (1/x, y/x^{g+1})$, to get a curve X. This X turns out to be the nice model. The morphisms π_1 and π_2 glue to give a k-morphism $\pi\colon X \to \mathbb{P}^1_k$.

One can check using the Hurwitz formula that the integer g defined in terms of $\deg f$ equals the genus of X.

2.8.2. The canonical map.

Proposition 2.8.2.

(i) *The divisor of dx/y on X is $K := (g-1)\pi^*\infty$, where ∞ is the point on $\mathbb{P}^1_k$ where x has a pole.*

(ii) *The functions*

$$1, x, \ldots, x^{g-1}$$

form a basis for $L(K)$.

(iii) *The differentials*

$$\frac{dx}{y}, \frac{x\,dx}{y}, \ldots, \frac{x^{g-1}\,dx}{y}$$

form a k-basis for the space of regular differentials on X.

(iv) *If $g \geq 1$, then the canonical map $X \to \mathbb{P}^{g-1}$ equals the composition of $\pi\colon X \to \mathbb{P}^1$ with the $(g-1)$-uple embedding*

$$\begin{aligned} \mathbb{P}^1 &\to \mathbb{P}^{g-1} \\ (x:1) &\mapsto (1 : x : x^2 : \cdots : x^{g-1}). \end{aligned}$$

Proof.

(i) The equation $y^2 = f(x)$ implies $\frac{dx}{2y} = \frac{dy}{f'(x)}$ in Ω_X. Since X_1 is smooth, at each closed point $P \in X_1$, either $2y$ or $f'(x)$ does not vanish, so one expression or the other shows that $v_P(dx/y) \geq 0$. Substituting $x = 1/u$ and $y = v/u^{g+1}$ into dx/y yields

$$\frac{dx}{y} = \frac{-du/u^2}{v/u^{g+1}} = -u^{g-1}\frac{du}{v}.$$

The same argument as above shows that du/v is regular on X_2. Thus if $P \in X$ lies above $\infty \in \mathbb{P}^1(k)$, then $v_P(dx/y) \geq v_P(u^{g-1}) = (g-1)v_P(u)$. The divisor of u on $\mathbb{P}^1$ is $(\infty) - (0)$, so the divisor of u on X is $\pi^*\infty - \pi^*0$. Thus $K \geq (g-1)\pi^*\infty$. But

$$\deg(g-1)\pi^*\infty = (g-1)(\deg\pi)(\deg\infty) = (g-1)\cdot 2 \cdot 1 = 2g-2 = \deg K,$$

so K must equal $(g-1)\pi^*\infty$.

(ii) The divisor of x on X is $\pi^*0 - \pi^*\infty$, so for $0 \le i \le g-1$, we have $K + (x^i) \ge 0$ and hence $x^i \in L(K)$. But these g functions x^i are linearly independent, and $L(K)$ has dimension g, so these functions are a basis of $L(K)$.

(iii) This follows from (i) and (ii).

(iv) This follows from (ii).

□

Remark 2.8.3. For an elliptic curve $y^2 = f(x)$ with f squarefree of degree 3, Proposition 2.8.2 gives the usual formula for an invariant differential.

Definition 2.8.4. A **hyperelliptic curve** over k is a nice k-curve X of genus $g \ge 2$ that has a separable degree-2 map π to a nice genus-0 curve Y.

Example 2.8.5. If $\operatorname{char} k \neq 2$ and $f(x) \in k[x]$ is a squarefree polynomial of degree ≥ 5, then the nice model of the affine curve $y^2 = f(x)$ is a hyperelliptic curve.

Warning 2.8.6. Some authors insist that the Y in Definition 2.8.4 be isomorphic to $\mathbb{P}^1_k$. There are two advantages, however, to allowing an arbitrary nice genus-0 curve:

- With our definition, X is hyperelliptic if and only if $\overline{X}$ is hyperelliptic.
- With our definition, Theorem 2.8.7 below is true.

Theorem 2.8.7. *Let X be a nice curve of genus $g \ge 2$.*

(i) *If X is hyperelliptic, and $X \to Y$ is a separable degree-2 morphism to a genus-0 curve Y, then the canonical map $X \to \mathbb{P}^{g-1}$ factors as $X \to Y \hookrightarrow \mathbb{P}^{g-1}$; in particular the canonical map is of degree 2 onto its image, which is a genus-0 curve in $\mathbb{P}^{g-1}$.*

(ii) *If X is not hyperelliptic, then the canonical map is an embedding.*

Proof. We will give the proof assuming $\operatorname{char} k \neq 2$, and leave the $\operatorname{char} k = 2$ case as an exercise. Without loss of generality, we may assume that k is algebraically closed.

(i) This is Proposition 2.8.2(iv).

(ii) Suppose that the canonical map is not an embedding. By Proposition 2.4.11, there exist $P, Q \in X(k)$ with $\ell(K - P - Q) \neq g - 2$. By Riemann-Roch, this is equivalent to $\ell(P + Q) \neq 1$. But $1 \in L(P + Q)$, so this implies that there is a non-constant $f \in L(P + Q)$. If we view f as a morphism $X \to \mathbb{P}^1$, then $0 < f^*\infty \le P + Q$, so $\deg f = \deg f^*\infty \le 2$. If $\deg f = 1$, then f is an isomorphism, which contradicts $g \ge 2$. If $\deg f = 2$, then f is automatically separable (either because $\operatorname{char} k \neq 2$, or because $g > 0$), so X is hyperelliptic.

□

2.9. Genus formulas

Here we gather some facts about the genus of certain curves, without supplying proofs. We will assume that k is algebraically closed, since the genus is unchanged by (finite separable) base extension.

2.9.1. Hyperelliptic curves. We have already seen that if $\operatorname{char} k \neq 2$, and $f(x)$ is a squarefree polynomial of degree $2g+1$ or $2g+2$ (where g is a nonnegative integer), then the smooth projective model of $y^2 = f(x)$ has genus g.

2.9.2. Plane curves. If X is a smooth curve of degree d in $\mathbb{P}^2_k$, then the genus of X is given by

$$g = \frac{(d-1)(d-2)}{2}.$$

An easy way to remember this: the genus of a line ($d = 1$) or a smooth conic ($d = 2$) is 0, and the genus of an elliptic curve ($d = 3$) is 1.

More generally, the genus of the smooth projective model of a possibly singular projective curve X in $\mathbb{P}^2$ is given by

$$g = \frac{(d-1)(d-2)}{2} - \sum_{\text{singularities } P \in X(k)} \delta_P,$$

where δ_P measures how bad the singularity at P is. Here are some examples of values of δ_P:

- If P is a node, like $(0,0)$ on $y^2 = x^3 + x^2$, then $\delta_P = 1$.
- If P is a (simple) cusp, like $(0,0)$ on $y^2 = x^3$, then $\delta_P = 1$.
- If the singularity P is analytically equivalent to an intersection of three smooth branches with distinct tangent directions (just as a node is an intersection of two smooth branches with distinct tangent directions), then $\delta_P = 3$.

More generally, if we shift coordinates to assume $P = (0,0) \in \mathbb{A}^2 \subseteq \mathbb{P}^2$, then the affine patch $X \cap \mathbb{A}^2$, is given by a (non-homogeneous) equation which we may write as

$$g_m(x,y) + g_{m+1}(x,y) + \cdots = 0,$$

where g_i is homogeneous of degree i in x and y, and g_m is not the zero polynomial. Then m is called the multiplicity of P on X. If moreover, the m linear factors of g_m are distinct (i.e., none is a scalar multiple of another), then $\delta_P = \binom{m}{2}$.

For the general definition and computation of δ_P, see Exercise IV.1.8 and Example V.3.9.3 in [Har77].

Remark 2.9.1. Suppose that k is infinite. Then every curve over k is birational to a (possibly singular) projective plane curve X having at worst nodes as singularities. This can be proved by embedding the smooth projective model in some large projective space $\mathbb{P}^N$, and then taking the image under a succession of sufficiently general linear projections

$$\mathbb{P}^N \dashrightarrow \mathbb{P}^{N-1} \dashrightarrow \cdots \dashrightarrow \mathbb{P}^2.$$

See [Har77, V.3.6, V.3.10] for details.

2.9.3. Newton polygons of two-variable polynomials.

Definition 2.9.2. A convex lattice polygon P in $\mathbb{R}^2$ is the convex hull of a finite subset of $\mathbb{Z}^2$. We (re)define the length of a side of P as $n-1$, where n is the number of lattice points on the side including the endpoints.

Suppose we have an irreducible Laurent polynomial

$$f(x,y) = \sum_{i,j} a_{ij} x^i y^j \in k[x^{\pm 1}, y^{\pm 1}] := k[x, 1/x, y, 1/y].$$

and a convex lattice polygon P containing $\{(i,j) \in \mathbb{Z}^2 : a_{ij} \neq 0\}$. For instance P could be the Newton polygon of f, defined as the convex hull of $\{(i,j) \in \mathbb{Z}^2 : a_{ij} \neq 0\}$.

Remark 2.9.3. The irreducibility of f in $k[x^{\pm 1}, y^{\pm 1}]$ implies that P is nondegenerate (i.e., 2-dimensional).

Given a side s of P, choose a direction along it, and label its lattice points 0, 1, ..., ℓ, where ℓ is the length of s; now form the homogeneous polynomial $f_s(t,u)$ of degree ℓ whose $\ell + 1$ coefficients are the coefficients of f corresponding to the lattice points on s in order (choose one of the two possible directions along s). We call f_s a side polynomial (this is not standard terminology).

Theorem 2.9.4. *Let $f = \sum a_{ij} x^i y^j$ be an irreducible Laurent polynomial. Let P be a convex lattice polygon containing $\{(i,j) \in \mathbb{Z}^2 : a_{ij} \neq 0\}$. Let X_0 be the (integral) subvariety of $(\mathbb{A}^1 - \{0\})^2$ defined by $f(x,y) = 0$. Suppose that*

(i) *The variety X_0 is smooth.*

(ii) *For each side s of P, the side polynomial f_s is squarefree.*

Let X be the smooth projective model of X_0. Then

(a) *The genus of X equals the number of lattice points in the interior of P.*

(b) *The differentials*

$$x^{i-1}y^{j-1}\frac{dx}{\partial f/\partial y}$$

for interior lattice points (i,j) form a basis for the space of regular differentials on X.

Remark 2.9.5. The zero polynomial is not squarefree. Thus the condition on the side polynomials will be satisfied usually only if P is close to being the Newton polygon on f.

Remark 2.9.6. One way to remember the formula for the differentials is to write it in the (meaningless) form

$$x^iy^j\frac{1}{df}\frac{dx}{x}\frac{dy}{y}.$$

Here $\frac{dx}{x}\frac{dy}{y}$ is the (unique up to scalar multiple) invariant 2-form on the torus $\mathbb{G}_m^2 = (\mathbb{A}^1 - \{0\})^2$.

Remark 2.9.7. Theorem 2.9.4 can be understood and generalized as follows. Associated to P is a 2-dimensional toric variety T containing $\mathbb{G}_m^2$ as a dense open subvariety, and the number of interior lattice points in P equals the arithmetic genus $p_a(\tilde{X})$ of the closure $\tilde{X}$ of X_0 in T, even if conditions (i) and (ii) of Theorem 2.9.4 are violated. Conditions (i) and (ii) are there to imply that $\tilde{X}$ is smooth. In general, the genus of the smooth projective model of X_0 can be computed as $p_a(\tilde{X}) - \sum_P \delta_P$, where the sum is a sum over singularities of $\tilde{X}$ as in Section 2.9.2.

♣♣♣ Bjorn: [If you know a simple proof of the statements in this subsection, let me know. I have a feeling maybe some of it can be done using Čech cohomology.]

2.10. The moduli space of curves

Theorem 2.10.1. *There is an irreducible quasi-projective k-variety $\mathcal{M}_g$ such that for every algebraically closed field L containing k, there is a bijection*

$$\frac{\{\textit{nice } L\textit{-curves of genus } g\}}{L\textit{-isomorphism}} \longleftrightarrow \mathcal{M}_g(L),$$

and these bijections are functorial in L. Here, "functorial in L" means that whenever we have $k \subseteq L \subseteq L'$ with L, L' algebraically closed, the map sending a nice L-curve X to its *base extension $X_{L'}$ is compatible with the natural inclusion $\mathcal{M}_g(L) \hookrightarrow \mathcal{M}_g(L')$. We have*

$$\begin{aligned} \mathcal{M}_0 &\simeq \operatorname{Spec} k \qquad \textit{(a point)} \\ \mathcal{M}_1 &\simeq \mathbb{A}^1_k \\ \dim \mathcal{M}_g &= 3g-3 \qquad \textit{for } g \geq 2. \end{aligned}$$

When g is large, the variety $\mathcal{M}_g$ is not rational *(birational to $\mathbb{P}^n$ for some n) and not even* unirational *(dominated by $\mathbb{P}^n$ for some n).* ♣♣♣ Bjorn: [Add references.]

We omit the proof since it is not so easy.

☡ Warning 2.10.2. It is unreasonable to hope for bijections that work functorially for all field extensions L instead of just the algebraically closed ones. There is a simple reason for this: if M is a variety, then for any extension of fields $L \subseteq L'$ containing the base field of M, the map $M(L) \to M(L')$ is injective, but the base extension map

$$\frac{\{\text{nice } L\text{-curves of genus } g\}}{L\text{-isomorphism}} \longrightarrow \frac{\{\text{nice } L'\text{-curves of genus } g\}}{L'\text{-isomorphism}}$$

need not be injective. For example, the smooth projective models of the two curves

$$\begin{aligned} y^2 &= x^3+1 \\ 2y^2 &= x^3+1 \end{aligned}$$

over $L := \mathbb{Q}$ become isomorphic after base extension to $L' := \mathbb{Q}(\sqrt{2})$. One could also consider genus-0 curves: there are infinitely many pairwise non-isomorphic nice genus-0 curves over $\mathbb{Q}$, but after base extension to $\overline{\mathbb{Q}}$ they are all isomorphic to $\mathbb{P}^1_{\overline{\mathbb{Q}}}$. These problems are related to the fact that some curves have nontrivial automorphisms. Because of these problems, one says that $\mathcal{M}_g$ is a coarse moduli space as opposed to a fine moduli space. (We will not define either term precisely here.)

☡ Warning 2.10.3. Suppose $g > 0$. Even if k is algebraically closed, there is no morphism of k-varieties $\pi \colon \mathcal{C}_g \to \mathcal{M}_g$ such that the fiber $\pi^{-1}(m)$ above each point $m \in \mathcal{M}_g(k)$ is a nice k-curve in the isomorphism class corresponding to m.

Remark 2.10.4. There are several ways to deal with the problems presented in Warnings 2.10.2 and 2.10.3:

(1) Discard all curves that have a nontrivial automorphism, even if the automorphism exists only over a field extension. The set of k-isomorphism classes of the nice

k-curves that remain are functorially in bijection with the set of k-points of a quasi-projective variety $\mathcal{N}_g$ (this is not a standard name for it), and there is a "universal family" $\pi\colon \mathcal{C}_g \to \mathcal{N}_g$ such that the fiber $\pi^{-1}(n)$ above any $n \in \mathcal{N}_g(k)$ is a curve is the isomorphism class corresponding to n. ♣♣♣ Bjorn: [Is the preceding sentence correct? This needs to be checked.] Discarding curves has its disadvantages, of course: for instance if $g \le 2$, then no curves are left (see Section 2.11), so $\mathcal{N}_g = \emptyset$, which is not very illuminating!

(2) Try to parameterize not just curves, but curves C equipped with extra structure S such as a sequence of n marked points (in which case the moduli space obtained is called $\mathcal{M}_{g,n}$) or an ordered basis of $L(3K)$. The effect of the extra structure is to "rigidify" the curve by eliminating automorphisms: even if some curves C have nontrivial automorphisms, it could be that none of them preserve S, so that the pair (C, S) always has trivial automorphism group. Each of these generalized moduli spaces has a morphism to $\mathcal{M}_g$ that forgets the extra structure. In fact, the standard approach to constructing $\mathcal{M}_g$ is to begin with some generalized moduli space $\mathcal{M}'_g$ and then to take the quotient by an equivalence relation. Often the equivalence classes are the orbits of some algebraic group G acting on $\mathcal{M}'_g$. Forming the quotient of a variety by the action an algebraic group is the subject of geometric invariant theory. This is the hardest part of the construction of $\mathcal{M}_g$.

(3) Enlarge the category of varieties to include objects called stacks which are even more general than schemes. Though we cannot find a variety $\mathcal{M}_g$ that does everything we want, we can find a stack $\mathcal{M}_g$, and for many purposes this is good enough. Stacks often arise in nature as the quotient of a variety by an algebraic group action, and these share many properties with true varieties. ♣♣♣ Bjorn: [Add reference.]

2.11. Describing all curves of low genus

Let k be any perfect field, and let $g \ge 0$. Our goal is to describe the set of isomorphism classes of nice k-curves of genus g.

2.11.1. Genus 0.

These are conics, as described in Section 2.7.

2.11.2. Elliptic curves.

Definition 2.11.1. An elliptic curve is a nice k-curve E of genus 1 equipped with a point $O \in E(k)$.

Elliptic curves can be classified by their j-invariant. Over an algebraically closed field k, there is exactly one elliptic curve E over k (up to isomorphism) with given j-invariant. Over an arbitrary perfect field k, there is at least one E, and the set of all of them is in bijection with a Galois cohomology set $H^1(k, \operatorname{Aut} E_{\overline{k}})$ (to be explained later). For most E, we have $\operatorname{Aut} E_{\overline{k}} \simeq \{\pm 1\}$, and if moreover $\operatorname{char} k \neq 2$ then $H^1(k, \operatorname{Aut} E_{\overline{k}}) \simeq k^\times / k^{\times 2}$. Concretely, if $\operatorname{char} k \neq 2$, then E is the smooth projective model of an affine curve $y^2 = f(x)$ with $\deg f = 3$, and if $\operatorname{Aut} E_{\overline{k}} = \{\pm 1\}$, then the other elliptic curves with the same j-invariant are the smooth projective models of $dy^2 = f(x)$ for $d \in k^\times$ (and the k-isomorphism type depends only on the image of d in $k^\times / k^{\times 2}$).

2.11.3. Genus 1. A torsor under an elliptic curve is a genus-1 curve, because it is so after base extension to $\overline{k}$. Conversely, if X is any genus-1 curve, its Jacobian E is an elliptic curve, and X is a torsor under E. (Jacobians will be discussed in Chapter 5.)

According to Section 1.12.3, the torsors under a given elliptic curve E are classified up to k-isomorphism by the group $H^1(k, E)$. But the elements of this group and the corresponding torsors are often hard to describe explicitly.

Warning 2.11.2. If one wants the set of torsors of E up to isomorphism as k-curves (which is weaker than isomorphism as torsors) then one should replace $H^1(k, E)$ by its quotient by the action of $\operatorname{Aut} E$.

Example 2.11.3. The smooth projective model of $y^2 = -x^4 - 1$ over $\mathbb{Q}$ is a genus-1 curve with no rational points.

2.11.4. Genus 2. Let X be a nice curve of genus 2. If the canonical map $X \to \mathbb{P}^{g-1} = \mathbb{P}^1$ were an embedding, then X would be isomorphic to $\mathbb{P}^1$, which contradicts the fact that $\mathbb{P}^1$ is of genus 0. Thus X is hyperelliptic. In particular, X is a double cover of (i.e., admits a separable degree-2 morphism to) a nice genus-0 curve Y. By Exercise 13, $Y \simeq \mathbb{P}^1_k$.

If we assume also that $\operatorname{char} k \neq 2$, then X is the smooth projective model of an affine curve $y^2 = f(x)$ where f is a squarefree polynomial of degree 5 or 6.

2.11.5. Genus 3. Let X be a nice curve of genus 3.

Suppose X is hyperelliptic. For simplicity, suppose also that $\operatorname{char} k \neq 2$. Then either X is the smooth projective model of an affine curve $y^2 = f(x)$ where f is a squarefree polynomial of degree 7 or 8, or X is a double cover of a nontrivial conic ("nontrivial" means not isomorphic to $\mathbb{P}^1_k$) ramified above 8 $\overline{k}$-points (by the Hurwitz formula).

Now suppose instead that X is not hyperelliptic. Then the canonical map $X \to \mathbb{P}^2$ identifies X with a (smooth) plane curve of degree $2g - 2 = 4$. Conversely, every smooth plane curve of degree 4 is a non-hyperelliptic curve of genus $(4-1)(4-2)/2 = 3$. (One can show that for a smooth plane curve $X \subseteq \mathbb{P}^2$ of degree 4, the canonical map is the inclusion $X \hookrightarrow \mathbb{P}^2$; this explains why X is non-hyperelliptic.)

2.11.6. Genus 4**.** Let X be a nice curve of genus 4.

Suppose X is hyperelliptic, then X is a double cover of $\mathbb{P}^1_k$; if moreover $\operatorname{char} k \neq 2$ then X is the smooth projective model of an affine curve $y^2 = f(x)$ where f is a squarefree polynomial of degree 9 or 10.

Now suppose instead that X is not hyperelliptic. Then the canonical map $X \to \mathbb{P}^3$ identifies X with a curve of degree $2g-2 = 6$ in $\mathbb{P}^3$. One can show that X is the complete intersection of a (uniquely determined, possibly singular) degree 2 hypersurface and a (not uniquely determined) degree 3 hypersurface in $\mathbb{P}^3$. Conversely, one can show that any smooth complete intersection of a hypersurface of degree 2 and a hypersurface of degree 3 in $\mathbb{P}^3$ is a nice non-hyperelliptic curve of genus 4.

2.11.7. Genus ≥ 5**.** One can continue for a few more values of g (see [ACGH85]), but the descriptions become ever more complicated. For larger values of g, there is no equally explicit description, but only a few general theorems such as Petri's theorem [ACGH85, p. 131, Theorem 2.3]. For the small values of g a general curve could be described by listing a few elements of k (the coefficients of some polynomials) subject only to some inequalities to guarantee smoothness. For higher values of g, $\mathcal{M}_g$ is non-unirational, as mentioned in Theorem 2.10.1, so the sequence of elements of k used to describe a general curve will necessarily have to be subject to some polynomial relations.

Exercises

2.1. Let X be the curve $x^2 + y^2 + z^2 = 0$ in $\mathbb{P}^2_{\mathbb{R}}$. Show that the cokernel of $\operatorname{Pic} X \to (\operatorname{Pic} \overline{X})^G$ is of order 2.

2.2. (a) Let K be a function field of a curve X over a finite field k. Prove the Dirichlet S-unit theorem for K, assuming the finiteness of $\operatorname{Pic}^0 X = J(k)$.

(b) Now suppose that k is infinite. Prove that $\mathcal{O}_{K,S}^\times / k^\times$ is finitely generated, but that its rank may be less than $\#S - 1$.

2.3. (a) Let K be a function field of a curve X over a finite field k. Let S be a nonempty set of places of K. Prove that $\operatorname{Cl}(\mathcal{O}_{K,S})$ is finite, assuming the finiteness of $\operatorname{Pic}^0 X = J(k)$.

(b) If instead k is infinite, is $\operatorname{Cl}(\mathcal{O}_{K,S})$ still finite?

2.4. Let X be a nice k-curve of genus g. Suppose $P \in X(k)$. Prove that every element of $\operatorname{Div}^0 X$ is linearly equivalent to $D - gP$ for some *effective* $D \in \operatorname{Div} X$ of degree g.

2.5. (a) Suppose $\pi\colon X \to Y$ is a dominant morphism of curves. Prove that the genus inequality $g_X \geq g_Y$ holds.

(b) Show that if equality holds, then either π is purely inseparable or $g_X \leq 1$.

2.6. Let X be a smooth plane curve of degree d in $\mathbb{P}^2$ over an algebraically closed field k.

(a) Given $P \in \mathbb{P}^2(k)$ with $P \notin X$, we have projection-from-P, which is a rational map $\mathbb{P}^2 \dashrightarrow \mathbb{P}^1$ defined everywhere except P. Prove that there exists P such that the composition $X \to \mathbb{P}^2 \dashrightarrow \mathbb{P}^1$, is a separable morphism π.

(b) Let R be the ramification divisor of π. Prove that R is the intersection of X with a curve of degree $d-1$.

(c) Use Bézout's theorem and the Hurwitz formula to prove the formula

$$g = (d-1)(d-2)/2$$

for the genus of X.

2.7. Prove that if one has access to an oracle for factoring integers, one can decide the existence of $\mathbb{Q}$-points on a conic in polynomial time. (Polynomial time means in time bounded by some polynomial in the bit length of the input. In this case, the input consists of the binary digits of the numerators and denominators of the coefficients of the conic.)

2.8. Let k be a perfect field of characteristic not 2. Let $f(x) \in k[x]$ be a non-constant squarefree polynomial. Let X_0 be the affine curve $y^2 = f(x)$ in $\mathbb{A}^2_k$.

(a) Prove that the projective closure of X_0 in $\mathbb{P}^2_k$ is smooth if and only if $\deg f \leq 3$.

(b) Let g be the integer such that $\deg f$ equals $2g+1$ or $2g+2$. Prove that the nice model of X_0 constructed in Section 2.8.1 has genus g.

2.9. In the notation of Proposition 2.8.2, prove that if $g \geq 2$ then

$$1, x, \ldots, x^{2g-2}, y, xy, \ldots, x^{g-3}y$$

is a basis for $L(2K)$.

2.10. Prove analogues of the results in Section 2.8 over a (perfect) field k of characteristic 2. For example, prove the following statements:

(a) A degree-2 extension $\mathcal{K}$ of $k(x)$ is obtained by adjoining a root y of $y^2 + y = f(x)$, where $f(x) \in k(x)$ is a rational function all of whose poles have odd order.

(b) Assume from now on that f is non-constant. Show that $\mathcal{K}$ is the function field of a nice k-curve C by showing that k is relatively algebraically closed in $\mathcal{K}$.

(c) Prove that if the orders of the poles of f are $n_1, \dots, n_m$, then the genus g of C equals

$$-1 + \sum_{i=1}^{m} \left(\frac{n_i + 1}{2} \right).$$

(d) Prove that C has a model defined by an equation $Y^2 + H(X,Z)Y = F(X,Z)$ in the weighted projective plane $\mathbb{P}(1, g+1, 1)$, where H and F are homogeneous of degree $\le g+1$ and $\le 2g+2$, respectively. Equivalently, construct C by glueing together two affine curves, as we did for $\operatorname{char} k \ne 2$.

(e) Prove that if we dehomogenize to obtain

$$y^2 + h(x)y = f(x)$$

(with $x = X/Z$ and $y = Y/Z^{g+1}$), the differentials

$$\frac{dx}{h(x)}, \quad x\frac{dx}{h(x)}, \quad \cdots \quad , \quad x^{g-1}\frac{dx}{h(x)}$$

form a k-basis for the space of regular differentials on C.

(f) Prove Theorem 2.8.7 for $\operatorname{char} k = 2$.

2.11. (a) Show that for any curve of genus $g \ge 2$, the rational map associated to $|3K|$ is an embedding into $\mathbb{P}^n$ for some n, and find n.

(b) For which curves of genus ≥ 2 is the same true for $|2K|$?

2.12. Let X be a nice k-curve of genus 0. Suppose that X has a divisor of odd degree. (This will hold, in particular, if $X(L) \ne \emptyset$ for some finite extension L with $[L : k]$ odd.) Prove that $X \simeq \mathbb{P}^1_k$.

2.13. Let X be a nice k-curve of genus $g \ge 2$. Let $X \to Y$ be a degree-2 morphism to a nice k-curve Y of genus 0. Prove that if g is even, then $Y \simeq \mathbb{P}^1_k$. (Hint: consider a hyperplane section of the image of the canonical map.)

2.14. Verify that Theorem 2.9.4 implies the genus formulas for the smooth projective model of $y^2 = f(x)$ and for smooth plane curves.

2.15. Let $f = \sum a_{ij}x^i y^j$ be an irreducible Laurent polynomial. Let P be a convex lattice polygon containing $\{(i,j) \in \mathbb{Z}^2 : a_{ij} \ne 0\}$. Let X_0 be the (integral) subvariety of $(\mathbb{A}^1 - \{0\})^2$ defined by $f(x,y) = 0$. Let X be the smooth projective model of X_0. Give an example to show that the genus of X can sometimes equal the number of interior lattice points in P even if some side polynomial f_s is not squarefree.

2.16. Let P and X be as in Theorem 2.9.4, and suppose that X has genus ≥ 2. Prove that X is hyperelliptic if and only if the interior lattice points of P lie on a line.

2.17. Prove that for every $g \ge 3$ there exists a nice non-hyperelliptic $\mathbb{Q}$-curve of genus g.

2.18. Fix $g \geq 2$, and let k be an algebraically closed field of characteristic $\neq 2$. Using the characterization of hyperelliptic curves as curves for which the canonical embedding is of degree 2 to its image in $\mathbb{P}^{g-1}$, it is possible to show that there is a closed subvariety $\mathcal{H}_g$ of $\mathcal{M}_g$ such that the set $\mathcal{H}_g(k)$ is the subset of points in $\mathcal{M}_g(k)$ corresponding to hyperelliptic curves. This exercise computes $\dim \mathcal{H}_g$. Let Δ be the "big diagonal" in

$$(\mathbb{P}^1)^{2g+2} = \mathbb{P}^1 \times \cdots \times \mathbb{P}^1;$$

i.e., $\Delta(k)$ is the set of $(p_1, \ldots, p_{2g+2}) \in (\mathbb{P}^1)^{2g+2}(k)$ such that there exists $i \neq j$ with $p_i = p_j$. Let U be the quasi-projective variety $(\mathbb{P}^1)^{2g+2} - \Delta$.

(a) Describe an action of $\mathrm{PGL}_2(k)$ on $U(k)$ such that the orbits are in bijection with $\mathcal{H}_g(k)$. (Hint: consider branch points of a degree-2 map $X \to \mathbb{P}^1$.) Your bijection should also be compatible with extension of k to a larger algebraically closed field.

(b) Show that the stabilizer of any $u \in U(k)$ is finite.

(c) Assuming that this means that $\dim \mathcal{H}_g = \dim U - \dim \mathrm{PGL}_2$, find a formula for $\dim \mathcal{H}_g$.

(d) Prove in as many ways as you can, using whatever you want, that the following are equivalent for $g \geq 2$:

(i) $g = 2$.

(ii) $\mathcal{H}_g = \mathcal{M}_g$.

(iii) $\dim \mathcal{H}_g = \dim \mathcal{M}_g$.

It follows that for $g \geq 3$, "most" curves are non-hyperelliptic.

CHAPTER 3

The Weil conjectures

The Weil conjectures give information about the number of points of varieties over finite fields.

3.1. Some examples

3.1.1. Projective space. We have

$$\mathbb{P}^d(\mathbb{F}_q) = \frac{(\mathbb{F}_q)^{d+1} - \{\vec{0}\}}{\mathbb{F}_q^\times},$$

so

$$\#\mathbb{P}^d(\mathbb{F}_q) = \frac{q^{d+1}-1}{q-1} = 1 + q + q^2 + \cdots + q^d,$$

and by the same argument,

$$\#\mathbb{P}^d(\mathbb{F}_{q^n}) = 1 + (q)^n + (q^2)^n + \cdots + (q^d)^n.$$

On the other hand, for any smooth projective variety X over $\mathbb{C}$, we may consider $X(\mathbb{C})$ as a complex manifold and compute its Betti numbers, which are defined in terms of singular cohomology:

$$b_i := \operatorname{rk} H^i(X(\mathbb{C}), \mathbb{Z}).$$

For $\mathbb{P}^d(\mathbb{C})$, the Betti numbers are as follows:

i	0	1	2	3	4	$\cdots$	$2d$
b_i	1	0	1	0	1	$\cdots$	1

3.1.2. Elliptic curves. Let E be an elliptic curve over $\mathbb{F}_q$. Hasse proved that

$$\#E(\mathbb{F}_{q^n}) = 1 - (\alpha^n + \beta^n) + q^n$$

for some algebraic integers $\alpha, \beta \in \mathbb{C}$ (depending on q and E) such that $|\alpha| = |\beta| = q^{1/2}$ and $\alpha = q/\beta$.

On the other hand, the Betti numbers for an elliptic curve E over $\mathbb{C}$ are

i	0	1	2
b_i	1	2	1

What's going on here?

3.2. The Weil conjectures

Let $\overline{\mathbb{Z}}$ be the ring of all algebraic integers, i.e., the integral closure of $\mathbb{Z}$ in $\overline{\mathbb{Q}}$.

THEOREM 3.2.1 (Weil conjectures).

(i) *Let X be a variety 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 in addition X is smooth and projective of dimension d, then the plus and minus terms can be grouped as follows in alternating batches according to the absolute value of the terms:*

$$\#X(\mathbb{F}_{q^n}) = \sum_{j=1}^{b_0} \alpha_{0j}^n - \sum_{j=1}^{b_1} \alpha_{1j}^n + \sum_{j=1}^{b_2} \alpha_{2j}^n - \cdots + \sum_{j=1}^{b_{2d}} \alpha_{2d,j}^n,$$

where

- *The $b_i \in \mathbb{Z}_{\geq 0}$ are called the* ℓ-adic Betti numbers, *and they satisfy $b_{2d-i} = b_i$ for $i = 0, \ldots, 2d$.*
- *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 $|\ |$ on the number field $\mathbb{Q}(\alpha_{ij})$. (This is called the* Riemann hypothesis *for X.)*

If moreover X is geometrically irreducible, then

$$b_0 = 1 \qquad b_{2d} = 1$$
$$\alpha_{01} = 1 \qquad \alpha_{2d,1} = q^d.$$

(iii) *Suppose k is a number field. Fix an embedding $k \hookrightarrow \mathbb{C}$. Let X be a smooth projective variety of dimension d over k. Let $\mathfrak{p}$ be a prime of k such that X has good reduction at $\mathfrak{p}$. Then for $i = 0, \ldots, 2d$, the b_i in (ii) for the reduction (a variety over the finite residue field $\mathcal{O}_k/\mathfrak{p}$) equals* $\operatorname{rk} H^i(X(\mathbb{C}), \mathbb{Z})$.

REMARK 3.2.2. F. K. Schmidt proved these statements for curves, except for the Riemann hypothesis part, which was proved by Hasse for elliptic curves and Weil for arbitrary curves. Weil proved these statements also for abelian varieties.

Part (iii) is especially surprising, in that it hints at a connection between singular cohomology and varieties over finite fields.

Weil conjectured Theorem 3.2.1 in [Wei49], but also secretly[1] proposed an explanation inspired by algebraic topology. If M is a d-dimensional compact real manifold, and $f\colon M \to M$ is a reasonable map, then f induces a linear map $f^*\colon H^i(M,\mathbb{Q}) \to H^i(M,\mathbb{Q})$ on singular cohomology for each i, and the Lefschetz trace formula says that the number of fixed points of f equals the alternating sum $\sum_{i=0}^{d}(-1)^i \operatorname{Tr}\left(f^*|_{H^i(M,\mathbb{Q})}\right)$. Weil knew this, and observed that for a smooth projective variety X over $\mathbb{F}_q$, the number $\#X(\mathbb{F}_{q^n})$ equals the number of fixed points of F^n where $F\colon X \to X$ is the relative q-power Frobenius morphism. This led Weil to suggest that $\#X(\mathbb{F}_{q^n})$ should be computable as a similar alternating sum of the trace of F^n acting on some conjectural cohomology spaces that would act like singular cohomology but be defined also for varieties in characteristic p. The $\alpha_{i,*}$ in the i-th batch would then be simply the eigenvalues of F acting on the i-th cohomology space. Note that i should run from 0 to $2d$, just as a complex variety of dimension d is $(2d)$-dimensional as a real manifold.

Part (i) of Theorem 3.2.1 was proved for varieties of arbitrary dimension by Dwork using elementary p-adic methods. This shocked many people, because he did it without developing the new cohomology theory that people thought was needed.

Finally, étale cohomology (also called ℓ-adic cohomology) was developed by M. Artin, Grothendieck, and others to serve as the cohomology theory that Weil was looking for. In particular, they proved an ℓ-adic Lefschetz trace formula that gives

$$\#X(\mathbb{F}_q) = \sum_{i=0}^{2d}(-1)^i \operatorname{Tr}\left(F^*|_{H^i_{\text{et}}(\overline{X},\mathbb{Q}_\ell)}\right),$$

and succeeded in proving all of Theorem 3.2.1 except the Riemann hypothesis part, which was proved later by Deligne, again using étale cohomology. ♣♣♣ Bjorn: [add references]

3.3. The case of curves

If X is a nice genus-g curve over $\mathbb{C}$, then

$$\begin{aligned} H^0(X(\mathbb{C}),\mathbb{Z}) &\simeq \mathbb{Z} \\ H^1(X(\mathbb{C}),\mathbb{Z}) &\simeq \mathbb{Z}^{2g} \\ H^2(X(\mathbb{C}),\mathbb{Z}) &\simeq \mathbb{Z}. \end{aligned}$$

[1] He told his friends, but did not dare publish such a wild idea.

Analogously, if X is a nice genus-g curve over $\mathbb{F}_q$, then its ℓ-adic Betti numbers are given by

$$\begin{aligned} b_0 &= 1 \\ b_1 &= 2g \\ b_2 &= 1. \end{aligned}$$

The Weil conjectures in this case say that there exist $\lambda_1, \ldots, \lambda_{2g} \in \overline{\mathbb{Z}}$ with $|\lambda_j| = q^{1/2}$ and $\lambda_{g+i} = q/\lambda_i$ for $i = 1, \ldots, g$, such that for all $n \geq 1$,

$$\#X(\mathbb{F}_{q^n}) = 1 - (\lambda_1^n + \cdots + \lambda_{2g}^n) + q^n.$$

In particular, we get the Hasse-Weil bound:

$$\#X(\mathbb{F}_q) = q + 1 + \epsilon$$

for some "error" $\epsilon \in \mathbb{Z}$ with $|\epsilon| \leq 2g\sqrt{q}$.

3.4. Zeta functions

The Riemann zeta function is defined for $s \in \mathbb{C}$ with $\operatorname{Re} s > 1$ by

$$\begin{aligned} \zeta(s) = \zeta_{\operatorname{Spec}\mathbb{Z}}(s) &:= \sum_{n \geq 1} n^{-s} \\ &= \prod_{\text{primes } p} \left(1 - p^{-s}\right)^{-1} \\ &= \prod_{\text{maximal ideals } \mathfrak{m} \subseteq \mathbb{Z}} \left(1 - (\mathrm{N}\mathfrak{m})^{-s}\right)^{-1} \qquad (\text{where } \mathrm{N}\mathfrak{m} := \#(\mathbb{Z}/\mathfrak{m})). \end{aligned}$$

Analogously, one can define the zeta function of $\mathbb{A}^1_{\mathbb{F}_q}$ for $\operatorname{Re} s > 1$ by

$$\begin{aligned} \zeta_{\mathbb{A}^1_{\mathbb{F}_q}}(s) = \zeta_{\operatorname{Spec}\mathbb{F}_q[t]}(s) &= \prod_{\text{maximal ideals } \mathfrak{m} \subseteq \mathbb{F}_q[t]} \left(1 - (\mathrm{N}\mathfrak{m})^{-s}\right)^{-1} \qquad (\text{where } \mathrm{N}\mathfrak{m} := \#(\mathbb{F}_q[t]/\mathfrak{m})) \\ &= \prod_{\text{monic irreducible } f \in \mathbb{F}_q[t]} \left(1 - (q^{\deg f})^{-s}\right)^{-1} \\ &= \prod_{\text{closed points } P \in \mathbb{A}^1_{\mathbb{F}_q}} \left(1 - (q^{\deg P})^{-s}\right)^{-1} \\ &= \prod_{\text{closed points } P \in \mathbb{A}^1_{\mathbb{F}_q}} \left(1 - T^{\deg P}\right)^{-1} \quad \in \mathbb{Z}[[T]], \end{aligned}$$

where $T := q^{-s}$.

Definition 3.4.1. Let X be a variety over $\mathbb{F}_q$. Define

$$Z_X(T) := \prod_{\text{closed points } P \in X} \left(1 - T^{\deg P}\right)^{-1} \quad \in \mathbb{Z}[[T]],$$
$$\zeta_X(s) := Z_X(q^{-s}).$$

A priori, these are formal series, but in fact they converge for $|T| < 1/q^d$ and $\operatorname{Re} s > d$, respectively, where $d := \dim X$: see Exercise 6.

Remark 3.4.2. In fact, there is a common generalization of the Riemann zeta function and zeta functions of varieties over finite fields. Namely, for an arbitrary scheme X of finite type over $\mathbb{Z}$, define

$$\zeta_X(s) := \prod_{\text{closed points } P \in X} \left(1 - (\mathrm{N}P)^{-s}\right)^{-1},$$

where $\mathrm{N}P$ is the size of the residue field of P. For example, if $\mathcal{O}_F$ is the ring of integers of a number field F, then $\zeta_{\operatorname{Spec} \mathcal{O}_F}$ is the Dedekind zeta function of F.

Proposition 3.4.3. *Let X be a variety over $\mathbb{F}_q$. Then $Z_X(0) = 1$ and*

$$T \frac{d}{dT} \log Z_X(T) = \sum_{n=1}^{\infty} \# X(\mathbb{F}_{q^n}) T^n.$$

Equivalently,

$$Z_X(T) = \exp\left(\sum_{n=1}^{\infty} \# X(\mathbb{F}_{q^n}) \frac{T^n}{n} \right).$$

Proof. See Exercise 7. □

3.5. The Weil conjectures in terms of zeta functions

We can reformulate Theorem 3.2.1 in terms of $Z_X(T)$:

Theorem 3.5.1 (restatement of Weil conjectures).

(i) *Let X be a variety over $\mathbb{F}_q$. Then $Z_X(T)$ is (the Taylor series of) a rational function*

$$\frac{(1-\beta_1 T)\cdots(1-\beta_s T)}{(1-\alpha_1 T)\cdots(1-\alpha_r T)} \quad \in \mathbb{Q}(T).$$

(ii) *If moreover X is smooth and projective of dimension d, 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 $|\alpha_{ij}| = q^{i/2}$. Also,

$$Z_X\left(\frac{1}{q^d T}\right) = \pm q^{d\chi/2} T^{\chi} Z_X(T), \tag{3.5.2}$$

where $\chi := b_0 - b_1 + b_2 - \cdots + b_{2d}$ is the Euler characteristic *of X. (Equation* (3.5.2) *can be equivalently expressed as a functional equation relating $\zeta_X(s)$ to $\zeta_X(d-s)$.) If in addition X is geometrically irreducible, then $P_0(T) = 1-T$ and $P_{2d}(T) = 1-q^dT$.*

(iii) *Same as in Theorem 3.2.1.*

3.6. Characteristic polynomials

Let R be a commutative ring. Let V be a free R-module of rank n. Let $F \in \operatorname{End}_R(V)$. If we choose an R-basis of V, we can think of F as an $n \times n$ matrix over R.

The characteristic polynomial of F is $P(x) := \det(x\mathbf{1} - F) \in R[x]$, where $\mathbf{1} \in \operatorname{End} V$ is the identity. We have

$$P(x) = x^n + a_1x^{n-1} + \ldots + a_n$$

for some $a_i \in R$. The reverse characteristic polynomial of F is $P^{\text{rev}}(T) := \det(\mathbf{1} - TF) \in R[T]$. We have

$$P^{\text{rev}}(T) = T^nP(1/T) = 1 + a_1T + \ldots + a_nT^n$$

for the same $a_i \in R$ as above.

Example 3.6.1. Let X be a smooth projective d-dimensional variety over $\mathbb{F}_q$. The factor $P_i(T)$ in Theorem 3.5.1(ii) equals the reverse characteristic polynomial of the q-power Frobenius F acting on the $\mathbb{Q}_\ell$-vector space $H^i_{\text{et}}(\overline{X}, \mathbb{Q}_\ell)$: this is what one gets if in the formula for $Z_X(T)$ in Proposition 3.4.3 one replaces $\#X(\mathbb{F}_{q^n})$ with the alternating sum

$$\#X(\mathbb{F}_{q^n}) = \sum_{i=0}^{2d} (-1)^i \operatorname{Tr}\left((F^n)^*|_{H^i_{\text{et}}(\overline{X},\mathbb{Q}_\ell)} \right),$$

given by the Lefschetz trace formula. Thus

$$Z_X(T) = \prod_{i=0}^{2d} \det\left(\mathbf{1} - TF^*|_{H^i_{\text{et}}(\overline{X},\mathbb{Q}_\ell)}\right)^{(-1)^i}$$

as a rational function in $\mathbb{Q}(T)$.

3.7. Computing the zeta function of a curve

If X is a nice genus-g curve over $\mathbb{F}_q$, then

$$Z_X(T) = \frac{P_1(T)}{(1-T)(1-qT)} \tag{3.7.1}$$

where $P_1(T) = \prod_{i=1}^{2g}(1 - \lambda_iT)$ with $|\lambda_i| = \sqrt{q}$. The functional equation implies that

$$P_1(T) = 1 + a_1T + a_2T^2 + \cdots + a_gT^g + qa_{g-1}T^{g+1} + q^2a_{g-2}T^{g+2} + \cdots + q^gT^{2g} \tag{3.7.2}$$

for some numbers $a_1, a_2, \dots, a_g$.

Here is a naive algorithm for computing $Z_X(T)$ that works well if q and g are not too large:

(1) Compute the g values $\#X(\mathbb{F}_q)$, $\#X(\mathbb{F}_{q^2})$, $\dots$, $\#X(\mathbb{F}_{q^g})$. The size of $X(\mathbb{F}_{q^n})$ for $n = 1, \dots, g$ can be determined by simple counting: for instance, if X is hyperelliptic, loop over x-values in $\mathbb{F}_{q^n}$ and count how many y-values one gets for each x-value.

(2) Since

$$\begin{aligned} P_1(T) &= (1-T)(1-qT)Z_X(T) \\ &= (1-T)(1-qT)\exp\left(\sum_{n=1}^{g} \#X(\mathbb{F}_{q^n})\frac{T^n}{n} + O\left(T^{g+1}\right)\right), \end{aligned}$$

we compute the latter and expand into

$$=: 1 + a_1 T + a_2 T^2 + \cdots + a_g T^g + O\left(T^{g+1}\right)$$

to define $a_1, \dots, a_g \in \mathbb{Q}$. (In fact, the a_i will be integers.)

(3) Substitute these values into (3.7.2) to get $P_1(T)$.

(4) Substitute into (3.7.1) to get $Z_X(T)$.

Remark 3.7.3. If computing the next point count $\#X(\mathbb{F}_{q^{g+1}})$ is not too costly, its value can be used to check the computed $P_1(T)$.

Exercises

3.1. Verify Theorem 3.2.1 for (not necessarily irreducible) 0-dimensional varieties.

3.2. Show that every nice curve of genus ≤ 1 over a finite field has a rational point.

3.3. (a) Show that there is a nice genus 2 curve over $\mathbb{F}_3$ with $X(\mathbb{F}_3) = \emptyset$.

(b) Is there a nice genus 2 curve over $\mathbb{F}_2$ with $X(\mathbb{F}_2) = \emptyset$?

3.4. Prove that there is no nice genus-2 curve X over $\mathbb{F}_4$ with $\#X(\mathbb{F}_4) = 13$. (Hint: The hard way to do this is to write down all genus-2 curves over $\mathbb{F}_4$ up to isomorphism, and to count how many points each one has. The easy way is to calculate what $\#X(\mathbb{F}_{16})$ would have to be.)

3.5. Let X be a nice curve of genus g over $\mathbb{F}_q$.

(a) Show that $X(\mathbb{F}_{q^n}) \neq \emptyset$ for all sufficiently large n.

(b) Can you specify an explicit n_0 depending only on q and g such that $X(\mathbb{F}_{q^n}) \neq \emptyset$ for all $n \geq n_0$?

(c) Show that X has a divisor of degree 1.

3.6. Let X be a d-dimensional variety over $\mathbb{F}_q$.

(a) Without assuming the Weil conjectures, prove that there exists a constant c (depending on X) such that $\#X(\mathbb{F}_{q^n}) \leq cq^{nd}$ for all $n \geq 1$. (Suggestion: Reduce to the affine case, and choose an appropriate projection $\pi\colon X \to \mathbb{A}^d$. Use induction on d to handle the positive-dimensional fibers of π.)

(b) Show that the product defining $Z_X(T)$ converges for $|T| < 1/q^d$, and hence that $\zeta_X(s)$ converges for $\operatorname{Re} s > d$.

3.7. Prove Proposition 3.4.3. (Hint: use (2.2.6).)

3.8. Show that Theorem 3.2.1 is equivalent to Theorem 3.5.1.

3.9. How is the "Riemann hypothesis" in Theorem 3.2.1 analogous to the Riemann hypothesis for the Riemann zeta function? (Hint: If X is a nice curve over $\mathbb{F}_q$, where are the complex zeros of $\zeta_X(s)$?)

3.10. Let X be the Hermitian curve $x^{q+1} + y^{q+1} + z^{q+1} = 0$ in $\mathbb{P}^2$ over $\mathbb{F}_q$.

(a) Check that X is nice.

(b) Calculate the genus of X.

(c) Calculate $\#X(\mathbb{F}_{q^2})$.

(d) Compute the zeta function of $X_{\mathbb{F}_{q^2}}$.

(e) Calculate $\#X(\mathbb{F}_q)$.

(f) Compute the zeta function of X.

CHAPTER 4

Abelian varieties

4.1. Abelian varieties over arbitrary fields

4.1.1. The category of abelian varieties.

Definition 4.1.1. An abelian variety over a field k is a nice group variety over k. If A and B are abelian varieties, a homomorphism of abelian varieties $A \to B$ is just a homomorphism of group varieties $A \to B$.

We get a category of abelian varieties over k.

☡ Warning 4.1.2. In keeping with our terminology for morphisms, if A and B are abelian varieties over k, a homomorphism of abelian varieties $A \to B$ is automatically "defined over k". When we mean a homomorphism defined over $\overline{k}$, we will say a homomorphism $A_{\overline{k}} \to B_{\overline{k}}$.

Remark 4.1.3. It turns out that the group law on an abelian variety is commutative.

Examples 4.1.4.

(i) The empty variety cannot be made into an abelian variety, just as the empty set cannot be made into a group.

(ii) A 0-dimensional abelian variety is the same thing as a point $\operatorname{Spec} k$ (i.e., there is a unique way to define m, i, e for $G := \operatorname{Spec} k$).

(iii) A 1-dimensional abelian variety is the same thing an elliptic curve, as we now explain.

Suppose (E, O) is an elliptic curve. Here $O \in E(k)$ is the point that E comes equipped with. Then one can show that there is a unique choice of morphisms m, i, e making E into a 1-dimensional abelian variety with O as the identity (the image of e).

Conversely, suppose X is a 1-dimensional abelian variety. Let g be the genus of X as a curve. Let $O \in X(k)$ be the identity. One can show that if one takes a nonzero element of the cotangent space at O, and pulls it back by all the translation maps $X \to X$, one gets a nowhere-vanishing regular 1-form on X. Taking its degree gives $2g - 2 = 0$, so $g = 1$. Thus (X, O) is an elliptic curve.

(iv) If E and E' are elliptic curves, then $E \times E'$ is a 2-dimensional abelian variety.

4.1.2. Torsion.

Theorem 4.1.5. *Let k be a field, and let $\overline{k}$ be an algebraic closure of k. Let A be a g-dimensional abelian variety over k. Let $n \in \mathbb{Z}_{>0}$. Then*

(i) *The multiplication-by-n map $A(\overline{k}) \xrightarrow{n} A(\overline{k})$ is surjective.*

(ii) *Define the n-torsion subgroup of A as the kernel $A[n](\overline{k})$ of $A(\overline{k}) \xrightarrow{n} A(\overline{k})$.*

(a) *If $\operatorname{char} k \nmid n$, then $A[n](\overline{k}) \simeq (\mathbb{Z}/n\mathbb{Z})^{2g}$ as an abelian group.*

(b) *If $p := \operatorname{char} k > 0$, there is an integer r satisfying $0 \leq r \leq g$ such that $A[p^m](\overline{k}) \simeq (\mathbb{Z}/p^m\mathbb{Z})^r$ for any $m \in \mathbb{Z}_{\geq 0}$; here r is called the p-rank of A.*

Theorem 4.1.5 is plausible if one knows the special case of elliptic curves, but it cannot be deduced from that special case, because not every abelian variety is isomorphic to a product of elliptic curves. We will omit the proof of the theorem.

Remark 4.1.6. As the notation hints, $A[n](\overline{k})$ is the group of $\overline{k}$-point of a group scheme $A[n]$ over k. Here $A[n]$ is defined as the kernel of $A \xrightarrow{n} A$ in the category of group schemes. This kernel is defined as the fiber product

$$\begin{tikzcd}
A[n] \arrow[r, dotted] \arrow[d, dotted] & A \arrow[d, "n"] \\
\operatorname{Spec} k \arrow[r, "e"] & A
\end{tikzcd}$$

and it turns out to be isomorphic as a scheme to $\operatorname{Spec} R$ for a finite-dimensional k-algebra R. The rank of $A[n]$ is defined as $\dim_k R$, and it equals n^{2g}, even if $\operatorname{char} k \mid n$. What happens when $\operatorname{char} k \mid n$ is that $A[n]$ is non-reduced, so the group $A[n](k)$ has order less than n^{2g}, even if k is algebraically closed.

Warning 4.1.7. Sometimes, especially when $\operatorname{char} k \nmid n$, we will write $A[n]$ when we mean the group $A[n](\overline{k})$.

4.1.3. Abelian subvarieties.

Definition 4.1.8. Let A be an abelian variety. An abelian subvariety B of A is a closed subvariety $B \subseteq A$ with its own m, i, e making it an abelian variety such that the inclusion morphism $B \to A$ is a homomorphism of abelian varieties. (In other words, the m, i, e for A must induce a group structure on the subvariety B.)

Warning 4.1.9. If B is an abelian subvariety of A, there need not exist another abelian subvariety C of A such that the map $B \times C \to A$ obtained by restriction the group operation m is an isomorphism.

Definition 4.1.10. An abelian variety A is called simple if it has exactly two abelian subvarieties: $\{O\} = \operatorname{Spec} k$ and A itself.

Warning 4.1.11. The trivial abelian variety is not simple, just as 1 is not a prime number!

Warning 4.1.12. Let A be an abelian variety over k, and let $L \supseteq k$ be a field extension. If A_L is simple, then A is simple. But the converse does not hold in general: abelian varieties, like polynomials, can decompose further when the ground field is enlarged.

Definition 4.1.13. An abelian variety A over k is geometrically simple if $A_{\overline{k}}$ is simple.

If $A_{\overline{k}}$ has a nonzero abelian subvariety other than itself, then that abelian subvariety can be defined using finitely many elements of $\overline{k}$. Thus A is geometrically simple if and only if A_L is simple for every finite extension $L \supseteq k$.

4.1.4. Isogenies.

Definition 4.1.14. An isogeny of abelian varieties $A \to B$ over a field k is a homomorphism of abelian varieties such that $A(\overline{k}) \to B(\overline{k})$ is surjective with finite kernel. If an isogeny exists, then A and B are called isogenous and we write $A \sim B$.

Warning 4.1.15. As in Warning 4.1.2, isogenies between k-varieties are automatically defined over k.

Remark 4.1.16. If A and B are isogenous abelian varieties, then $\dim A = \dim B$.

Remark 4.1.17. Suppose $\phi\colon A \to B$ is an isogeny. Then ϕ is a dominant rational map, so it induces an inclusion of function fields $\mathbf{k}(B) \hookrightarrow \mathbf{k}(A)$. Since $\dim A = \dim B$, this is a finite extension of fields. Thus we may define the notions of degree and separability, just as we did in Section 2.1.3 for dominant maps between curves. One can show that $\deg \phi$ equals the rank of the group scheme $A[\phi] := \ker \phi$; if moreover ϕ is separable, this rank equals $\# A[\phi](\overline{k}) = \# \ker \big(A(\overline{k}) \to B(\overline{k})\big)$.

Example 4.1.18. Let A be a g-dimensional abelian variety, and let $n \in \mathbb{Z}_{>0}$. Then the multiplication-by-n map $A \to A$ is an isogeny, by Theorem 4.1.5. By Remark R:A[n], its degree is n^{2g}.

Proposition 4.1.19. *If $\phi\colon A \to B$ is an isogeny of degree m between g-dimensional abelian varieties then there exists a unique isogeny $\psi\colon B \to A$ of degree m^{2g-1} such that $\psi \circ \phi = m$ (the multiplication-by-m map on A).*

Proof. (Sketch) This follows from the fact that the kernel of ϕ is contained in the kernel of m on A. □

Thus $A \sim B$ is an equivalence relation.

☡ Warning 4.1.20. The relationship between ϕ and ψ in Proposition 4.1.19 is not a duality if $g > 1$: i.e., if one does the operation twice then one does not return to ϕ. (Even the degree is wrong.)

4.1.5. Decomposition.

Theorem 4.1.21 (Poincaré irreducibility theorem). *Let B be an abelian subvariety of A. Then there exists another abelian subvariety $C \subseteq A$ such that the "addition" map $B \times C \to A$ obtained by restricting m is an isogeny.*

Corollary 4.1.22 (Decomposition up to isogeny). *Let A be an abelian variety. Then there exist pairwise non-isogenous simple abelian varieties $A_1, \ldots, A_r$ and positive integers $n_1, \ldots, n_r$ such that $A \sim A_1^{n_1} \times \cdots \times A_r^{n_r}$. This decomposition is unique up to isogeny; i.e., if also $A \sim B_1^{m_1} \times \cdots \times B_s^{m_s}$ is another decomposition of the same type, then $r = s$, and after permuting the terms we have $A_i \sim B_i$ and $n_i = m_i$ for all i.*

☡ Warning 4.1.23. Not every abelian variety is *isomorphic* to a product of simple abelian varieties.

4.1.6. Vector spaces associated to an abelian variety.

Let A be a g-dimensional abelian variety over a field k. Here are four vector spaces associated to A.

(1) Define $\operatorname{Lie} A$ as the Zariski tangent space to A at the identity $O \in A(k)$.

(2) The space $H^0(A, \Omega^1)$ of regular 1-forms on A is also the space of translation-invariant 1-forms on A, which is isomorphic to the cotangent space of A at O.

(3) Let $\ell \neq \operatorname{char} k$ be a prime. Let $A[\ell^n]$ mean $A[\ell^n](\overline{k})$. The ℓ-adic Tate module of A is the inverse limit

$$T_\ell A := \varprojlim_n A[\ell^n],$$

with respect to the multiplication-by-ℓ maps $A[\ell^{n+1}] \xrightarrow{\ell} A[\ell^n]$. It follows from Theorem 4.1.5 that $T_\ell A$ is a free $\mathbb{Z}_\ell$-module of rank $2g$. Moreover, it comes equipped with an action of $\operatorname{Gal}(\overline{k}/k)$; i.e., there is a homomorphism

$$\operatorname{Gal}(\overline{k}/k) \to \operatorname{Aut}_{\mathbb{Z}_\ell} T_\ell A.$$

Sometimes it is more convenient to have a vector space over a field instead of a module over a ring like $\mathbb{Z}_\ell$, so we also define a $\mathbb{Q}_\ell$-vector space

$$V_\ell A := T_\ell A \underset{\mathbb{Z}_\ell}{\otimes} \mathbb{Q}_\ell.$$

(4) Let $\ell \neq \operatorname{char} k$ be a prime. Then one can define $H^1_{\text{et}}(\overline{A}, \mathbb{Q}_\ell)$, where $\overline{A} := A \underset{k}{\otimes} \overline{k}$.

Each of these four constructions gives a functor (possibly contravariant) from the category of abelian varieties over k to the category of finite-dimensional vector spaces over k or $\mathbb{Q}_\ell$. Some have an action of $G := \operatorname{Gal}(\overline{k}/k)$. This is summarized in the following table.

Vector space	Over what field?	Dimension	Functoriality	Remarks
$\operatorname{Lie} A$	k	g	covariant	
$H^0(A, \Omega_1)$	k	g	contravariant	dual to $\operatorname{Lie} A$
$V_\ell A$	$\mathbb{Q}_\ell$	$2g$	covariant	has G-action
$H^1_{\text{et}}(\overline{A}, \mathbb{Q}_\ell)$	$\mathbb{Q}_\ell$	$2g$	contravariant	dual to $V_\ell A$, has G-action

Proposition 4.1.24. *Each of the four functors above takes an isogeny ϕ to an isomorphism of vector spaces, provided that the vector spaces under consideration are over a field of characteristic* 0*, or at least of characteristic not dividing* $\deg \phi$*.*

Proof. The inverse map is induced by ψ composed with multiplication by $(\deg \phi)^{-1}$, where ψ is as in Proposition 4.1.19. □

Remark 4.1.25. Here we explain that Tate modules are like lattices and also like homology groups.

Suppose A is an abelian variety over $\mathbb{C}$. Section 4.3 will show that $A(\mathbb{C}) \simeq \mathbb{C}^g/\Lambda$ analytically for some lattice Λ. There is no way to construct a lattice associated to abelian varieties over all fields (see Exercise 15), but Tate modules can be viewed as the best approximation. Tate modules are a good analogue, because one can show that for A over $\mathbb{C}$, one has $T_\ell A \simeq \Lambda \otimes \mathbb{Z}_\ell$.

Moreover, Λ can be identified with $H_1(A(\mathbb{C}), \mathbb{Z})$. Because of this, and because $V_\ell A$ is dual to $H^1_{\text{et}}(\overline{A}, \mathbb{Q}_\ell)$, it is reasonable to think of $T_\ell A$ for any A over k as being an étale *homology* group. One could even denote it as $H_1^{\text{et}}(\overline{A}, \mathbb{Z}_\ell)$.

4.2. Abelian varieties over finite fields

4.2.1. Newton polygon of a one-variable polynomial over a valued field.

Definition 4.2.1. Let S be a set of points in $\mathbb{R}^2$. The lower convex hull of S is the intersection of all the half-spaces of the form $\{ (x, y) \in \mathbb{R}^2 : y \geq ax + b \}$ that contain S.

If S is a finite set, then the lower convex hull of S will consist of the graph of a piecewise-linear convex function on an interval, together with all the points directly above it. The graph will be a union of line segments whose slopes are strictly increasing as one goes from left to right. Define the width of a segment from (a, b) to (a', b') (with $a < a'$) to be $a' - a$.

Definition 4.2.2. Let K be a field with a nonarchimedean valuation $v \colon K^\times \to G$ where G is an additive subgroup of $\mathbb{R}$. Let $P(t) = \sum_{i=0}^n a_i t^i \in K[t]$ be a polynomial. The Newton polygon of P is the lower convex hull of the finite set $\{ (i, v(a_i)) : 0 \leq i \leq n \text{ and } a_i \neq 0 \}$ in $\mathbb{R}^2$.

The following theorem is the main reason for introducing Newton polygons.

Theorem 4.2.3. *Suppose in addition that K is algebraically closed. Then for each $s \in \mathbb{R}$,*

$$\#\{ \alpha \in K : P(\alpha) = 0 \text{ and } v(\alpha) = -s \} \quad = \quad \textit{the width of the segment of slope } s,$$

where the right hand side is to be interpreted as 0 *if there is no segment of slope s.*

☡ Warning 4.2.4. Many people draw their Newton polygons backwards: i.e., they write their polynomial in the form $\sum_{i=0}^n a_i t^{n-i}$ and then take the lower convex hull of $\{ (i, v(a_i)) : 0 \leq i \leq n \text{ and } a_i \neq 0 \}$. This eliminates the minus-sign in Theorem 4.2.3, but is problematic when one tries to generalize to power series, as we will do in Section **??**.

4.2.2. Characteristic polynomial of Frobenius. Let $\mathbb{F}_q$ be a finite field of characteristic p. Let A be an abelian variety over $\mathbb{F}_q$ of dimension g. The relative q-power Frobenius morphism $F \colon A \to A$ is the morphism that maps each point to a point whose coordinates are the q-th power of the original coordinates. It is an endomorphism of the abelian variety A.

Fix a prime $\ell \neq \operatorname{char} \mathbb{F}_q$. Then F induces $F|_{T_\ell A} \in \operatorname{End}_{\mathbb{Z}_\ell}(T_\ell A)$, which may be thought of as a $2g \times 2g$ matrix if we choose a $\mathbb{Z}_\ell$-basis of $T_\ell A$. Define its characteristic polynomial

$$P_A(x) := \det(x\mathbf{1} - F|_{T_\ell A}) \in \mathbb{Z}_\ell[t].$$

Obviously, $P_A(x)$ is monic of degree $2g$. Amazingly, its coefficients are in $\mathbb{Z}$ and are independent of the choice of ℓ (as the notation prematurely suggested).

Remark 4.2.5. The duality between the $\mathbb{Q}_\ell$-vector spaces $V_\ell A$ and $H^1_{\text{et}}(\overline{A}, \mathbb{Q}_\ell)$ implies that $P_A(x)$ equals the characteristic polynomial of F acting on $H^1_{\text{et}}(\overline{A}, \mathbb{Q}_\ell)$. On the other hand, by Example 3.6.1, the polynomial $P_1(T)$ in the factorization of $Z_X(T)$ in Theorem 3.5.1(ii) equals the reverse of the characteristic polynomial of F acting on $H^1_{\text{et}}(\overline{A}, \mathbb{Q}_\ell)$. Thus

$$P_1(T) = T^n P_A(T^{-1}).$$

Remark 4.2.6. For any nice variety X, there is a canonical "cup-product" morphism

$$\bigwedge^i H^1_{\text{et}}(\overline{X}, \mathbb{Q}_\ell) \to H^i_{\text{et}}(\overline{X}, \mathbb{Q}_\ell).$$

For an abelian variety A it turns out to be an isomorphism. Therefore if $\lambda_1, \ldots, \lambda_{2g}$ are the eigenvalues of the q-power Frobenius endomorphism acting on $H^1_{\text{et}}(\overline{A}, \mathbb{Q}_\ell)$, the corresponding eigenvalues for $H^2_{\text{et}}(\overline{X}, \mathbb{Q}_\ell)$ are the products $\lambda_i \lambda_j$ with $i < j$, and so on. In this case, the Lefschetz trace formula gives

$$\begin{aligned} \#A(\mathbb{F}_q) &= 1 - \sum_i \lambda_i + \sum_{i<j} \lambda_i \lambda_j - \cdots + \lambda_1 \lambda_2 \cdots \lambda_{2g} \\ &= (1 - \lambda_1) \cdots (1 - \lambda_{2g}) \\ &= P_1(1) \\ &= P_A(1). \end{aligned}$$

Here are a few other facts:

- If $A \sim B$, then $P_A(x) = P_B(x)$. This follows from Proposition 4.1.24.
- If $A \sim \prod A_i^{n_i}$ is a decomposition of an abelian variety up to isogeny into simple factors, then $P_A(x) = \prod P_{A_i}(x)^{n_i}$.
- The polynomial $P_A(x)$ factors over $\mathbb{C}$ as $P_A(x) = \prod_{i=1}^{2g}(x - \lambda_i)$ with $|\lambda_i| = \sqrt{q}$. This follows from the Riemann hypothesis for A: see Theorem 3.5.1(iii).

Definition 4.2.7. Let q be a power of p. Let the q-valuation $v \colon \overline{\mathbb{Q}}_p^\times \to \mathbb{Q}$ be the p-adic valuation *normalized so that* $v(q) = 1$. Given a polynomial $h(x) \in \overline{\mathbb{Q}}_p[x]$, define its

q-Newton polygon to be the Newton polygon of $h(x)$ with respect to v. (This terminology is not standard.)

Definition 4.2.8. Let A be an abelian variety over $\mathbb{F}_q$. The Newton polygon of A is the q-Newton polygon of $P_A(x)$.

Remark 4.2.9. There is a different definition of the Newton polygon of an abelian variety over a field k of characteristic p that gives the same notion when k is finite, but makes sense even if k is not finite.

4.2.3. Honda-Tate theory. Fix a finite field $\mathbb{F}_q$. Honda-Tate theory classifies abelian varieties over $\mathbb{F}_q$ up to isogeny (over $\mathbb{F}_q$).

Definition 4.2.10. A q-Weil number is an algebraic integer in $\overline{\mathbb{Q}}$ all of whose $\operatorname{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$-conjugates have complex absolute value $\sqrt{q}$.

Warning 4.2.11. An algebraic integer in $\overline{\mathbb{Q}}$ all of whose $\operatorname{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$-conjugates have complex absolute value 1 is a root of unity, but a q-Weil number need not be $\sqrt{q}$ times a root of unity. Consider, for instance, the 5-Weil number $2 + \sqrt{-1}$.

Theorem 4.2.12 (Honda-Tate).

(i) *If A is a simple abelian variety, then $P_A(x) = h(x)^e$ for some* irreducible *polynomial $h(x) \in \mathbb{Z}[x]$ and some $e \geq 1$.*

(ii) *There is a bijection*

$$\begin{array}{rcl} \left\{ \begin{array}{c} \textit{isogeny classes of} \\ \textit{simple abelian varieties over } \mathbb{F}_q \end{array} \right\} & \to & \left\{ \begin{array}{c} \textit{conjugacy classes of} \\ q\textit{-Weil numbers} \end{array} \right\} \\ \textit{isogeny class of } A & \mapsto & \textit{the set of zeros of } P_A(x). \end{array}$$

(iii) *Given a $\operatorname{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$-conjugacy class of q-Weil numbers, let $h(x)$ be the minimal polynomial of any number in this conjugacy class. Then there exists a unique $e \geq 1$ such that $h(x)^e$ is $P_A(x)$ for some simple abelian variety A over $\mathbb{F}_q$: it is the smallest positive integer such that*

  (a) *$h(0)^e > 0$, and*

  (b) *For each monic $\mathbb{Q}_p$-irreducible factor $g(x) \in \mathbb{Q}_p[x]$ of $h(x)$, the q-valuation $v(g(0)^e)$ is in $\mathbb{Z}$.*

Corollary 4.2.13 (Tate). *Two abelian varieties A and A' over $\mathbb{F}_q$ are isogenous if and only if $P_A = P_{A'}$.*

PROOF. We have already seen that $A \sim A'$ implies $V_\ell A \simeq V_\ell A'$ as $\operatorname{Gal}(\overline{\mathbb{F}}_q/\mathbb{F}_q)$-modules, and hence implies $P_A = P_{A'}$. The converse follows from the injectivity in Theorem 4.2.12(ii): the multiplicity of a simple abelian variety B in A can be read off from P_A as the power of P_B that divides P_A. □

REMARK 4.2.14. Let A be a simple abelian variety over $\mathbb{F}_q$, and let π be a corresponding q-Weil number. Then $E := \mathbb{Q} \otimes \operatorname{End} A$ can be described in terms of π as follows. It is a finite-dimensional central division algebra of dimension e^2 over the field $K := \mathbb{Q}(\pi)$, where e is as in Theorem 4.2.12(iii). Any such algebra can be described by giving its invariant at each place v of K, i.e., by giving the class of $E \otimes K_v$ in $\operatorname{Br} K_v \hookrightarrow \mathbb{Q}/\mathbb{Z}$. For E coming from A as above, the invariant is the image in $\mathbb{Q}/\mathbb{Z}$ of the $i_v \in \mathbb{Q}$ satisfying $\|\pi\|_v = q^{-i_v}$, where $\| \, \|_v$ is the normalized[1] absolute value on K_v.

REMARK 4.2.15. It is impossible to express $\operatorname{End} A$ itself in terms of π, since isogenous simple abelian varieties can have different endomorphism rings.

REMARK 4.2.16. Let $M(\mathbb{F}_q)$ be the "category of abelian varieties over $\mathbb{F}_q$ up to isogeny": the objects of $M(\mathbb{F}_q)$ are abelian varieties over $\mathbb{F}_q$, but the arrows from A to B are defined to be elements of $\mathbb{Q}\otimes\operatorname{Hom}(A, B)$. Isogenies have inverses in $M(\mathbb{F}_q)$, and hence are isomorphisms in $M(\mathbb{F}_q)$. Whereas the category of abelian varieties over $\mathbb{F}_q$ with the usual homomorphisms is only an additive category (kernels do not exist within the category), $M(\mathbb{F}_q)$ is an abelian category, and is even semisimple, because of Corollary 4.1.22. Then Theorem 4.2.12 and Remark 4.2.14 together give a complete description of $M(\mathbb{F}_q)$.

Some good references for this section are [Tat], [Wat69], and [WM71].

4.2.4. Ordinary abelian varieties.

THEOREM 4.2.17. *Let A be an abelian variety over $\mathbb{F}_q$. Let $v\colon \overline{\mathbb{Q}}_p^\times \to \mathbb{Q}$ be the p-adic valuation normalized so that $v(q) = 1$. Then the following are equivalent:*

(i) *The Newton polygon of A is as low as possible: the diagonal line segment from $(0, g)$ to $(g, 0)$ followed by the horizontal line segment from $(g, 0)$ to $(2g, 0)$.*

(ii) *The middle coefficient of $P_A(x)$ is not divisible by p.*

(iii) *Half of the zeros of $P_A(x)$ in $\overline{\mathbb{Q}}_p$ are p-adic units and the other half have q-valuation 1.*

[1] The normalization is such that $\|\alpha\|_v$ is the amount that the multiplication-by-α map on K_v scales volume (Haar measure) by. More concretely, if v lies above p, then $\|\alpha\|_v := |N_{K_v/\mathbb{Q}_p}(\alpha)|_p$, where $| \, |_p$ is the usual p-adic absolute value on $\mathbb{Q}_p$ normalized by $|p|_p = 1/p$ (or the usual absolute value on $\mathbb{Q}_\infty = \mathbb{R}$, if $p = \infty$). This normalization also makes the product formula $\prod_v \|\alpha\|_v = 1$ true, for any $\alpha \in K^\times$.

(iv) *Every monic irreducible factor $h(x) \in \mathbb{Z}[x]$ of $P_A(x)$ has even degree and has middle coefficient not divisible by p.*

(v) *The size of the subgroup $A[p] \subseteq A(\overline{\mathbb{F}}_q)$ is as large as possible: p^g.*

If (any of) these conditions are satisfied, then A is called ***ordinary****.*

Remark 4.2.18. In general, the p-rank of A equals the width of the slope-zero segment of the Newton polygon of A.

One can show (see Exercise 10) that for an ordinary simple abelian variety A over $\mathbb{F}_q$, the integer e of Theorem 4.2.12(iii) equals 1. Thus for any ordinary abelian variety A over $\mathbb{F}_q$, the factorization of $P_A(x)$ corresponds *exactly* to the decomposition of A up to isogeny into simple abelian varieties.

Remark 4.2.19. Although we have been classifying abelian varieties only up to isogeny, Deligne has used the theory of the Serre-Tate canonical lift to describe the category of ordinary abelian varieties over $\mathbb{F}_q$ up to *isomorphism*: see [Del69].

4.2.5. Supersingular abelian varieties.

Theorem 4.2.20. *Let A be an abelian variety over $\mathbb{F}_q$. The following are equivalent:*

(i) *The Newton polygon of A is as high as possible: the straight line segment of slope $-1/2$ from $(0, g)$ to $(2g, 0)$.*

(ii) *All zeros of $P_A(x)$ in $\overline{\mathbb{Q}}_p$ have q-valuation $1/2$.*

(iii) *Each complex zero of $P_A(x)$ is a root of unity times $\sqrt{q}$.*

(iv) *There exists a non-ordinary[2] elliptic curve E over $\overline{\mathbb{F}}_q$ such that $\overline{A} := A_{\overline{\mathbb{F}}_q}$ is isogenous to E^g.*

(v) *For any non-ordinary elliptic curves $E_1, \dots, E_g$ over $\overline{\mathbb{F}}_q$, the abelian variety $\overline{A}$ is isogenous to $E_1 \times \cdots \times E_g$.*

If (any of) these conditions are satisfied, then A is called ***supersingular****.*

Warning 4.2.21. It is not true in general that A is supersingular if and only if $A[p](\overline{\mathbb{F}}_p) = 0$. See Exercise 13.

Warning 4.2.22. There are many abelian varieties that are neither ordinary nor supersingular: their Newton polygons lie between the two extremes. And over every finite field, there is exactly one abelian variety up to isomorphism that is both ordinary and supersingular!

[2] One could also write "supersingular" here, once the term has been defined!

4.2.6. Extending the ground field. Let A be an abelian variety of dimension g over $\mathbb{F}_q$, and let $n \geq 1$. Let $A' = A_{\mathbb{F}_{q^n}}$. Then $P_{A'}(x) \in \mathbb{Z}[x]$ is the monic polynomial of degree $2g$ whose zeros are the n^{th} powers of the zeros of $P_A(x)$, counted with multiplicity. Hence $P_{A'}(x)$ can be computed as the resultant of $P_A(t)$ and $t^n - x$ with respect to t.

The Newton polygon of A' (with respect to the q^n-valuation) equals the Newton polygon of A (with respect to the q-valuation). Thus A' is ordinary if and only if A is, and A' is supersingular if and only if A is, and the p-rank of A' equals that of A.

Warning 4.2.23. As in Warning 4.1.12, if A is simple, it may still be that A' is not simple.

4.2.7. Example. Suppose A is an abelian variety over $\mathbb{F}_2$, and suppose it is known that

$$P_A(x) = (x^2 - 2)^2(x^4 + x^3 + x^2 + 2x + 4)^2.$$

What can we say about the splitting of A?

First of all, $\dim A = \frac{1}{2} \deg P_A = 6$. Let $\alpha \in \mathbb{C}$ be a zero of the irreducible polynomial $x^4 + x^3 + x^2 + 2x + 4$. The decomposition of A up to isogeny into simple abelian varieties over $\mathbb{F}_2$ will involve two non-isogenous factors B and B' corresponding to the 2-Weil numbers $\sqrt{2}$ and α, but to determine their dimensions and the power to which they appear in A, we must do more work. For the factor $h(x) := x^2 - 2$, the integer e must be 2, in order to make $h(0)^e > 0$ (the second condition is automatic). (It follows that there is no abelian variety over $\mathbb{F}_2$ with characteristic polynomial $x^2 - 2$ or any odd power of $x^2 - 2$.) Hence $P_B(x) = (x^2 - 2)^2$. Moreover, B is supersingular, since the roots of $P_B(x)$ in $\overline{\mathbb{Q}}_2$ have 2-adic valuation $1/2$.

On the other hand, the factor $h'(x) := x^4 + x^3 + x^2 + 2x + 4$ has middle coefficient 1 not divisible by 2, so it corresponds to an ordinary simple abelian variety over $\mathbb{F}_2$, and e equals 1 for it. In other words, $P_{B'}(x) = x^4 + x^3 + x^2 + 2x + 4$, and B' is an ordinary 2-dimensional abelian variety over $\mathbb{F}_2$ appearing with multiplicity 2 in A. To summarize, $A \sim B \times (B')^2$ where $\dim B = \dim B' = 2$.

Now we consider splitting of B over $\mathbb{F}_4$. The zeros of $P_B(x)$ are $\sqrt{2}, \sqrt{2}, -\sqrt{2}, -\sqrt{2}$; squaring these shows that $P_{B_{\mathbb{F}_4}}(x) = (x - 2)^4$. The e corresponding to the 4-Weil number 2 is 2, since $h(x) = x - 2$ must be squared to make its constant term positive and to make the 4-valuation of its value at 0 an integer. Hence $B_{\mathbb{F}_4} \sim E^2$ for a simple abelian variety E over $\mathbb{F}_4$ with $P_E(x) = (x - 2)^2$; here E must be a supersingular elliptic curve over $\mathbb{F}_4$. We cannot get further splitting of B by enlarging the ground field again, since E is already 1-dimensional.

We now prove that B' is geometrically simple. Equivalently, we prove that $B'_{\mathbb{F}_{2^n}}$ is simple for all $n \geq 1$. We have

$$\begin{aligned} B'_{\mathbb{F}_{2^n}} \text{ is simple } &\iff P_{B'_{\mathbb{F}_{2^n}}}(x) \text{ is irreducible} \qquad \text{(since } B' \text{ is ordinary)} \\ &\iff \alpha^n \text{ has degree 4 over } \mathbb{Q} \\ &\iff \alpha^n \text{ does not lie in a proper subfield of } \mathbb{Q}(\alpha). \end{aligned}$$

But one can check, by computing the Galois group of $h'(x)$ for instance, that the only proper subfields of $\mathbb{Q}(\alpha)$ are $\mathbb{Q}$ and $\mathbb{Q}(\beta)$, where $\beta = \alpha + 2/\alpha = \frac{-1+\sqrt{13}}{2}$ generates the subfield fixed by the complex conjugation automorphism σ of $\mathbb{Q}(\alpha)$, taking α to $2/\alpha$. Thus if α^n were in a proper subfield, we would have ${}^\sigma(\alpha^n) = \alpha^n$, and ${}^\sigma\alpha/\alpha$ would be a root of unity. But one can check that the minimal polynomial of ${}^\sigma\alpha/\alpha = 2/\alpha^2$ over $\mathbb{Q}$ is $x^4 + x^3/2 + 5x^2/4 + x/2 + 1$, so ${}^\sigma\alpha/\alpha$ is not even an algebraic integer. Thus B' is geometrically simple, and the decomposition of A_k for any field k containing $\mathbb{F}_4$ is $A_k \sim (E_k)^2 \times (B'_k)^2$.

4.3. Abelian varieties over $\mathbb{C}$

If E is an elliptic curve over $\mathbb{C}$, then $E(\mathbb{C})$ is analytically isomorphic to $\mathbb{C}/\Lambda$ for some rank-2 discrete $\mathbb{Z}$-submodule of $\mathbb{C}$. The expected generalization to abelian varieties holds:

Theorem 4.3.1 (Uniformization of abelian varieties). *Let A be an abelian variety of dimension g over $\mathbb{C}$. Then:*

(i) *There exists an analytic isomorphism $e\colon \mathbb{C}^g/\Lambda \to A(\mathbb{C})$ of Lie groups over $\mathbb{C}$, where Λ is a discrete subgroup of $\mathbb{C}^g$ isomorphic to $\mathbb{Z}^{2g}$.*

(ii) *The inverse isomorphism e^{-1} can be obtained by integrating some basis $\omega_1, \dots, \omega_g$ of the space $H^0(A, \Omega^1)$ of translation-invariant 1-forms:*

$$\begin{aligned} e^{-1}\colon A(\mathbb{C}) &\to \mathbb{C}^g/\Lambda \\ P &\mapsto \int_O^P (\omega_1, \dots, \omega_g). \end{aligned}$$

(Although the integral on the right depends on a choice of path from O to P in $A(\mathbb{C})$, its value is well-defined modulo Λ.)

Proof.

(i) Since A is smooth, the group $A(\mathbb{C})$ is a Lie group over $\mathbb{C}$. Since A is commutative, $A(\mathbb{C})$ is commutative. Since A is projective, $A(\mathbb{C})$ is compact. Since A is connected, one can show that $A(\mathbb{C})$ is connected. These are the only facts about $A(\mathbb{C})$ that we will use to get e.

Choose a $\mathbb{C}$-basis of $\operatorname{Lie} A$ to get an isomorphism $\operatorname{Lie} A \simeq \mathbb{C}^g$. The exponential map $\exp\colon \operatorname{Lie} A \to A(\mathbb{C})$ is a homomorphism since $A(\mathbb{C})$ is commutative, and it is a local diffeomorphism at 0, so its image is an open subgroup of $A(\mathbb{C})$. But $A(\mathbb{C})$ is connected, so its only open subgroup is $A(\mathbb{C})$ itself. Thus exp is surjective and induces an isomorphism $\mathbb{C}^g/\Lambda \simeq A(\mathbb{C})$, where $\Lambda := \ker(\exp)$. Since exp is a local diffeomorphism, Λ is discrete, so $\Lambda = \mathbb{Z}\lambda_1 + \cdots + \mathbb{Z}\lambda_r \subseteq \operatorname{Lie} A$ for some $\mathbb{R}$-independent elements $\lambda_1, \ldots, \lambda_r \in \operatorname{Lie} A$. Extending $(\lambda_1, \ldots, \lambda_r)$ to an $\mathbb{R}$-basis shows that then $\mathbb{C}^g/\Lambda \simeq (\mathbb{R}/\mathbb{Z})^r \oplus \mathbb{R}^{2g-r}$ as a Lie group over $\mathbb{R}$. But it is isomorphic to the compact group $A(\mathbb{C})$, so $2g - r = 0$, and $\Lambda \simeq \mathbb{Z}^{2g}$.

(ii) If $z_1, \ldots, z_g$ are the coordinate functions on the $\mathbb{C}^g$, then $dz_1, \ldots, dz_g$ form a basis for the translation-invariant holomorphic 1-forms on $\mathbb{C}^g/\Lambda$, so they must correspond under e to a basis $\omega_1, \ldots, \omega_g$ of $H^0(A, \Omega^1)$. (In fact, it is the basis dual to the chosen basis of $\operatorname{Lie} A$.)

The map

$$\begin{aligned} \mathbb{C}^g &\to \mathbb{C}^g \\ P &\mapsto \int_0^P (dz_1, \ldots, dz_g) \end{aligned}$$

is the identity, and induces the identity

$$\begin{aligned} \mathbb{C}^g/\Lambda &\to \mathbb{C}^g/\Lambda \\ P &\mapsto \int_0^P (dz_1, \ldots, dz_g). \end{aligned}$$

The latter integral depends on a choice of path from 0 to P in $\mathbb{C}^g/\Lambda$, but changing the path changes its value only by an element of Λ, so the image in $\mathbb{C}^g/\Lambda$ is well-defined. Precomposing with $e^{-1}\colon A(\mathbb{C}) \to \mathbb{C}^g/\Lambda$ shows that the map

$$\begin{aligned} A(\mathbb{C}) &\to \mathbb{C}^g/\Lambda \\ P &\mapsto \int_O^P (\omega_1, \ldots, \omega_g). \end{aligned}$$

is e^{-1}. In particular, the integral again is well-defined modulo Λ. □

Remark 4.3.2. Here we give a natural coordinate-free reinterpretation of $\mathbb{C}^g/\Lambda$. First, $\mathbb{C}^g$ is really $\operatorname{Lie} A \simeq H^0(A, \Omega^1)^\vee$, as the proof of Theorem 4.3.1(i) showed. Second, we claim that Λ is really $H_1(A(\mathbb{C}), \mathbb{Z})$. Since Λ acts freely by translation on the simply connected space $\mathbb{C}^g$, the fundamental group $\pi_1(\mathbb{C}^g/\Lambda)$ equals Λ, and hence $\pi_1(A(\mathbb{C})) \simeq \Lambda$. Taking abelianizations gives $H_1(A(\mathbb{C}), \mathbb{Z}) \simeq \Lambda$ as claimed.

The inclusion of $H_1(A(\mathbb{C}),\mathbb{Z}) \simeq \Lambda$ as a discrete subgroup of $H^0(A,\Omega^1)^\vee \simeq \mathbb{C}^g$ is given by integration:

$$\begin{aligned} H_1(A(\mathbb{C}),\mathbb{Z}) &\to H^0(A,\Omega^1)^\vee \\ [\gamma] &\mapsto \left(\omega \mapsto \int_\gamma \omega\right), \end{aligned}$$

where $[\gamma]$ is the class of a closed path γ in $A(\mathbb{C})$.

Remark 4.3.3. A meromorphic function on $\mathbb{C}^g/\Lambda$ is the same thing as a meromorphic function f on $\mathbb{C}^g$ that is periodic in the sense that $f(\vec{z}+\vec{w}) = f(\vec{z})$ for every $\vec{w} \in \Lambda$. For this reason, Λ is called the period lattice. As we saw, elements of Λ arise by integrating translation-invariant 1-forms along closed paths in $A(\mathbb{C})$. By abuse of terminology, the integral of any meromorphic 1-form along a closed path in a complex projective variety may be called a period.

☡ Warning 4.3.4. A complex torus is a complex Lie group of the form $\mathbb{C}^g/\Lambda$, where Λ is a discrete $\mathbb{Z}$-submodule of $\mathbb{C}^g$ of rank $2g$. Theorem 4.3.1 shows that every abelian variety A over $\mathbb{C}$ gives rise to a complex torus. One can ask: Does every complex torus arise as $A(\mathbb{C})$ for some abelian variety A over $\mathbb{C}$? The answer is yes for $g = 1$, but no in general for $g \geq 2$; there is a condition on Λ that is equivalent to the existence of A.

The GAGA principle [Ser55] (see also [Har77, Appendix B]) shows that for any nice $\mathbb{C}$-variety X, the map

$$\mathbf{k}(X) \to \{\text{meromorphic functions on the complex manifold } X(\mathbb{C})\}$$

is an isomorphism. We know $\operatorname{trdeg}(\mathbf{k}(X)/\mathbb{C}) = \dim X$. But it turns out that the field of meromorphic functions on certain complex tori $\mathbb{C}^g/\Lambda$ can have transcendence degree $< g$; such tori cannot come from abelian varieties. ♣♣♣ Bjorn: [cite Shafarevich?]

4.4. Abelian varieties over finite extensions of $\mathbb{Q}_p$

Let k be a finite extension of $\mathbb{Q}_p$. Let A be an abelian variety over k. Then $A(k)$ can be viewed as a p-adic Lie group.

☡ Warning 4.4.1. There is no everywhere-defined map $\exp\colon \operatorname{Lie} A \to A(k)$ as in the proof of Theorem 4.3.1(i). This is not surprising, if one remembers that the usual exponential series $\exp(x) := \sum_{n\geq 0} x^n/n!$ has a finite radius of convergence when considered over $\mathbb{Q}_p$ or k, because of the powers of p in the denominators.

We therefore try to construct the inverse map by integrating translation-invariant 1-forms as in Theorem 4.3.1(ii).

We will define integration on $A(k)$, as in classical differential geometry, by working in a manifold chart. Since A is smooth, there exist rational functions $t_1, \ldots, t_g$ giving a diffeomorphism

$$\vec{t} := (t_1, \ldots, t_g) \colon U \to V$$

(not a homomorphism) between a p-adic open neighborhood U of $O \in A(k)$ and a p-adic open neighborhood V of $0 \in k^g$.

Fix $\omega \in H^0(A, \Omega^1)$. The restriction of ω to U corresponds to $\sum_{j=1}^{g} w_j \, dt_j$ for some $w_j \in k[[t_1, \ldots, t_g]]$, Integrating formally term by term gives a power series $\lambda \in k[[t_1, \ldots, t_g]]$, and one can show that it converges on some neighborhood of 0 in V. By shrinking U and V, we may assume it converges on V. Then for $P \in U$, we may define $\int_O^P \omega := \lambda(\vec{t}(P))$.

If we repeat the previous paragraph for a basis of $H^0(A, \Omega^1)$, and shrink U so that it works for all ω, we get a map

$$\begin{aligned} \log \colon U &\to H^0(A, \Omega^1)^\vee \simeq \operatorname{Lie} A \\ P &\mapsto (\omega \mapsto \int_O^P \omega) \end{aligned}$$

whose derivative at O is the identity $\operatorname{Lie} A \to \operatorname{Lie} A$. With a little more work, one can shrink U to make it an open subgroup of $A(k)$, and then prove using the translation-invariance of the 1-forms that $\log \colon U \to \operatorname{Lie} A$ is a homomorphism.

We have that U has finite index in $A(k)$, since $A(k)$ is compact. On the other hand, $\operatorname{Lie} A$ is uniquely divisible (for any $n \geq 1$, multiplication-by-n on it is an isomorphism). Using these two facts one can show that there a unique extension of log to a homomorphism defined on all of $A(k)$. To summarize:

THEOREM 4.4.2. *Let k be a finite extension of $\mathbb{Q}_p$. Let A be an abelian variety over k. There exists a canonical map*

$$\log \colon A(k) \to \operatorname{Lie} A$$

that is both a homomorphism and a local diffeomorphism.

♣♣♣ Bjorn: [mention p-adic uniformization]

4.5. Cohomology of the Kummer sequence for an abelian variety

Let k be a perfect field, and let $G = \operatorname{Gal}(\overline{k}/k)$. Let n be an integer with $\operatorname{char} k \nmid n$. There is an exact sequence of G-modules

$$0 \to \mu_n \to \overline{k}^\times \xrightarrow{n} \overline{k}^\times \to 0.$$

where $\mu_n := \{x \in \overline{k}^\times : x^n = 1\}$. Part of the associated long exact sequence of Galois cohomology is

$$\begin{tikzcd}
\cdots \arrow[r] & k^\times \arrow[r, "n"] & k^\times \arrow[dll, rounded corners] \\
H^1(k,\mu_n) \arrow[r] & H^1(k,\overline{k}^\times) \arrow[r] & \cdots .
\end{tikzcd}$$

Hilbert's Theorem 90 (as generalized by E. Noether) states that $H^1(k,\overline{k}^\times) = 0$, so we get an isomorphism

$$\frac{k^\times}{k^{\times n}} \xrightarrow{\sim} H^1(k,\mu_n).$$

If moreover k contains the n-th roots of 1, then $H^1(k,\mu_n) \simeq \operatorname{Hom}_{\text{conts}}(\operatorname{Gal}(\overline{k}/k),\mu_n)$, and this gives a quick proof of Kummer theory, which classifies the abelian extensions K/k with $\operatorname{Gal}(K/k)$ killed by n.

Remark 4.5.1. Let L be a finite-dimensional associative k-algebra with 1 (not necessarily commutative). Then G acts on $\overline{L} := L \underset{k}{\otimes} \overline{k}$ through its action on the second factor. A generalization of Hilbert's Theorem 90 states that the pointed set $H^1(G,\overline{L}^\times)$ is trivial. In the case where L is commutative, this leads to an isomorphism

$$\frac{L^\times}{L^{\times n}} \to H^1(G,\mu_n(\overline{L})),$$

where $\mu_n(\overline{L}) := \{x \in \overline{L}^\times : x^n = 1\}$.

There is also an analogue in which the multiplicative group variety $\mathbb{G}_m$ (with $\mathbb{G}_m(\overline{k}) = \overline{k}^\times$) is replaced by an abelian variety A over k. The Kummer sequence associated to A is the exact sequence of G-modules

$$0 \to A[n] \to A(\overline{k}) \xrightarrow{n} A(\overline{k}) \to 0.$$

Part of the associated long exact sequence of Galois cohomology is

$$\begin{tikzcd}
\cdots \arrow[r] & A(k) \arrow[r, "n"] & A(k) \arrow[dll, rounded corners, "\delta"] \\
H^1(k, A[n]) \arrow[r] & H^1(k, A) \arrow[r, "n"] & H^1(k, A) \arrow[dll, rounded corners] \\
\cdots . & &
\end{tikzcd}$$

In contrast with Hilbert's Theorem 90, the group $H^1(k, A)$ can be very complicated, but in any case, we can extract the short exact sequence

$$0 \to \frac{A(k)}{nA(k)} \xrightarrow{\delta} H^1(k, A[n]) \to H^1(k, A)[n] \to 0. \tag{4.5.2}$$

This is sometimes called the descent sequence.

4.6. Abelian varieties over number fields

4.6.1. The Mordell-Weil theorem. The following was proved by Weil, who generalized Mordell's proof for elliptic curves over $\mathbb{Q}$:

THEOREM 4.6.1 (Mordell-Weil theorem). *Let k be a number field, and let A be an abelian variety over k. Then the abelian group $A(k)$ is finitely generated.*

There is essentially only one known proof of this theorem. After fixing an integer $n \geq 2$, it consists of two steps:

(1) Prove that $\frac{A(k)}{nA(k)}$ is finite. (This is called the weak Mordell-Weil theorem, since it is a consequence of the Mordell-Weil theorem, but does not by itself imply the Mordell-Weil theorem. Its proof is explained in Sections 4.6.2 and 4.6.3.)

(2) Find a function $|\ |\colon A(k) \to \mathbb{R}$ satisfying
   (a) For each $B \in \mathbb{R}$, the set $\{ P \in A(k) : |P| < B \}$ is finite.
   (b) $|P + Q| \leq |P| + |Q| + O(1)$ and $|nP| = n|P| + O(1)$ for all $P, Q \in A(k)$, where the implied constants depend on k and A, but not on P and Q.

   It turns out that one can use $|P| := \sqrt{h(P)}$ where h is a (logarithmic) height function.

Theorem 4.6.1 follows almost formally from these two steps: see Exercise 18.

REMARK 4.6.2. The Mordell-Weil theorem holds over global function fields as well, and even over finitely generated fields (i.e., fields that are finitely generated as a field over $\mathbb{Q}$ or some $\mathbb{F}_p$). This follows from the Lang-Néron theorem. ♣♣♣ Bjorn: [add reference]

4.6.2. Definition of the Selmer group. We continue to let A be an abelian variety over a number field k, and let $n \geq 2$ be an integer. The weak Mordell-Weil theorem is proved by bounding the image of the descent map $\frac{A(k)}{nA(k)} \xrightarrow{\delta} H^1(k, A[n])$ in Section 4.5 by a finite subgroup $\operatorname{Sel} = \operatorname{Sel}(k, A[n])$ of $H^1(k, A[n])$. The purpose of this section is to define Sel.

The descent map δ in (4.5.2) is compatible with extension of k, so we have a commutative square

(4.6.3)
$$\begin{tikzcd}
\frac{A(k)}{nA(k)} \arrow[r, hook, "\delta"] \arrow[d] & H^1(k, A[n]) \arrow[d, "\prod \operatorname{res}_v"] \\
\prod_v \frac{A(k_v)}{nA(k_v)} \arrow[r, hook, "\prod \delta_v"] & \prod_v H^1(k_v, A[n])
\end{tikzcd}$$

in which each product is over all the places v of k, including the archimedean places.

Definition 4.6.4. The n-Selmer group $\operatorname{Sel} = \operatorname{Sel}(k, A[n])$ is the subgroup of $H^1(k, A[n])$ consisting of ξ such that $\prod \operatorname{res}_v(\xi)$ is in the image of $\prod \delta_v$.

In other words,

$$\operatorname{Sel} := \bigcap_v \operatorname{res}_v^{-1} \delta_v \left(\frac{A(k_v)}{nA(k_v)} \right) \quad \subseteq H^1(k, A[n]),$$

so an element of $H^1(k, A[n])$ belongs to Sel if and only if it satisfies infinitely many Selmer conditions, one for each v.

The point of Definition 4.6.4 is that (4.6.3) shows that δ maps $\frac{A(k)}{nA(k)}$ into Sel.

4.6.3. Finiteness of the Selmer group.

Definition 4.6.5. Let M be a G-module, where $G = \operatorname{Gal}(\overline{k}/k)$. Let v be a place of k, and let k_v^{unr} be the maximal unramified extension of k_v, so the absolute Galois group of k_v^{unr} is an inertia subgroup of G. An element of $H^1(k, M)$ or $H^1(k_v, M)$ is called unramified at v if its image in $H^1(k_v^{\mathrm{unr}}, M)$ is zero. Let $H^1_{\mathrm{unr}}(k_v, M)$ be the set of elements of $H^1(k_v, M)$ that are unramified at v. If S is a set of places of k, let $H^1_S(k, M)$ be the subgroup of $H^1(k, M)$ consisting of elements that are unramified at every $v \notin S$.

Lemma 4.6.6. *Suppose v is a nonarchimedean place of good reduction for A, and v lies above a rational prime not dividing n. Then*

$$\delta_v \left(\frac{A(k_v)}{nA(k_v)} \right) = H^1_{\mathrm{unr}}(k_v, M).$$

Thus at all but finitely many v, the Selmer condition at v is the same as the condition of being unramified at v.

Proof. ♣♣♣ Bjorn: [To be added.] □

Corollary 4.6.7. *Let S be a finite set of places of k containing the archimedean places, the places lying above rational primes dividing n, and the places of bad reduction for A. Then* $\mathrm{Sel} \subseteq H^1_S(k, A[n])$.

More precisely, Sel is the subgroup of $H^1_S(k, A[n])$ consisting of elements that satisfy the remaining Selmer conditions, namely those for $v \in S$.

Lemma 4.6.8. *The group $H^1_S(k, A[n])$ is finite.*

Proof. ♣♣♣ Bjorn: [To be added.] □

Summarizing, we have

$$\frac{A(k)}{nA(k)} \hookrightarrow \mathrm{Sel} \subseteq H^1_S(k, A[n]) \subseteq H^1(k, A[n]),$$

so the finiteness of $H^1_S(k, A[n])$ implies the finiteness of $\frac{A(k)}{nA(k)}$.

4.6.4. Algorithmic issues. An important problem is to determine, given a number field k and an abelian variety A, generators for the group $A(k)$. But it is not known whether there is an algorithm that solves this problem in general, even for the case of elliptic curves over $\mathbb{Q}$. In fact, the following problems are equivalent in the sense that there is an algorithm that can solve them all in principle given a solution to any one of them (for a particular A over k):

(1) Compute generators of $A(k)$.
(2) Compute the rank of $A(k)$.
(3) Compute $\#\frac{A(k)}{2A(k)}$.
(4) Given an torsor X under A, decide whether $X(k) = \emptyset$.
(5) Given an torsor X under A such that the class of X in $H^1(k, A)$ has order 2, decide whether $X(k) = \emptyset$.

For instance, $\#\frac{A(k)}{2A(k)}$ is related to the rank of $A(k)$ by the following easy lemma:

Lemma 4.6.9. *If A is an abelian variety over a number field k, and $A(k)$ has rank r, then*

$$\dim_{\mathbb{F}_2} \frac{A(k)}{2A(k)} = r + \dim_{\mathbb{F}_2} A[2](k).$$

Proof. Write $A(k) \simeq \mathbb{Z}^r \oplus T$, where T is a finite abelian group. Then

$$\frac{A(k)}{2A(k)} \simeq \left(\frac{\mathbb{Z}}{2\mathbb{Z}}\right)^r \oplus \frac{T}{2T},$$

and $T/2T$ has the same order as $T[2] = A[2](k)$, as one sees by writing T as a product of finite cyclic groups. □

Remark 4.6.10. Replacing the integer 2 in the above problems by any other integer ≥ 2 gives an equivalent problem.

Remark 4.6.11. If the Shafarevich-Tate group $Ш(A)$ is finite, as is conjectured, then all the problems above can be solved.

Exercises

4.1. Let A be an abelian variety over a field k, and let $\ell \neq \operatorname{char} k$ be a prime. Prove that $T_\ell A \simeq \operatorname{Hom}_{\text{groups}}(\mathbb{Q}_\ell/\mathbb{Z}_\ell, A(\overline{k}))$ as $\mathbb{Z}_\ell$-modules.

4.2. Prove that Theorem 4.1.21 implies Corollary 4.1.22.

4.3. Prove Theorem 4.2.3. (Hint: By changing $P(x)$ to $P(\lambda x)$ for suitable $\lambda \in K^\times$, reduce to the case $s = 0$. Start with $P(x)$ in factored form, and in terms of the number of zeros of positive and negative valuation, determine the location of the slope-zero part of the Newton polygon.)

4.4. Let $P(x)$ be a polynomial over a valued field K, and let $n \in \mathbb{Z}_{>0}$. How does the Newton polygon of $P(x)^n$ relate to the Newton polygon of $P(x)$?

4.5. How does the Newton polygon of a product of polynomials relate to the Newton polygons of the factors?

4.6. Let A be a g-dimensional abelian variety over $\mathbb{F}_q$. Prove that

$$(\sqrt{q}-1)^{2g} \leq \#A(\mathbb{F}_q) \leq (\sqrt{q}+1)^{2g}.$$

4.7. Fix $\mathbb{F}_q$. For which $a \in \mathbb{Z}$ does there exist an elliptic curve E over $\mathbb{F}_q$ such that $P_E(x) = x^2 - ax + q$? Describe a criterion that is as simple as possible, and use Theorem 4.2.12 to prove its correctness.

4.8. Prove the equivalence of (i)-(iv) in Theorem 4.2.17.

4.9. (a) Let A be an abelian variety over $\mathbb{F}_q$. Prove that the corners of the Newton polygon of A have integer coordinates.

(b) Give an example of a q and a polynomial $h(x) \in \mathbb{Z}[x]$ satisfying

(i) $h(x)$ is monic and irreducible over $\mathbb{Q}$,

(ii) $h(0) > 0$,

(iii) the zeros of h are q-Weil numbers, and

(iv) the corners of the q-Newton polygon of h all have integer coordinates, but

(v) there is no abelian variety A over $\mathbb{F}_q$ with $P_A(x) = h(x)$.

4.10. Let A be an ordinary simple abelian variety over $\mathbb{F}_q$, and write $P_A(x)$ as $h(x)^e$ where $h(x) \in \mathbb{Z}[x]$ is irreducible.

(a) Prove that $h(x)$ has no real zeros.

(b) Prove that $e = 1$.

4.11. Prove Theorem 4.2.20.

4.12. Explain the claims made in Warning 4.2.22.

4.13. Let A be an abelian variety of dimension g over $\mathbb{F}_q$. Suppose that the p-rank of A is 0. For which values of g does it follow necessarily that A is supersingular?

4.14. Let A be an abelian variety over $\mathbb{C}$, and let $\Lambda = H_1(A(\mathbb{C}), \mathbb{Z})$ be the associated lattice. Let ℓ be any prime. Prove that there is a natural isomorphism of $\mathbb{Z}_\ell$-modules $T_\ell A \simeq \Lambda \otimes \mathbb{Z}_\ell$. ("Natural" means that it should be functorial with respect to abelian variety homomorphisms $A \to B$.)

4.15. To an abelian variety A over $\mathbb{C}$, we can associate the lattice $H_1(A(\mathbb{C}), \mathbb{Z})$, which is a free $\mathbb{Z}$-module of rank $2 \dim A$. To an abelian variety A over any field k, we can similarly associate the Tate module $T_\ell A$, a $\mathbb{Z}_\ell$-module of rank $2 \dim A$ for any $\ell \neq \operatorname{char} k$. In contrast:

(a) Prove that there is no additive functor F from the category of abelian varieties over $\overline{\mathbb{F}}_p$ to the category of $\mathbb{Z}$-modules such that $F(A)$ is free of rank $2 \dim A$ for every abelian variety A.

(b) Prove the stronger statement that the nonexistence still holds if the category of $\mathbb{Z}$-modules is replaced by the category of vector spaces over $\mathbb{Q}$ or $\mathbb{Q}_p$.

(Hint for both parts: consider the endomorphism ring of a supersingular elliptic curve.)

4.16. Let k be a finite extension of $\mathbb{Q}_p$. Let A be an abelian variety over k. Let $\log\colon A(k) \to \operatorname{Lie} A$ be the homomorphism in Theorem 4.4.2.

(a) Prove that $\ker(\log)$ is finite.

(b) Prove that $\ker(\log)$ equals the torsion subgroup of $A(k)$.

(c) Prove that $\log$ is never surjective (unless $\dim A = 0$).

4.17. Prove that the homomorphism log in Theorem 4.4.2 behaves functorially both with respect to extension of k and with respect to homomorphisms of abelian varieties $A \to B$.

4.18. Deduce Theorem 4.6.1 from the weak Mordell-Weil theorem and the existence of the function $|\ |$.

CHAPTER 5

Jacobian varieties

5.1. The Picard functor and the definition of the Jacobian

THEOREM 5.1.1. *Let X be a nice k-curve. Suppose that X has a k-point, or at least a divisor of degree* 1*. Then there is a k-variety $J = \operatorname{Jac} X$ called the Jacobian of X such that $J(k)$ is naturally in bijection with $\operatorname{Pic}^0 X$. More precisely, for every field extension $L \supseteq k$, one should have a bijection $J(L) \to \operatorname{Pic}^0 X_L$ and these should be compatible with base extension: i.e., if $\sigma\colon L \to L'$ is a k-algebra homomorphism between field extensions of k, then the diagram*

$$\begin{tikzcd}
J(L) \arrow[r] \arrow[d] & \operatorname{Pic}^0 X_L \arrow[d] \\
J(L') \arrow[r] & \operatorname{Pic}^0 X_{L'}
\end{tikzcd}$$

should commute, where the left vertical map is applying σ coordinatewise to each point, and the right vertical map is induced by $\operatorname{Div} X_L \to \operatorname{Div} X_{L'}$.

REMARK 5.1.2. It would be better to allow L to be any k-algebra, or even any k-scheme. The disadvantage of this is that the group $\operatorname{Pic}^0 X_L$ must then be replaced by a more complicated generalization. But one advantage of having a functor from the category of k-schemes to the category of sets (or abelian groups) is that the representing object J is unique once one knows that it exists, by Yoneda's Lemma. Also, one can deduce more properties of J from knowing $J(S)$ for k-schemes S than by knowing only $J(L)$ for fields $L \supseteq k$: for instance, $J(k[\epsilon]/(\epsilon^2))$ gives information about $\operatorname{Lie} J$ (in particular, its dimension).

Theorem 5.1.1 is not so easy to prove: a proof can be found in [Mil86].

REMARK 5.1.3. Let X be any nice k-curve. Let $G = \operatorname{Gal}(\overline{k}/k)$ and $\overline{X} = X_{\overline{k}}$. Suppose the functor from the category of field extensions of k to the category of sets defined by $L \mapsto \operatorname{Pic}^0 X_L$ is representable by a k-scheme J. Then the bijectivity of $J(k) \to J(\overline{k})^G$ (which follows from Galois theory applied to coordinates) implies the bijectivity of $\operatorname{Pic}^0 X \to (\operatorname{Pic}^0 \overline{X})^G$.

Warning 5.1.4. Theorem 5.1.1 does not hold for every nice k-curve X. Let X be the smooth projective model of $y^2 = -x^4 - 1$ over $\mathbb{R}$. By Exercise 2, $\operatorname{Pic}^0 X \to (\operatorname{Pic}^0 \overline{X})^G$ is not a bijection. By Remark 5.1.3, the functor $L \mapsto \operatorname{Pic}^0 X_L$ is not representable by a k-scheme. (It follows also that X has no divisor of degree 1.)

Nevertheless, we have the following:

Remark 5.1.5. For an arbitrary nice k-curve X (with or without a divisor of degree 1), one can define the Jacobian J as a k-variety representing a slightly different functor: $J(L) = (\operatorname{Pic}^0 X_{\overline{L}})^{\operatorname{Gal}(\overline{L}/L)}$ for (perfect) field extensions $L \supseteq k$.

Remark 5.1.6. The functor taking L to the set of degree-d elements in $(\operatorname{Pic} X_{\overline{L}})^{\operatorname{Gal}(\overline{L}/L)}$ (instead of degree-0) is again represented by a k-variety, sometimes denoted $\mathbf{Pic}^d_{X/k}$. It is a torsor under the Jacobian $J = \mathbf{Pic}^0_{X/k}$.

If instead one uses $L \mapsto (\operatorname{Pic} X_{\overline{L}})^{\operatorname{Gal}(\overline{L}/L)}$ without restricting the degree, then the representing object is not a k-variety, but a non-noetherian k-scheme $\mathbf{Pic}_{X/k} = \coprod_{d \in \mathbb{Z}} \mathbf{Pic}^d_{X/k}$.

Remark 5.1.7. The relative Picard functor for a scheme X over an arbitrary base S is defined as the fppf sheaf associated to the functor $T \mapsto \operatorname{Pic}(X \underset{S}{\times} T)$. The fppf-sheafification process involved (which in fact is a two-stage process, involving also a sheafification with respect to the Zariski topology) can be viewed as the appropriate generalization to arbitrary base schemes (as opposed to field extensions of a perfect field k) of the operation of taking Galois invariants. See [BLR90, §8.1].

5.2. Basic properties of the Jacobian

Here we list some facts about Jacobians. Not all proofs will be given. For $D \in \operatorname{Div} X$, we write $[D]$ for its class in $\operatorname{Pic} X$.

(1) J is an abelian variety, and the bijection $J(L) \to (\operatorname{Pic} X_{\overline{L}})^{\operatorname{Gal}(\overline{L}/L)}$ is a group homomorphism. In fact, once one knows that J is a k-variety representing a functor from the category of k-schemes to the category of groups, Yoneda's lemma automatically makes J into a group variety.

(2) $\dim J = g$, where g is the genus of X.

(3) If X has a k-point P (or more generally a divisor P of degree 1), each point in $J(k)$ can be written as $[D - gP]$ for some effective $D \in \operatorname{Div} X$ of degree g: cf. Exercise 4. Effective divisors of degree g are parametrized by the g-th symmetric

power $\operatorname{Sym}^g X$ (the quotient of X^g by the action of the symmetric group S_g), and the previous sentence can be interpreted as giving a morphism $\operatorname{Sym}^g X \to J$. In fact, it turns out to be a birational morphism between nice k-varieties; in other words, $\operatorname{Sym}^g X$ can be obtained by blowing up J along some subscheme. This is a key point in Weil's construction of the Jacobian.

(4) Suppose $\pi\colon X \to Y$ is a dominant morphism between nice k-curves. The group homomorphisms

$$\begin{tikzcd}\operatorname{Pic}^0 X \arrow[r, shift left, "\pi_*"] & \operatorname{Pic}^0 Y \arrow[l, shift left, "\pi^*"]\end{tikzcd}$$

correspond to homomorphisms of abelian varieties between the Jacobians

$$\begin{tikzcd}J_X \arrow[r, shift left, "\pi_*"] & J_Y . \arrow[l, shift left, "\pi^*"]\end{tikzcd}$$

5.3. The Jacobian as Albanese variety

Theorem 5.3.1. *Let X be a nice k-curve. Let $J = \operatorname{Jac} X$. Suppose that P is a k-point of X. Then:*

(i) *The map*

$$\begin{aligned}\iota\colon X &\to J\\ Q &\mapsto [Q - P]\end{aligned}$$

(for any $Q \in X(L)$, for any field extension $L \supseteq k$ or even any k-scheme L) is a morphism of varieties.

(ii) *Any morphism $f\colon X \to B$ from X to an abelian variety B satisfying $f(P) = O$ (the identity of B) factors uniquely through J: i.e., there is a unique homomorphism of abelian varieties $h\colon J \to B$ such that the diagram*

$$\begin{tikzcd}X \arrow[rr, "f"] \arrow[dr, "\iota"'] & & B \\ & J \arrow[ur, dotted, "h"'] & \end{tikzcd}$$

commutes.

Definition 5.3.2. Any morphism ι associated to some $P \in X(k)$ as in Theorem 5.3.1 or more generally associated to some degree-1 divisor P on X (or even to an element $P \in (\operatorname{Pic}^1 \overline{X})^G$) is called an Albanese morphism.

Remark 5.3.3. More generally, given a nice k-variety X of arbitrary dimension and a point $P \in X(k)$, the Albanese variety of (X, P) is an abelian variety A that is universal for morphisms from X to abelian varieties sending P to O. Thus A comes equipped with a morphism $\iota \colon X \to A$ (called an Albanese morphism) such that any morphism $X \to B$ from X to an abelian variety B mapping P to $O \in B(k)$ factors uniquely through A. It turns out that such an pair (A, ι) always exists, and the universal property guarantees that it is unique up to isomorphism. ♣♣♣ Bjorn: [Generalize to non-nice varieties using rational maps?]

One can show that for a nice curve X of genus $g \geq 1$ any Albanese morphism $X \to J$ is an embedding. If $g = 1$, then $\dim X = 1 = \dim J$, so this embedding must be an isomorphism. (Remember that this is still under the assumption that X has a k-point, or at least a divisor of degree 1, in order that we have the Albanese morphism.)

Remark 5.3.4. More canonically, for any nice k-curve X, one has a natural morphism $X \to \mathbf{Pic}^1_{X/k}$ sending each $Q \in X(L)$ to $[Q]$. The choice of $P \in X(k)$ lets us identify $\mathbf{Pic}^1_{X/k}$ with J.

Here are some other facts that we mention without proof:

Theorem 5.3.5. *Let X be a nice curve of genus g, and let $\iota \colon X \to J$ be an Albanese morphism. Then*

(i) *The induced map $\iota^* \colon H^0(J, \Omega^1) \to H^0(X, \Omega^1)$ is an isomorphism of k-vector spaces (of dimension g).*

(ii) *The induced map $\iota^* \colon H^1_{\text{et}}(\overline{J}, \mathbb{Q}_\ell) \to H^1_{\text{et}}(\overline{X}, \mathbb{Q}_\ell)$ is a $\operatorname{Gal}(\overline{k}/k)$-equivariant isomorphism of $\mathbb{Q}_\ell$-vector spaces (of dimension $2g$).*

Remark 5.3.6. It is easy to show that the Albanese variety of (X, P) is independent of the choice of $P \in X(k)$: see Exercise 4. In fact, there is a different notion of Albanese variety $A = \operatorname{Alb} X$ for a variety X that makes sense even when $X(k)$ is empty: instead of having a morphism $\iota \colon X \to A$, however, one has a morphism $X \times X \to A$. In the case where one has an ι coming from some $P \in X(k)$, the morphism $X \times X \to A$ equals (ι, ι) followed by subtraction.

5.4. Jacobians over finite fields

Let X be a nice curve over a finite field $\mathbb{F}_q$. By Exercise 5, X automatically has a divisor of degree 1, so its Jacobian J satisfies $J(L) \simeq \operatorname{Pic}^0 X_L$ for any field extension $L \supseteq \mathbb{F}_q$.

Suppose

$$P_1(T) = \prod_{i=1}^{2g}(1 - \lambda_i T) = 1 + a_1 T + \cdots + q^g T^{2g}$$

is the numerator of the zeta function $Z_X(T)$, so $\#X(\mathbb{F}_{q^n}) = q^n + 1 - \sum_{i=1}^{2g} \lambda_i^n$ for all $n \geq 1$. Theorem 5.3.5(ii) implies that the $P_1(T)$ for X equals the $P_1(T)$ for J. Remark 4.2.5 implies that this common $P_1(T)$ equals the *reverse* of the characteristic polynomial $P_J(x)$. Thus

$$P_J(x) = \prod_{i=1}^{2g}(x - \lambda_i) = x^{2g} + a_1 x^{2g-1} + \cdots + q^g.$$

In particular, Section 3.7 can be used to compute $P_J(x)$. Also, by Remark 4.2.6,

$$\#J(\mathbb{F}_q) = P_J(1) = P_1(1) = \prod_{i=1}^{2g}(1 - \lambda_i). \tag{5.4.1}$$

5.5. Jacobians over $\mathbb{C}$

Let X be a nice $\mathbb{C}$-curve of genus g. Since $\mathbb{C}$ is algebraically closed, we may pick $P \in X(\mathbb{C})$. Let $\omega_1, \ldots, \omega_g$ be a basis for $H^0(X, \Omega^1)$. For each closed 1-cycle γ in $X(\mathbb{C})$ we get a "period"

$$\int_\gamma (\omega_1, \ldots, \omega_g) \in \mathbb{C}^g.$$

This induces the period map

$$H_1(X(\mathbb{C}), \mathbb{Z}) \to \mathbb{C}^g,$$

whose image is called the period lattice Λ. Fix $P \in X(\mathbb{C})$. The map

$$\begin{aligned} X(\mathbb{C}) &\to \mathbb{C}^g/\Lambda \\ Q &\mapsto \int_P^Q (\omega_1, \ldots, \omega_g) \end{aligned}$$

is well-defined, since changing the path from P to Q in $X(\mathbb{C})$ changes the integral on the right by an element of Λ.

THEOREM 5.5.1 (Abel-Jacobi theorem). *The map $X(\mathbb{C}) \to \mathbb{C}^g/\Lambda$ is the Albanese map $\iota\colon X \to J$ associated to P, if we identify $\mathbb{C}^g/\Lambda$ with $J(\mathbb{C})$ as in Theorem 4.3.1 using the basis of $H^0(J, \Omega^1)$ mapped by the isomorphism ι^* to the basis $\omega_1, \ldots, \omega_g$ of $H^0(X, \Omega^1)$*

The proof is an exercise, given our work in Section 4.3: see Exercise 11.

Exercises

5.1. Prove Theorem 5.1.1 in the case of a genus-0 curve.

5.2. Let X be the smooth projective model of $y^2 = -x^4 - 1$ over $\mathbb{R}$, and let $G = \operatorname{Gal}(\mathbb{C}/\mathbb{R})$. Prove that $\operatorname{Pic}^0 X \to (\operatorname{Pic}^0 \overline{X})^G$ is not a bijection.

5.3. Let $\pi\colon X \to Y$ be a dominant morphism of degree d between nice k-curves.

(a) Prove that the composition

$$\begin{tikzcd} J_Y \arrow[r, "\pi^*"] & J_X \arrow[r, "\pi_*"] & J_Y \end{tikzcd}$$

equals the multiplication-by-d map on J_Y.

(b) Prove that J_X is isogenous to $J_Y \times A$ for some abelian variety A.

5.4. Let X be a nice k-variety. Let $P, P' \in X(k)$. Let (A, ι) be the Albanese variety of (X, P) and let (A', ι') be the Albanese variety of (X, P'). Prove that $A \simeq A'$.

5.5. (a) Let k be an algebraically closed field. Let $X \to J$ be an Albanese morphism. Prove that the image of $X(k) \to J(k)$ generates $J(k)$ as an abelian group.

(b) Was the hypothesis that k be algebraically closed necessary?

5.6. Let X be a nice k-curve of genus $g \geq 1$. Let $\iota\colon X \to J$ be an Albanese morphism associated to some $P \in X(k)$. Without assuming that ι is an embedding, prove that ι gives an injection $X(k) \to J(k)$.

5.7. Let k be a field of characteristic not 2.

(a) Let X be the smooth projective model of the curve $y^2 = h(x^2)$ where $\deg h = 3$; assume that X has genus 2. In this case, prove also X has an involution (automorphism of order 2) not equal to the hyperelliptic involution.

(b) Do the same for $y^2 = f(x)$ where f is a polynomial of degree ≤ 6 such that $f = f^{\text{rev}}$ (where one considers f to be of degree 6 in the computation of f^{rev}).

5.8. Let X be any nice genus-2 curve having an involution α not equal to the hyperelliptic involution ι.

(a) Prove that the involutions α and ι commute. (Hint: ι is defined in terms of the canonical map.)

(b) Let $Y := X/\langle\alpha\rangle$ be the nice k-curve whose function field is the subfield of $\mathbf{k}(X)$ fixed pointwise by the automorphism induced by α. Define $Y' := X/\langle\alpha\iota\rangle$ similarly. The Galois theory correspondence between subgroups of $\langle\alpha, \iota\rangle$ and subfields of $\mathbf{k}(X)$

gives a diagram

$$\begin{tikzcd}
 & X \arrow[dl] \arrow[d] \arrow[dr] & \\
Y \arrow[dr] & Y' \arrow[d] & \mathbb{P}^1 \arrow[dl] \\
 & \mathbb{P}^1 &
\end{tikzcd}$$

of nice curves. Prove that Y and Y' are of genus 1.

(c) How many points ramify in each of the morphisms $Y \to \mathbb{P}^1$, $Y' \to \mathbb{P}^1$, and $\mathbb{P}^1 \to \mathbb{P}^1$ in the diagram? Prove that there is exactly one point of the bottom $\mathbb{P}^1$ that ramifies in both $Y \to \mathbb{P}^1$ and $\mathbb{P}^1 \to \mathbb{P}^1$, and prove that that point is a k-point.

(d) Prove that the curve Y is birational to $y^2 = h(x)$ for some polynomial h of degree 3.

(e) Prove that the curve X is birational to $y^2 = h(x^2)$.

(f) Prove that the curve Y' is birational to $y^2 = h^{\text{rev}}(x)$, where h^{rev} is computed as a polynomial of degree 3. In particular, Y and Y' may be viewed as elliptic curves.

(g) Let J be the Jacobian of X. The morphism $X \to Y$ gives (by Albanese functoriality) a homomorphism of abelian varieties $J \to Y$, and $X \to Y'$ gives $J \to Y'$. Prove that the product homomorphism $J \to Y \times Y'$ is an isogeny. (Hint: what do regular differentials on Y and Y' pull back to on X?)

5.9. (a) Prove that for fixed g, there is a polynomial in $\mathbb{Q}[x_1, \ldots, x_g]$ whose value at

$$(\#X(\mathbb{F}_q), \#X(\mathbb{F}_{q^2}), \ldots, \#X(\mathbb{F}_{q^g})) \quad \in \mathbb{Z}^g$$

for any nice genus-g curve X over $\mathbb{F}_q$ equals $\#J(\mathbb{F}_q)$, where $J := \operatorname{Jac} X$.

(b) Find this polynomial explicitly for $g = 2$.

5.10. Let X be the curve in Exercise 10, and let g be its genus. Let $J := \operatorname{Jac} X$.

(a) Prove that J is supersingular.

(b) Show that the q^2-power Frobenius endomorphism on J equals multiplication by $-q$ on J.

(c) Prove that $J(\mathbb{F}_{q^2}) \simeq \left(\frac{\mathbb{Z}}{(q+1)\mathbb{Z}}\right)^{2g}$ as abelian groups.

5.11. Using Theorem 5.3.5(i) and results from Section 4.3, prove the Abel-Jacobi theorem (Theorem 5.5.1).

CHAPTER 6

2-descent on hyperelliptic Jacobians

We use the following notation throughout this chapter:

k: a perfect field of characteristic $\neq 2$

$\overline{k}$: an algebraic closure of k

$G := \operatorname{Gal}(\overline{k}/k)$

g: an integer ≥ 1

f: a squarefree polynomial in $k[x]$ of degree $2g+1$

X: the smooth projective model of the affine curve $y^2 = f(x)$

π: the x-coordinate map $X \to \mathbb{P}^1$

∞: the unique point on X above ∞ on $\mathbb{P}^1$; it is a k-point

$J := \operatorname{Jac} X$.

As mentioned in Section 2.8.1, the genus of X equals g. Thus $\dim J = g$.

6.1. 2-torsion of hyperelliptic Jacobians

We eventually want to use Section 4.5 to compute $J(k)/2J(k)$ when k is a number field. It injects into $H^1(k, J[2])$, so we will need to describe the G-action on $J[2]$.

Let $\alpha_1, \ldots, \alpha_{2g+1}$ be the zeros of $f(x)$ in $\overline{k}$. Let $W_i = (\alpha_i, 0) \in X(\overline{k})$. Let $\mathcal{W} = \{W_1, \ldots, W_{2g+1}\}$, which is a G-set. The set $\mathcal{W} \cup \{\infty\}$ of $2g+2$ points is the set of ramification points of π over $\overline{k}$. Let $\left(\frac{\mathbb{Z}}{2\mathbb{Z}}\right)^{\mathcal{W}}$ be the free $\mathbb{Z}/2\mathbb{Z}$-module with basis $W_1, \ldots, W_{2g+1}$: it is a G-module.

Proposition 6.1.1. *There is a split exact sequence of G-modules*

$$\begin{tikzcd}
0 \arrow[r] & \frac{\mathbb{Z}}{2\mathbb{Z}} \arrow[r, "\Delta"] & \left(\frac{\mathbb{Z}}{2\mathbb{Z}}\right)^{\mathcal{W}} \arrow[r, "s"] & J[2] \arrow[r] & 0 \\
& 1 \arrow[r, mapsto] & (1,\ldots,1) & & \\
& & (a_1,\ldots,a_{2g+1}) \arrow[r, mapsto] & \sum a_i[W_i-\infty]. &
\end{tikzcd}$$

Proof.

Step 1: s is well-defined.

The rational function $x-\alpha_i$ on $\mathbb{P}^1_{\overline{k}}$ has divisor $(\alpha_i)-(\infty)$, so when viewed as a function on $\overline{X}$ (via composing with π), its divisor is $\pi^*((\infty)-(\alpha_i)) = 2W_i - 2\infty$, where the last ∞ is the unique point at infinity on $\overline{X}$: the coefficients 2 that arise are the ramification indices of π at W_i and ∞. Therefore in $J(\overline{k}) = \operatorname{Pic}^0 \overline{X}$, we have

$$0 = [2W_i - 2\infty] = 2[W_i - \infty],$$

so $[W_i - \infty] \in J[2]$. Thus s is well-defined.

Step 2: The maps Δ and s are G-module homomorphisms.

This is obvious.

Step 3: The composition $s \circ \Delta$ is 0.

Let v_∞ be the valuation on $\mathbf{k}(\overline{X})$ associated to the point ∞. From $v_\infty(x) = -2$, we get $v_\infty(f(x)) = (2g+1)(-2)$, and the equation $y^2 = f(x)$ implies $v(y) = -(2g+1)$. On the other hand, the rational function y has a zero at each W_i, and the degree of its divisor must be 0, so its divisor is

$$(y) = W_1 + \cdots + W_{2g+1} - (2g+1)\infty.$$

Taking classes in $\operatorname{Pic}^0 \overline{X} = J(\overline{k})$, we get

$$0 = [W_1 - \infty] + \cdots + [W_{2g+1} - \infty].$$

Thus $s \circ \Delta = 0$.

Step 4: $\ker(s)$ *is generated by* $(1,\ldots,1)$.

Suppose $(a_1,\ldots,a_{2g+1}) \in \ker(s)$, where $a_i \in \{0,1\}$ are not all 1. Then

$$\sum_{i=1}^{2g+1} a_i[W_i - \infty] = 0,$$

so there exists $h \in \mathbf{k}(\overline{X})$ such that

$$\sum a_i W_i - (\sum a_i)\infty = (h).$$

In particular, h is regular outside ∞, so h is in the affine coordinate ring of $y^2 = f(x)$, and hence

$$h = h_1(x) + h_2(x)y$$

for some polynomials h_1 and h_2. Now

$$2g+1 > \sum a_i = -v_\infty(h) = \max\{2\deg h_1, 2\deg h_2 + (2g+1)\}.$$

Thus $h_2 = 0$, and $h = h_1(x) = \prod(x - \lambda_j)$ for some $\lambda_j \in \overline{k}$. But $x - \lambda_j$ has even valuation (either 0 or 2) at every W_i, so $a_i = v_{W_i}(h)$ is even. Thus $a_i = 0$ for all i.

Step 5: The map s is surjective.

The image of s has size

$$\#\left(\frac{\mathbb{Z}}{2\mathbb{Z}}\right)^{\mathcal{W}} / \# \frac{\mathbb{Z}}{2\mathbb{Z}} = 2^{2g+1}/2 = 2^{2g} = \#J[2],$$

where the last equality is from Theorem 4.1.5(ii).

Step 6: The exact sequence splits.

The injection Δ is split by the homomorphism

$$\begin{aligned} \left(\frac{\mathbb{Z}}{2\mathbb{Z}}\right)^{\mathcal{W}} &\overset{\text{sum}}{\to} \frac{\mathbb{Z}}{2\mathbb{Z}} \\ (a_1, \ldots, a_{2g+1}) &\mapsto \sum a_i \end{aligned}$$

in the opposite direction: $\text{sum} \circ \Delta$ is the identity on $\mathbb{Z}/2\mathbb{Z}$ since $2g+1$ is odd. □

We now work towards a reinterpretation of Proposition 6.1.1 that will make computing $H^1(k, J[2])$ easier. Let $L = \frac{k[T]}{(f(T))}$, which is a finite-dimensional k-algebra. Since f is squarefree, L will be a product of fields, one for each irreducible factor of f. Also define the $\overline{k}$-algebra

$$\overline{L} := L \underset{k}{\otimes} \overline{k} \simeq \frac{\overline{k}[T]}{(f(T))} \simeq \prod \frac{\overline{k}[T]}{(T - \alpha_i)} \simeq \overline{k}^{\mathcal{W}}.$$

For any ring R, define $\mu_2(R) := \{r \in R : r^2 = 1\}$; this is a group under multiplication. Since $\overline{L}$ is a finite-dimensional $\overline{k}$-algebra, we have a norm map $\mathrm{N}_{\overline{L}/\overline{k}} \colon \overline{L} \to \overline{k}$. If we write $(a_1, \ldots, a_{2g+1}) \in \overline{k}^{\mathcal{W}} \simeq \overline{L}$, then $\mathrm{N}_{\overline{L}/\overline{k}}((a_1, \ldots, a_{2g+1})) = a_1 \cdots a_{2g+1} \in \overline{k}$.

Proposition 6.1.2. *There is a split exact sequence of G-modules*

$$0 \to J[2] \to \mu_2(\overline{L}) \overset{\mathrm{N}}{\to} \mu_2(\overline{k}) \to 0.$$

Proof. Since the exact sequence in Proposition 6.1.1 is split, its middle term is the direct sum of the outer terms, and we may write the sequence backwards:

$$0 \to J[2] \to \left(\frac{\mathbb{Z}}{2\mathbb{Z}}\right)^{\mathcal{W}} \overset{\text{sum}}{\to} \frac{\mathbb{Z}}{2\mathbb{Z}} \to 0.$$

Under the identifications

$$\begin{aligned} \mu_2(\overline{L}) &\simeq \mu_2\left(\overline{k}^{\mathcal{W}}\right) = \{\pm 1\}^{\mathcal{W}} \simeq \left(\frac{\mathbb{Z}}{2\mathbb{Z}}\right)^{\mathcal{W}} \\ \mu_2(\overline{k}) &= \{\pm 1\} \simeq \frac{\mathbb{Z}}{2\mathbb{Z}}, \end{aligned}$$

the homomorphism N: $\mu_2(\overline{L}) \to \mu_2(\overline{k})$ induced by $\mathrm{N}_{\overline{L}/\overline{k}}$ corresponds to

$$\left(\frac{\mathbb{Z}}{2\mathbb{Z}}\right)^{\mathcal{W}} \overset{\text{sum}}{\to} \frac{\mathbb{Z}}{2\mathbb{Z}}.$$

□

6.2. Galois cohomology of $J[2]$

Theorem 6.2.1. *There is an isomorphism*

$$H^1(k, J[2]) \simeq \ker\left(\frac{L^\times}{L^{\times 2}} \overset{\mathrm{N}}{\to} \frac{k^\times}{k^{\times 2}}\right).$$

Proof. The exact sequence in Proposition 6.1.2 is split, so the long exact sequence of cohomology breaks into short exact sequences. In particular,

$$H^1(k, J[2]) \simeq \ker\left(H^1(k, \mu_2(\overline{L})) \overset{\mathrm{N}}{\to} H^1(k, \mu_2(\overline{k}))\right).$$

Now substitute the identifications

$$\begin{aligned} H^1(k, \mu_2(\overline{L})) &\simeq \frac{L^\times}{L^{\times 2}} \\ H^1(k, \mu_2(\overline{k})) &\simeq \frac{k^\times}{k^{\times 2}} \end{aligned}$$

given by Remark 4.5.1. □

6.3. The $x - T$ map

By (4.5.2) we have a descent map

$$\delta \colon \frac{J(k)}{2J(k)} \hookrightarrow H^1(k, J[2]).$$

Theorem 6.2.1 gives a concrete interpretation of $H^1(k, J[2])$. So δ can be interpreted as a map

$$\frac{J(k)}{2J(k)} \hookrightarrow \ker\left(\frac{L^\times}{L^{\times 2}} \xrightarrow{\mathrm{N}} \frac{k^\times}{k^{\times 2}}\right).$$

The goal of this section is to describe this map explicitly without having to mention cocycles and coboundaries.

Start with the map of G-sets

$$\begin{aligned} X(\overline{k}) - (\mathcal{W} \cup \{\infty\}) &\to \overline{L}^\times \\ P &\mapsto x(P) - T, \end{aligned}$$

where T is the image of T in $\overline{L} = \frac{\overline{k}[T]}{(f(T))}$. Extend by linearity to get a G-module homomorphism

$$\begin{aligned} (\operatorname{Div} \overline{X})' &\to \overline{L}^\times \\ \sum n_P P &\mapsto \prod (x(P) - T)^{n_P}, \end{aligned}$$

where $(\operatorname{Div} \overline{X})'$ is the subgroup of divisors in $\operatorname{Div} \overline{X}$ in which the points of $\mathcal{W} \cup \{\infty\}$ do not appear. Taking G-invariants gives a homomorphism

$$(\operatorname{Div} X)' \to L^\times.$$

If $h \in \mathbf{k}(X)^\times$ has no zeros or poles in $\mathcal{W} \cup \{\infty\}$, then this homomorphism maps the divisor $\operatorname{div} h := (h)$ to an element of $L^\times$ whose i^{th} component in $\overline{L}^\times \simeq \overline{k}^{\mathcal{W}}$ equals

$$(x - \alpha_i)(\operatorname{div} h) = h(\operatorname{div}(x - \alpha_i)) = h(2W_i - 2\infty) = h(W_i - \infty)^2,$$

where we used Theorem 1.9.5 in the first step. It follows that (h) maps to an element of $L^{\times 2}$. Therefore we get a well-defined homomorphism

$$\operatorname{Pic} X \to \frac{L^\times}{L^{\times 2}}:$$

we do not need to write $(\operatorname{Pic} X)'$, since every divisor in $\operatorname{Div} X$ is linearly equivalent to one in $(\operatorname{Div} X)'$. Since $X(k)$ is nonempty (it contains ∞), we have $J(k) = \operatorname{Pic}^0 X$. The composition

$$J(k) = \operatorname{Pic}^0 X \hookrightarrow \operatorname{Pic} X \to \frac{L^\times}{L^{\times 2}}$$

is called the $x-T$ map. If $P=(a,b)\in X(\overline{k})$ then $\mathrm{N}_{\overline{L}/\overline{k}}(a-T)=\prod_{i=1}^{2g+1}(a-\alpha_i)=f(a)=b^2$; from this we deduce that the image of the $x-T$ map is contained in $\ker\left(\frac{L^\times}{L^{\times 2}}\xrightarrow{\mathrm{N}}\frac{k^\times}{k^{\times 2}}\right)$. The codomain of the $x-T$ map is killed by 2, so we get an induced $x-T$ map

$$\frac{J(k)}{2J(k)}\xrightarrow{x-T}\ker\left(\frac{L^\times}{L^{\times 2}}\xrightarrow{\mathrm{N}}\frac{k^\times}{k^{\times 2}}\right).$$

Theorem 6.3.1. *This $x-T$ map equals the composition of the maps*

$$\frac{J(k)}{2J(k)}\overset{\delta}{\hookrightarrow}H^1(k,J[2])\simeq\ker\left(\frac{L^\times}{L^{\times 2}}\xrightarrow{\mathrm{N}}\frac{k^\times}{k^{\times 2}}\right)$$

given in (4.5.2) *and Theorem 6.2.1.*

Proof. ♣♣♣ Bjorn: [Skipped.] □

6.4. The 2-Selmer group

In this section, k is a number field. Section 4.6.2 defined the 2-Selmer group $\mathrm{Sel}=\mathrm{Sel}(k,J[2])$ as a subgroup of $H^1(k,J[2])$. We can now use the $x-T$ map in place of the descent map δ to give a concrete description of Sel. First, (4.6.3) becomes

(6.4.1)
$$\begin{tikzcd}
\frac{J(k)}{2J(k)} \arrow[r, hook, "\text{global } x-T"] \arrow[d] & \ker\left(\frac{L^\times}{L^{\times 2}}\xrightarrow{\mathrm{N}}\frac{k^\times}{k^{\times 2}}\right) \arrow[d, "\prod \mathrm{res}_v"] \\
\prod_v \frac{J(k_v)}{2J(k_v)} \arrow[r, hook, "\text{local } x-T"] & \prod_v \ker\left(\frac{L_v^\times}{L_v^{\times 2}}\xrightarrow{\mathrm{N}}\frac{k_v^\times}{k_v^{\times 2}}\right),
\end{tikzcd}$$

where $L_v:=L\underset{k}{\otimes}k_v\simeq\frac{k_v[T]}{(f(T))}$. Thus Sel is concretely the subgroup of $\ker\left(\frac{L^\times}{L^{\times 2}}\xrightarrow{\mathrm{N}}\frac{k^\times}{k^{\times 2}}\right)$ consisting of elements whose image in $\prod_v\ker\left(\frac{L_v^\times}{L_v^{\times 2}}\xrightarrow{\mathrm{N}}\frac{k_v^\times}{k_v^{\times 2}}\right)$ is in the image of the product of the local $x-T$ maps.

♣♣♣ Bjorn: [To be continued]

Exercises

6.1. Prove that

$$\dim_{\mathbb{F}_2}J[2](k)=\#\{G\text{-orbits in }\mathcal{W}\}-1.$$

6.2. Suppose instead that f is squarefree of degree $2g+2$. Let $\alpha_1,\dots,\alpha_{2g+2}$ be the zeros of f in $\overline{k}$, let $W_i=(\alpha_i,0)$, and let $\mathcal{W}=\{W_1,\dots,W_{2g+2}\}$. Let $\left(\frac{\mathbb{Z}}{2\mathbb{Z}}\right)^{\mathcal{W}}_{\mathrm{sum}=0}$ be the kernel of the sum map $\left(\frac{\mathbb{Z}}{2\mathbb{Z}}\right)^{\mathcal{W}}\to\frac{\mathbb{Z}}{2\mathbb{Z}}$. Prove that there is a (not necessarily split) exact sequence of G-modules

$$0\to\frac{\mathbb{Z}}{2\mathbb{Z}}\to\left(\frac{\mathbb{Z}}{2\mathbb{Z}}\right)^{\mathcal{W}}_{\mathrm{sum}=0}\to J[2]\to 0.$$

CHAPTER 7

Étale covers and general descent

Étale covers are the algebraic analogue of covering spaces in topology.

Warning 7.0.2. More precisely, we should say connected finite étale covers. But we will deal only with étale covers $X' \to X$ in which both X' and X are nice varieties; in this case, one can show that the extra adjectives "connected" and "finite" are automatic.

7.1. Definition of étale

Definition 7.1.1. Let $\pi \colon X' \to X$ be a dominant morphism of nice k-varieties of the same dimension, as in Section 1.8.4. Then π is étale if the following two conditions are satisfied:

(1) For each $x \in X(\overline{k})$, the fiber $\pi^{-1}(x)$ is finite (0-dimensional).

(2) The morphism π is unramified at every irreducible divisor D' of X'.

In this case, X is called an étale cover of Y.

Remark 7.1.2. One can show that a morphism $\pi \colon X' \to X$ is étale if and only if it is so after an extension of the base field.

Remark 7.1.3. In the definition of étale morphism between more general schemes, the first condition is replaced by the condition that π be *flat*. In the situation we are considering (a dominant morphism between nice varieties of the same dimension), flatness is equivalent to the geometric condition we have given. ♣♣♣ Bjorn: [Check this.]

Warning 7.1.4. By restricting attention to nice varieties, we excluded some covers that technically are étale. Some examples: a Zariski open subvariety of an étale cover is étale, and a disjoint union of étale covers is étale.

7.2. Constructions of étale covers

7.2.1. A non-example. Let $X = \mathbb{P}^2$, and let $\pi \colon X' \to X$ be the blowup of X at a point $P \in \mathbb{P}^2(k)$. Although every irreducible divisor on X' mapping surjectively to a divisor on X is unramified, the morphism π is not étale, because the fiber above P is not finite.

7.2.2. Another non-example. Let E be an elliptic curve, the smooth projective model of $y^2 = f(x)$ over $\mathbb{Q}$, where f is a squarefree polynomial of degree 3. Then the x-coordinate map $x\colon E \to \mathbb{P}^1$ has finite fibers, but is not étale since it is ramified at $(\alpha, 0) \in E(\overline{\mathbb{Q}})$ for any zero α of f.

7.2.3. An étale cover of a hyperelliptic curve. Let X be the smooth projective model of $y^2 = (x^2+2)(x^3+5)$ over $\mathbb{Q}$, as constructed in Section 2.8.1. So $\mathbf{k}(X) = \mathbb{Q}(x, \sqrt{(x^2+2)(x^3+5)})$. Let X' be the nice curve with $\mathbf{k}(X') = \mathbf{k}(X)(\sqrt{x^2+2})$, so we have a degree-2 morphism $\pi\colon X' \to X$.

$$\begin{tikzcd}
& \mathbf{k}(X') = \mathbb{Q}(x, \sqrt{x^2+2}, \sqrt{x^3+5}) \arrow[dl, dash] \arrow[d, dash, "\text{unramified}"] \arrow[dr, dash] & \\
\mathbb{Q}(x, \sqrt{x^2+2}) \arrow[dr, dash] & \mathbf{k}(X) = \mathbb{Q}(x, \sqrt{(x^2+2)(x^3+5)}) \arrow[d, dash] & \mathbb{Q}(x, \sqrt{x^3+5}) \arrow[dl, dash] \\
& \mathbb{Q}(x) &
\end{tikzcd}$$

Proposition 7.2.1. *The morphism π is étale.*

Proof. Each fiber is finite, since otherwise it would be all of X'. Also, π is unramified above any point of X where x^2+2 has even valuation; this includes $\infty \in X$ (since x^2+2 equals x^2 times a unit there) and all affine points on $y^2 = (x^2+2)(x^3+5)$ where x^2+2 is nonvanishing. But $\mathbf{k}(X')$ is the same field as $\mathbf{k}(X)(\sqrt{x^3+5})$, so π is unramified also above any affine point where x^3+5 is nonvanishing. Since $\gcd(x^2+2, x^3+5) = 1$, the morphism π is everywhere unramified. □

For a generalization, see Example 7.2.6.

7.2.4. Abhyankar's lemma.

Definition 7.2.2. Suppose we have a commutative diagram of nice curves

$$\begin{tikzcd}
& Z \arrow[dl] \arrow[dr] & \\
Y_1 \arrow[dr, "\pi_1"'] & & Y_2 \arrow[dl, "\pi_2"] \\
& X. &
\end{tikzcd}$$

Identify $\mathbf{k}(X)$, $\mathbf{k}(Y_1)$, $\mathbf{k}(Y_2)$ with their images in $\mathbf{k}(Z)$. Call Z a compositum of Y_1, Y_2 over X if $\mathbf{k}(Z)$ is the compositum of its subfields $\mathbf{k}(Y_1), \mathbf{k}(Y_2)$.

Theorem 7.2.3 (Abhyankar's Lemma). *Suppose Z is a compositum as above. Suppose moreover that for each $y_1 \in Y_1(\overline{k})$ and $y_2 \in Y_2(\overline{k})$ such that $\pi_1(y_1) = \pi_2(y_2)$, the ramification indices satisfy*

$$\operatorname{char} k \nmid e_{\pi_2}(y_2) \mid e_{\pi_1(y_1)}.$$

Then $Z \to Y_1$ is étale.

Definition 7.2.4. When the ramification divisibilities are satisfied, one says that $Y_1 \to X$ absorbs the (tame) ramification of $Y_2 \to X$.

Remark 7.2.5. Abhyankar's lemma is really a local statement: to check whether $Z \to Y_1$ is étale at a point $z \in Z$, one need only check the ramification conditions at the images y_1, y_2 of z in Y_1, Y_2, respectively. The algebraic fact underlying Abhyankar's lemma is that if $k = \overline{k}$ and $\operatorname{char} k \nmid n$, then the only degree-$n$ field extension of the Laurent series field $k((t))$ is $k((t^{1/n}))$.

Example 7.2.6. Let k be a field of characteristic not 2. Let $f(x), g(x) \in k[x]$ be relatively prime squarefree non-constant polynomials, such that either $\deg f$ or $\deg g$ is even. Let Y_1 be the smooth projective model of the affine curve $y^2 = f(x)g(x)$. Let Z be the degree-2 cover of Y_1 with $\mathbf{k}(Z) = \mathbf{k}(Y_1)(\sqrt{f(x)}) = \mathbf{k}(Y_1)(\sqrt{g(x)})$. We will use Abhyankar's lemma to prove that $Z \to Y_1$ is étale.

Without loss of generality, assume that $\deg f$ is even. Let X and Y_2 be the curves with function fields $k(x)$ and $k(x, \sqrt{f(x)})$, respectively. Thus we have a diagram

$$\begin{tikzcd}
& Z \arrow[dl, "\text{étale?}"'] \arrow[dr] & \\
Y_1 \arrow[dr, "\pi_1"'] & & Y_2 \arrow[dl, "\pi_2"] \\
& X = \mathbb{P}^1 &
\end{tikzcd}$$

in which Z is the compositum of Y_1 and Y_2. The ramification of $\pi_2 \colon Y_2 \to X$ lies above the zeros of f (and not above ∞, since $\deg f$ is even), and the ramification index at each ramified point is 2. Above these same points of X, the morphism $\pi_1 \colon Y_1 \to X$ is ramified with ramification index 2 (and π_1 is also ramified at other points). Thus $Y_1 \to X$ absorbs the ramification of $Y_2 \to X$, and $Z \to Y_1$ is étale.

7.2.5. Étale covers of abelian varieties. Let $\pi\colon A' \to A$ be an isogeny of abelian varieties. Then π is étale if and only if it is separable.

Suppose that π is separable and that the $\overline{k}$-points of $\ker \pi$ are individually defined over k. Then $\mathbf{k}(A')$ is a Galois extension of $\mathbf{k}(A)$ with Galois group canonically isomorphic to the abelian group $\ker \pi$ (i.e., the group of k-points of $\ker \pi$). A point $P \in \ker \pi$ acts on a rational function $f \in \mathbf{k}(A')$ by composing f with translation-by-P.

Remark 7.2.7. If $k = \overline{k}$, all (nice) étale covers of A arise from separable isogenies.

7.2.6. Geometric class field theory. Let X be a nice k-curve of genus $g \geq 1$. Let $J = \operatorname{Jac} X$. Suppose that we have $P \in X(k)$, so we get an Albanese morphism $X \hookrightarrow J$ as in Theorem 5.3.1. Let $\pi\colon A \to J$ be a separable isogeny. Then in the following diagram, $\pi^{-1}(X) \subseteq A$ is an étale cover of X:

$$\begin{tikzcd}
\pi^{-1}(X) \arrow[r] \arrow[d] & A \arrow[d] \\
X \arrow[r] & J.
\end{tikzcd}$$

Remark 7.2.8. It is true, but not obvious, that $\pi^{-1}(X)$ is irreducible.

Suppose $k = \overline{k}$. Then, as in Section 7.2.5, $\mathbf{k}(\pi^{-1}(X))$ is an abelian extension of $\mathbf{k}(X)$. One of the results of geometric class field theory says that all unramified abelian extensions of the function field $\mathbf{k}(X)$ arise in this way.

Remark 7.2.9. There exist *generalized Jacobians* that are to the Jacobian as ray class groups are to the class group in the number field situation. All abelian extensions of the function field of a curve X, ramified or not, arise from separable isogenies to generalized Jacobians of X.

A good reference for everything in this section is [Ser88].

7.2.7. Fundamental group. This section should be considered an extended remark: we will give no proofs.

Let X be a nice variety over $\mathbb{C}$. If $X' \to X$ is an étale morphism from another nice $\mathbb{C}$-variety X', then $X'(\mathbb{C}) \to X(\mathbb{C})$ is a finite-to-1 topological covering. Conversely, a generalization of the *Riemann existence theorem* implies that any finite-to-1 topological covering comes from an étale morphism of nice algebraic varieties.

Let $\pi_1(X(\mathbb{C}))$ be the topological fundamental group of the connected compact complex manifold $X(\mathbb{C})$. The isomorphism classes of topological covering spaces of $X(\mathbb{C})$ are in bijection with the (conjugacy classes of) subgroups of $\pi_1(X(\mathbb{C}))$. And the isomorphism classes of finite-to-1 topological covering spaces are in bijection with the (conjugacy classes of) finite-index subgroups of $\pi_1(X(\mathbb{C}))$, or equivalently the open subgroups of the profinite completion $\pi_1(X(\mathbb{C}))$.

Putting the previous two paragraphs together, we may construct étale covers of X by giving a finite-index subgroup of $\pi_1(X(\mathbb{C}))$. Turning things around, we can define the profinite completion of $\pi_1(X(\mathbb{C}))$ purely algebraically, in terms of étale covers: the group so defined is called the algebraic fundamental group of X and is denoted $\pi_1^{\text{alg}}(X)$.

Warning 7.2.10. Strictly speaking, we should fix a basepoint when defining all these fundamental groups.

Example 7.2.11. If X is a nice genus-g curve over $\mathbb{C}$, then $X(\mathbb{C})$ is a g-holed torus. Algebraic topology then implies that $\pi_1(X(\mathbb{C}))$ is a finitely presented group with $2g$ generators $x_1, \ldots, x_g, y_1, \ldots, y_g$ and a single relation

$$[x_1, y_1][x_2, y_2] \cdots [x_g, y_g] = 1,$$

where $[x, y]$ is an abbreviation for the commutator $xyx^{-1}y^{-1}$. If $g \geq 2$, this group is non-abelian and moreover has many non-abelian finite quotients.

Remark 7.2.12. We will not make this precise, but if k is an algebraically closed field of characteristic $p \geq 0$, and X is a nice k-variety, we can ask how $\pi_1^{\text{alg}}(X)$ compares to $\pi_1^{\text{alg}}(Y)$ for a $\mathbb{C}$-variety Y having the "same geometry" as X (e.g., a curve of the same genus, if X is a curve). It turns out that these profinite groups need not be isomorphic, but the largest prime-to-p quotient of $\pi_1^{\text{alg}}(X)$ is isomorphic to the largest prime-to-p quotient of $\pi_1^{\text{alg}}(Y)$. This can be used to prove the existence of certain étale covers of nice varieties in positive characteristic.

7.3. Galois étale covers

Definition 7.3.1. Let $\pi \colon X' \to X$ be an étale morphism between nice k-varieties. Let G be a finite group. One says that X' is a Galois étale cover of X with Galois group G if $\mathbf{k}(X')$ is Galois over $\mathbf{k}(X)$ with Galois group G.

Remark 7.3.2. Suppose $g \in G$. Then g induces a rational map $X' \dashrightarrow X'$ and one can show that in fact it is an automorphism of X' over X. We view G as acting on the left on

$\mathbf{k}(X')$ and on the right on X'. Hence we get a morphism of k-varieties

$$\begin{aligned} X' \times G &\to X' \\ (x, g) &\mapsto xg \end{aligned}$$

in which G is to be interpreted as a constant group scheme consisting of a disjoint union of copies of $\operatorname{Spec} k$, one for each element of G, so that $X' \times G$ is a similar disjoint union of copies of X'.

This leads to an equivalent definition of Galois cover. Namely, suppose that $\pi\colon X' \to X$ is an étale morphism between nice k-varieties and G is a finite group acting on X' such that each $g \in G$ respects π; i.e.,

$$\begin{tikzcd} X' \arrow[rr, "g"] \arrow[dr, "\pi"'] & & X' \arrow[dl, "\pi"] \\ & X & \end{tikzcd}$$

commutes. Then $\pi\colon X' \to X$ is Galois étale with Galois group G if and only if the morphism

$$\begin{aligned} X' \times G &\to X' \underset{X}{\times} X' \\ (x, g) &\mapsto (x, xg) \end{aligned}$$

is an isomorphism of varieties. This is the same as saying that X' is a family of torsors under G over the base X!

Example 7.3.3. Let $\pi\colon A' \to A$ be a separable isogeny between abelian varieties over k. Then π is Galois étale if and only if all points of $\ker \pi$ are defined over k (and in this case the Galois group is the group of k-points of $\ker \pi$).

Definition 7.3.4. Let $\pi\colon X' \to X$ be an étale morphism between nice k-varieties. Let G be a finite group. One says that X' is a geometrically Galois étale cover of X with Galois group G if the base extension $X'_{\overline{k}} \to X_{\overline{k}}$ is Galois étale with Galois group G.

If $\pi\colon X' \to X$ is a geometrically Galois étale cover with Galois group G, then the action of $\mathcal{G} := \operatorname{Gal}(\overline{k}/k)$ on automorphisms of $X'_{\overline{k}}$ makes G into a $\mathcal{G}$-group, i.e., a (possibly non-abelian) group equipped with a (left) action of $\mathcal{G}$.

7.4. Descent using Galois étale covers: an example

7.4.1. An example. Suppose (as in [Fly00] ♣♣♣ Bjorn: [add page number]) 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

$$\begin{aligned} Z^2 &\equiv -X^2 \pmod{p} \\ Z^4 &\equiv -X^4 \pmod{p} \end{aligned}$$

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 affine curves

$$\begin{aligned} Y_1^\circ: &\quad w^2 = x^4 + 1 \\ Y_2^\circ: &\quad 2w^2 = x^4 + 1. \end{aligned}$$

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 $Y_1^\circ(\mathbb{Q})$, and $(1, 1)$ belongs to $Y_2^\circ(\mathbb{Q})$, 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

$$\begin{aligned} \text{32A2}: &\quad y^2 = x^3 - x \\ \text{64A1}: &\quad y^2 = x^3 - 4x, \end{aligned}$$

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. It follows that rational points on Y_1° satisfy $x = 0$ (there are two more rational points at infinity), and rational points on Y_2° satisfy $x \in \{\pm 1\}$. So the answer to the original problem is that there are six solutions, namely:

$$(0,1),(0,-1),(1,2),(1,-2),(-1,2),(-1,-2).$$

7.4.2. 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 $\mathbb{Q}$-curve containing U as an open subscheme. By Section 2.8.1, X is a genus-2 curve over $\mathbb{Q}$, obtained by glueing U to another affine curve U' (which happens to be isomorphic to U). 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' Theorem.

Let Z be the nice $\mathbb{Q}$-curve birational to the curve in (x, y, w)-space defined by the system

$$\begin{aligned} y^2 &= (x^2+1)(x^4+1) \\ w^2 &= x^4+1, \end{aligned}$$

so $\mathbf{k}(Z) = \mathbb{Q}(x, \sqrt{x^2+1}, \sqrt{x^4+1})$. For $c \in \mathbb{Q}^\times$, let Z_c be the twist of Z that is birational to the curve

$$\begin{aligned} y^2 &= (x^2+1)(x^4+1) \\ cw^2 &= x^4+1. \end{aligned}$$

For each c, there is a degree-2 morphism

$$\begin{aligned} Z_c &\to X \\ (x,y,w) &\mapsto (x,y). \end{aligned}$$

By Abhyankar's lemma, as in Example 7.2.6, $Z_c \to X$ is étale for each c. In fact, it is a Galois étale cover with Galois group $\mathbb{Z}/2\mathbb{Z}$.

The argument of the previous section can be reinterpreted as follows:

- Each point in $X(\mathbb{Q})$ is the image of $f_c\colon Z_c(\mathbb{Q}) \to X(\mathbb{Q})$ for some $c \in \mathbb{Q}^\times$.

- Up to multiplying c by an element of $\mathbb{Q}^{\times 2}$, 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

$$\begin{aligned} \pi_c \colon Z_c &\to Y_c \\ (x, y, w) &\mapsto (x, w). \end{aligned}$$

Fortunately, for $c \in \{1, 2\}$, the curve Y_c is an elliptic curve of rank 0, so $Y_c(\mathbb{Q}) = Y_c(\mathbb{Q})_{\mathrm{tors}}$ 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 7.4.1. The elliptic curve

$$E\colon \quad y^2 = (t + 1)(t^2 + 1)$$

is dominated by X, by the morphism

$$\begin{aligned} \phi \colon X &\to E \\ (x, y) &\mapsto (x^2, y). \end{aligned}$$

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 $\operatorname{rk} J(\mathbb{Q}) = 2$ is not less than $g(X) = 2$, so the method of Chabauty and Coleman cannot be applied directly to X. On the other hand, X has two independent maps to E, so another way to determine $X(\mathbb{Q})$ would be to use the method of Demjanenko-Manin [Ser97]♣♣♣ Bjorn: [add precise section number].

7.5. Descent using Galois étale covers: general theory

♣♣♣ Bjorn: [To be added]

Remark 7.5.1. ♣♣♣ Bjorn: [Mention descent using torsors of positive-dimensional groups]

7.6. The Chevalley-Weil theorem

As a consequence of the previous section ♣♣♣ Bjorn: [], we can deduce the following weak version of Theorem **??**.

THEOREM 7.6.1. *Let k be a number field. Let $\pi\colon X' \to X$ be an étale morphism between nice k-varieties. Then there exists an effectively computable finite extension L of k in $\overline{k}$ such that the inverse image of $X(k)$ under $X'(\overline{k}) \to X(\overline{k})$ is contained in $X'(L)$.*

REMARK 7.6.2. There is a version of the Chevalley-Weil theorem for not necessarily projective varieties, but this general version is a theorem about *finite* étale morphisms and *integral* points. When we restrict to projective varieties X over a number field k, we can choose a projective model $\mathcal{X}$ over some ring $\mathcal{O}_{k,S}$ of S-integers, and then the valuative criterion for properness [Har77, II.4] ♣♣♣ Bjorn: [fix this], implies $X(k) = \mathcal{X}(\mathcal{O}_{k,S})$; also étale morphisms between projective varieties are automatically finite. This is why for projective varieties we can state the Chevalley-Weil theorem as a theorem about rational points.

Exercises

7.1. (a) Let k be an algebraically closed field of characteristic not 2. Let X be a genus-g curve over k. Prove that there exists a Galois étale cover $X' \to X$ with Galois group $(\mathbb{Z}/2\mathbb{Z})^{2g}$.

(b) If X is the smooth projective model of $y^2 = f(x)$ where f is a squarefree polynomial of degree $2g+2$, construct the function field of such an X' as an explicit extension of $k(x)(\sqrt{f(x)})$.

7.2. Let X be the smooth projective model over $y^3 = (x^3+2)(x^3+x+5)$ over a field k of characteristic not 3. Let X' be the nice curve whose function field is $\mathbf{k}(X)(\sqrt[3]{x^3+2})$.

(a) Prove that $X' \to X$ is étale.

(b) Prove that $X' \to X$ is geometrically Galois étale with Galois group isomorphic to the $\mathcal{G}$-group μ_3 whose elements are the cube roots of 1 in $\overline{k}$.

(c) For what k is $X' \to X$ Galois étale?

7.3. For $n \geq 1$, let C_n denote the smooth projective model of the affine curve $y^n = x(x-1)$ over $\mathbb{C}$.

(a) Compute the ramification of $x\colon C_n \to \mathbb{P}^1$.

(b) A Belyi map for a nice curve X is a dominant morphism $X \to \mathbb{P}^1$ ramified at most above $0, 1, \infty \in \mathbb{P}^1$. Belyi's theorem states that any nice curve X over $\overline{\mathbb{Q}}$ has a Belyi map. (Conversely, a nice curve X over $\mathbb{C}$ with a Belyi map is automatically definable over $\overline{\mathbb{Q}}$.) Using Belyi's theorem, prove that any nice curve X over $\overline{\mathbb{Q}}$ is dominated by an étale cover of C_n for some $n \geq 1$.

CHAPTER 8

The method of Chabauty and Coleman

CHAPTER 9

The Mordell-Weil sieve

Acknowledgements

I thank David Brown, David Freeman, Anthony Varilly, and David Zywina for comments and corrections. (If I forgot to thank you, let me know so that I can add your name here.)

Bibliography

[ACGH85] E. Arbarello, M. Cornalba, P. A. Griffiths, and J. Harris, *Geometry of algebraic curves. Vol. I*, Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences], vol. 267, Springer-Verlag, New York, 1985.MR770932 (86h:14019) ↑2.11.7

[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) ↑5.1.7

[Cre97] J. E. Cremona, *Algorithms for modular elliptic curves*, 2nd ed., Cambridge University Press, Cambridge, 1997.MR1628193 (99e:11068) ↑7.4.1

[Del69] Pierre Deligne, *Variétés abéliennes ordinaires sur un corps fini*, Invent. Math. **8** (1969), 238–243 (French).MR0254059 (40 #7270) ↑4.2.19

[Fly00] E. Victor Flynn, *Coverings of curves of genus 2*, Algorithmic number theory (Leiden, 2000), 2000, pp. 65–84.MR1850599 (2002f:11074) ↑7.4.1

[Har77] Robin Hartshorne, *Algebraic geometry*, Springer-Verlag, New York, 1977. Graduate Texts in Mathematics, No. 52.MR0463157 (57 #3116) ↑1.5.1, 2.9.2, 2.9.1, 4.3.4, 7.6.2

[Hir64] Heisuke Hironaka, *Resolution of singularities of an algebraic variety over a field of characteristic zero. I, II*, Ann. of Math. (2) 79 (1964), 109–203; ibid. (2) **79** (1964), 205–326.MR0199184 (33 #7333) ↑2.1.2

[Mil86] J. S. Milne, *Jacobian varieties*, Arithmetic geometry (Storrs, Conn., 1984), 1986, pp. 167–212.MR861976 ↑5.1

[Ser02] Jean-Pierre Serre, *Galois cohomology*, Corrected reprint of the 1997 English edition, Springer Monographs in Mathematics, Springer-Verlag, Berlin, 2002. Translated from the French by Patrick Ion and revised by the author.MR1867431 (2002i:12004) ↑1.10

[Ser97] ———, *Lectures on the Mordell-Weil theorem*, 3rd ed., Aspects of Mathematics, Friedr. Vieweg & Sohn, Braunschweig, 1997. Translated from the French and edited by Martin Brown from notes by Michel Waldschmidt; With a foreword by Brown and Serre.MR1757192 (2000m:11049) ↑7.4.1

[Ser88] ———, *Algebraic groups and class fields*, Graduate Texts in Mathematics, vol. 117, Springer-Verlag, New York, 1988. Translated from the French.MR918564 (88i:14041) ↑7.2.6

[Ser55] ———, *Géométrie algébrique et géométrie analytique*, Ann. Inst. Fourier, Grenoble **6** (1955), 1–42 (French).MR0082175 (18,511a) ↑4.3.4

[Sil92] Joseph H. Silverman, *The arithmetic of elliptic curves*, Graduate Texts in Mathematics, vol. 106, Springer-Verlag, New York, 1992. Corrected reprint of the 1986 original.MR 95m:11054 ↑1.9, 1.9.6

[Tat] John Tate, *Classes d'isogénie des variétés abéliennes sur un corps fini (d'après T. Honda)*, Séminaire Bourbaki. Vol. 1968/69: Exposés 347–363, LEcture Notes in Mathematics, Vol. 179, Springer-Verlag, Berlin, 1971. Exposé 352, Novembre 1968. ↑4.2.3

[Wat69] William C. Waterhouse, *Abelian varieties over finite fields*, Ann. Sci. École Norm. Sup. (4) **2** (1969), 521–560.MR0265369 (42 #279) ↑4.2.3

[WM71] W. C. Waterhouse and J. S. Milne, *Abelian varieties over finite fields*, 1969 Number Theory Institute (Proc. Sympos. Pure Math., Vol. XX, State Univ. New York, Stony Brook, N.Y., 1969), 1971, pp. 53–64.MR0314847 (47 #3397) ↑4.2.3

[Wei49] André Weil, *Numbers of solutions of equations in finite fields*, Bull. Amer. Math. Soc. **55** (1949), 497–508.MR0029393 (10,592e) ↑3.2.2