NOTES ON THE ARITHMETIC OF ELLIPTIC CURVES

TYLER GENAO

Contents

Date: Last updated July 6, 2025.

Preface

This is a draft of my notes for a graduate topics course that I taught in Spring 2025 at the Ohio State University, on *the arithmetic of elliptic curves*. For the most part, these notes closely follow Silverman's book of the same name [Sil09]; however, I have included several new exercises and theorems, additional comments and details for several remarks and proofs from [Sil09], and an introductory "chapter zero" on elliptic curves from a planar perspective that should be accessible to a broad range of students.

There were a large number of earlier-year graduate students interested in attending this class, so the only prerequisite was a basic course on algebraic number theory. I did not assume prior knowledge of algebraic geometry; however, experience with that can help motivate the material in Chapters 1 and 2.

Any errors in these notes are my own, and if you spot any, then please let me know. My hope is that these notes can help beginning students in number theory learn about elliptic curves from the "canonical" elliptic curves textbook [Sil09] without too many prerequisites. If you find these notes helpful, or have comments or suggestions, feel free to reach out to me at genao.5@osu.edu – I would love to hear it!

Introduction

For more than a millennium, a centerpiece of number theory has been the study of **Diophantine equations:** simply put, these are polynomial equations over $\mathbb{Q}$. It has been, and still is, of great interest to determine whether specially chosen Diophantine equations $f(x_1, x_2, \ldots, x_n) \in \mathbb{Q}[x_1, x_2, \ldots, x_n]$ have *integral* or *rational* solutions: i.e., tuples $(a_1, a_2, \ldots, a_n)$ in $\mathbb{Z}^n$ or $\mathbb{Q}^n$ such that

$$f(a_1, a_2, \ldots, a_n) = 0.$$

An example of this is the *congruent number problem:* is there a worthwhile description of all *congruent* numbers, i.e., rational numbers which are the area of some right triangle with all rational sides (including the hypotenuse)? As it turns out, a number $\alpha \in \mathbb{Q}$ is a congruent number if and only if the equation

$$y^2 = x^3 - \alpha^2 x$$

has a rational solution $(x, y) \in \mathbb{Q}^2$ with $y \neq 0$.

Analyzing a Diophantine equation with "complete" geometry (i.e., over $\mathbb{C}$ or another algebraically closed field) can make it easier to find solutions, but integral and rational solutions are delicate, and can break unless special care is taken. This makes studying integral/rational solutions more difficult – and thus more interesting!

Certain types of Diophantine equations have well-known ways to parametrize their integral or rational solutions. Here are examples of this, in increasing difficulty:

1. An *integral (planar) line* has the form
$$ax + by = c$$
where $a, b, c \in \mathbb{Z}$.
   a. Rational solutions: take any $x \in \mathbb{Q}$, and then solve for y! (If $b = 0$ and $a \neq 0$, then instead let $x = c/a$ and $y \in \mathbb{Q}$. If $a = b = c = 0$, then anything works.)
   b. Integral solutions: there exists an integral solution $(x, y) \in \mathbb{Z}^2$ if and only if $\gcd(a, b) \mid c$; in such a case, this equation has infinitely many solutions, all of which are in fact parametrizable.
2. A *rational conic* is a plane curve with an equation of the form
$$ax^2 + bxy + cy^2 + dx + ey + f = 0$$
where $a, b, c, d, e, f \in \mathbb{Q}$. This includes circles, ellipses, parabolas and hyperbolas.
   a. For determining rational solutions, we have the *Hasse-Minkowski theorem:* this quadratic equation has a rational solution if and only if it has a real solution, along with, for each prime $p \in \mathbb{Z}^+$, a solution over $\mathbb{Q}_p$, the *field of p-adic numbers.* (This is an example of a *local-global principle* for quadratic equations.)
3. For $n \geq 3$, consider the equation
$$x^n + y^n = z^n.$$

Such an equation has no integer solutions $(a, b, c) \in (\mathbb{Z}_{>0})^3$; this is a consequence of **Fermat's last theorem.** A proof of this theorem came out in 1994, 357 years after it was originally stated in 1637. This was proven by contradiction: if there exists such a solution (a, b, c), then one can construct an *elliptic curve* $E_{a,b,c}$ from this solution which has self-contradicting properties. QED.

After studying curves of degrees 1 and 2 (lines and conics), it's natural to study the special class of cubic curves called **elliptic curves.** These curves are usually given as an equation

$$E : y^2 = x^3 + Ax + B$$

where A, B lie in a fixed field k (such as $k = \mathbb{Q}, \mathbb{R}, \mathbb{F}_p$, $\mathbb{Q}_p$ or $\mathbb{C}$). Unlike other curves, elliptic curves have the unique property that there is a *group law* on them which, when pictured as a planar curve, can be given by a *chord and tangent method.* The additional group structure lends itself to a rich theory of rational points on elliptic curves.

In these notes, we will cover the following topics:

1. Elliptic curves and their group law, from an introductory planar perspective.
2. A review of basic modern algebraic geometry (varieties, curves and their morphisms, divisors and differentials, the Riemann-Roch theorem).
3. The foundational theory of elliptic curves, this time from the perspective of modern algebraic geometry.
4. Elliptic curves over finite fields, particularly the Hasse-Weil bound.
5. Elliptic curves over local fields, culminating in the Néron-Ogg-Shafarevich criterion.
6. The Mordell-Weil theorem, which includes Galois cohomology and the theory of heights of points.
7. Computing the weak Mordell-Weil group of an elliptic curve via descent.

Acknowledgments

I would like to thank Jennifer Courts, Hugh Dennin, Ted Fu, Jake Huryn, Will Newman, Santak Panda, Natalie Patten, Aden Shaw, Wo Wu, Yifei Zhang and Shifan Zhao for comments that helped improve the accuracy and quality of these notes.

0. Elliptic Curves: A Planar Approach

0.1. **Introduction.** In this section, we will define and describe elliptic curves without couching them too much in the language of modern algebraic geometry. This allows us to get intuition about elliptic curves before working with them on a more abstract level. This approach is "coordinate-based," and we will always have equations for elliptic curves in mind.

Here is our first definition of an elliptic curve:

Definition 0.1.1. Given a field k, an **elliptic curve over k,** denoted $E_{/k}$, is a non-singular projective cubic plane curve with a fixed k-rational point.

Remark 0.1.1. For intuition, we can take $k = \mathbb{R}$; this lets us draw elliptic curves in the real plane. For example, here are some graphs of elliptic curves:

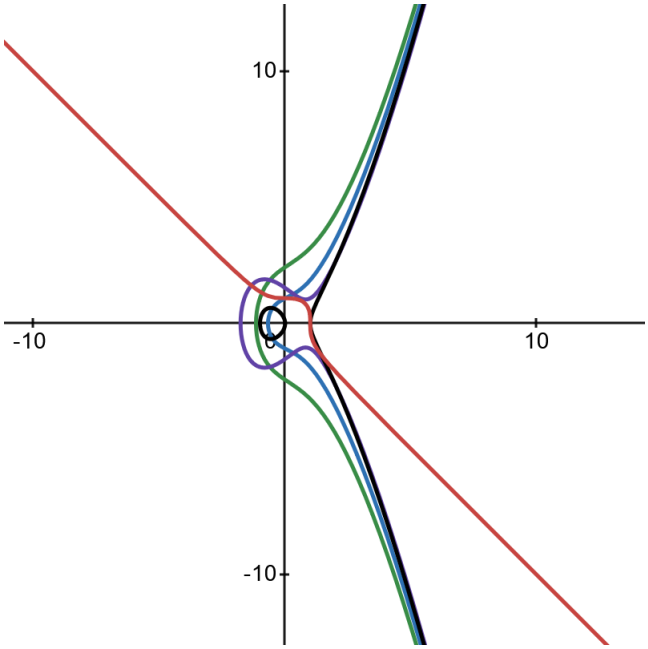


Figure 0.1.1. A variety of elliptic curves in $\mathbb{R}^2$.

For the rest of this chapter, we will review the geometric terms necessary for our first definition of an elliptic curve. We will revisit them in the following chapter, in a more general context.

0.2. **The affine plane.** For the rest of this chapter, k will denote a *perfect field.*[1] Once and for all, fix an algebraic closure $\overline{k}$ of k (sometimes, this will also denote an algebraically closed field containing k).

Recall that the *affine plane over* k is $\mathbb{A}^2(k) := k^2$. For example, the real affine plane is $\mathbb{R}^2$. We will write $\mathbb{A}^2 := \mathbb{A}^2(\overline{k})$.

Here we have our first definition of a curve.

[1]Recall that a **perfect field** k a field for which every algebraic extension of k is separable.

Definition 0.2.1. Given a polynomial $f(x, y) \in k[x, y]$, the **algebraic set** defined by f, written as C_f, is the set of solutions in $\mathbb{A}^2$ to f. Equivalently,

$$C_f = \{(x, y) \in \mathbb{A}^2 : f(x, y) = 0\}.$$

We will sometimes write

$$C : f(x, y) = 0$$

where $C := C_f$. When the ideal $(f) \subseteq \overline{k}[x, y]$ is prime, we say that C is an **algebraic curve.** In both cases, since f is defined over k, we say that C is **defined over k,** and write $C_{/k}$.

We will talk more about the primality assumption in Chapter 1, in the context of varieties; it is connected to *irreducibility* of the algebraic set with regards to the Zariski topology. For now, we content ourselves with the following *notes exercise,* showing that algebraic sets which aren't curves are the union of two smaller curves.

(In these notes, we have so-called "notes exercises" which are meant to be small exercises you attempt on your own when reviewing these notes. These are different from the standard exercises, which are more like homework exercises and can vary in difficulty.)

Notes Exercise 0.2.1. Let $C := C_f \subseteq \mathbb{A}^2$ be an affine curve defined by

$$f(x, y) = 0$$

where $f \in k[x, y]$. Show that if $f = g \cdot h$ in $\overline{k}[x, y]$, then we have

$$C = C_g \cup C_h.$$

Definition 0.2.2. Given an algebraic set $C_{/k}$ and an extension ℓ/k, we say that a point $P = (x, y) \in C$ is **ℓ-rational** if its coordinates $x, y \in \ell$.

0.3. **The projective plane.** While we often think of curves as living in $\mathbb{A}^2$, the *projective plane* lets us spot "invisible points" on curves – which is important for understanding the group law on an elliptic curve.

Definition 0.3.1. Let us define the **projective plane over** k as the quotient space

$$\mathbb{P}^2(k) := (k^3 \smallsetminus \{(0, 0, 0)\})/\sim,$$

where we say points $(a, b, c), (d, e, f) \in k^3$ are equivalent if there exists $\lambda \in k^\times$ with

$$(d, e, f) = (\lambda a, \lambda b, \lambda c).$$

We write $[a : b : c] \in \mathbb{P}^2(k)$ for the equivalence class of (a, b, c). We will write $\mathbb{P}^2 := \mathbb{P}^2(\overline{k})$.

Notes Exercise 0.3.1. Show that two nonzero points $P, Q \in k^3$ are equivalent in $\mathbb{P}^2(k)$ iff P and Q lie on the same line through the origin. Thus $\mathbb{P}^2(k)$ can be interpreted as "lines in k^3 through the origin."

Definition 0.3.2. we can embed $\mathbb{A}^2(k)$ into $\mathbb{P}^2(k)$ via

$$(a, b) \mapsto [a : b : 1].$$

Projective points in $\mathbb{P}^2(k) \smallsetminus \mathbb{A}^2(k)$ are called **points at infinity.** Necessarily, such points have the form $[a : b : 0]$.

For example, the curve $y = x^2$ has the point at infinity $[0 : 1 : 0]$ (see the following figure).

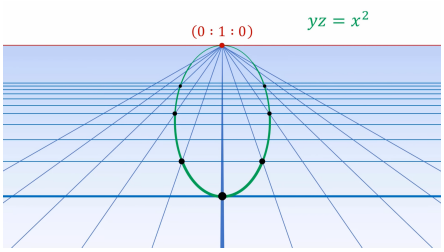


FIGURE 0.3.1. The parabola $y = x^2$ in $\mathbb{P}^2(\mathbb{R})$. Picture from here.

The usual intuition for the projective plane is to imagine that in $\mathbb{P}^2(k)$, "all parallel lines in $\mathbb{A}^2(k)$ converge at a point." Thus, two plane curves in $\mathbb{A}^2(k)$ which go off in different directions can *intersect* at previously unknown points at infinity.

Remark 0.3.1. In case you'd like to build intuition on the projective plane (which is where you "see" the canonical identity element for an elliptic curve, namely the point at infinity), here's a really nice video on it, titled "Putting Algebraic Curves in Perspective": `https://www.youtube.com/watch?v=XXzhqStLG-4`

The definition of a *projective curve* requires slightly more care than that of an affine curve. This brings us to *homogeneity.*

Definition 0.3.3. A polynomial $G(X, Y, Z) \in k[X, Y, Z]$ is called **homogeneous** if every monomial in G has the same degree: i.e., there exists $d \in \mathbb{Z}_{\geq 0}$ such that we can write

$$G(X, Y, Z) = \sum_{a+b+c=d} \alpha_{a,b,c} \cdot X^a Y^b Z^c,$$

i.e., all terms in $G(X, Y, Z)$ have equal total degree. Then the **projective algebraic set (over k)** defined by G, denoted $C := C_G$, is the set of solutions in $\mathbb{P}^2$ to $G(X, Y, Z)$. We will write this as

$$C : G(X, Y, Z) = 0.$$

When the ideal $(G) \subseteq \overline{k}[X, Y, Z]$ is prime, we say that C is a **projective curve (over k).**

Example 0.3.1. As a quick example, the polynomial $F(X, Y, Z) := Y^2Z - X^3 - XZ^2 \in \mathbb{Q}[X, Y, Z]$ defines a projective curve

$$C_{/\mathbb{Q}} : Y^2Z = X^3 + XZ^2.$$

However, the polynomial $G(X, Y, Z) := X^3 + Y^2 + Z \in \mathbb{Q}[X, Y, Z]$ does not, since it is not homogeneous.

The definition of a rational point in the projective plane is slightly subtle:

Definition 0.3.4. Say that a point $[a : b : c] \in \mathbb{P}^2$ is **k-rational** if we can write $[a : b : c] = [d : e : f]$ with $d, e, f \in k$, equivalently, if there exists $\lambda \in \overline{k}^\times$ with $\lambda a, \lambda b, \lambda c \in k$. Then given a projective curve $C_{/k} \subseteq \mathbb{P}^2$, we let $C(k)$ denote its set of k-rational points.

Example 0.3.2. We observe that $[1 : 0 : 0] \in \mathbb{P}^2(\overline{\mathbb{Q}})$ is $\mathbb{Q}$-rational ($\lambda := 1$). However, the point $[\pi : 2\pi : 3\pi] \in \mathbb{P}^2(\overline{\mathbb{Q}})$ is also $\mathbb{Q}$-rational, since

$$[\pi : 2\pi : 3\pi] = [1 : 2 : 3].$$

Just remember that you can (nonzero) scale points in $\mathbb{P}^2$!

Here is an important notes exercise on the construction of the zero set of a projective curve being well-defined:

Notes Exercise 0.3.2. Check that for a homogeneous polynomial $G \in K[X, Y, Z]$, for any point $[a : b : c] \in \mathbb{P}^2(k)$ one has

$$G(a, b, c) = 0$$

iff for all $\lambda \in \overline{k}^\times$,

$$G(\lambda a, \lambda b, \lambda c) = 0.$$

Thus, the solution set $C_G(k)$ in $\mathbb{P}^2$ makes sense.

We previously noted that $\mathbb{A}^2(k) \subseteq \mathbb{P}^2(k)$. As it turns out, we can also realize affine curves $C \subseteq \mathbb{A}^2$ as living in $\mathbb{P}^2$.

Definition 0.3.5. Given a degree d polynomial $f(x, y) \in k[x, y]$, the **homogenization of f,** denoted by $F(X, Y, Z) \in k[X, Y, Z]$, is defined as

$$F(X, Y, Z) := f\left(\frac{X}{Z}, \frac{Y}{Z}\right) \cdot Z^d.$$

Practically speaking: you can homogenize $f(x, y)$ by multiplying each monomial in f by the new variable Z until the monomial's degree is equal to d.

Conversely, given a homogeneous polynomial $G(X, Y, Z) \in k[X, Y, Z]$, you can **dehomogenize** G into a polynomial $g(x, y) \in k[x, y]$ by setting $g(x, y) := G(x, y, 1)$.

Example 0.3.3. The polynomial $f(x, y) := x^2 + y^2 - 1 \in \mathbb{R}[x, y]$ has as its curve C the unit circle at the origin; one has that its homogenization is $F(X, Y, Z) = X^2 + Y^2 - Z^2$. On the other hand, for $G(X, Y, Z) := Y^2Z - X^3 + 3XZ^2 - Z^3 \in \mathbb{Q}[X, Y, Z]$, we have that its dehomogenization is $g(x, y) = y^2 - x^3 + 3x - 1$ (an elliptic curve equation over $\mathbb{Q}$).

The upshot to homogenization/dehomogenization is that we can pass curves between $\mathbb{A}^2$ and $\mathbb{P}^2$.

Definition 0.3.6. Given an affine curve $C \subseteq \mathbb{A}^2$ defined by $f(x, y) \in k[x, y]$, we have that its **projective closure** C_H is the projective curve defined by

$$C_H : F(X, Y, Z) = 0$$

where $F(X,Y,Z) \in k[X,Y,Z]$ is the homogenization of f. Similarly, given a projective curve $C \subseteq \mathbb{P}^2$ defined by $G(X,Y,Z) \in k[X,Y,Z]$, we can **affinize** C by dehomogenizing G, to get an affine curve

$$C_h : g(x,y) = 0$$

where $g(x,y) := G(x,y,1)$.

Remark 0.3.2. Something we have taken for granted above is that the projective closure of a curve is still a curve, i.e., irreducibility is preserved. This is proven in Exercise 1.2.1.

Notes Exercise 0.3.3. Verify that for an affine curve $C \subseteq \mathbb{A}^2$, one has $(C_H)_h = C$.

Notes Exercise 0.3.4. Double-check that for an affine curve $C \subseteq \mathbb{A}^2$, one has an embedding

$$C \hookrightarrow C_H.$$

Example 0.3.4. It will often be the case that elliptic curves $E_{/k}$ are given in a "short Weierstrass form"

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

where $A, B \in k$. We can homogenize E to produce

$$E_H : Y^2Z = X^3 + AXZ^2 + BZ^3.$$

There exists exactly one point in $E_H(k) \smallsetminus E(k)$: necessarily, it is a point at infinity, so it has the form $[a : b : 0]$ by Definition 0.3.2. One can plug $Z = 0$ into the equation for E_H and find that $[a : b : 0] = [0 : 1 : 0]$, and this is the *only* point at infinity on E_H. It is a k-rational point, and is the usual choice for the identity element of the group law on $E(k)$.

0.4. **Singular points.**

Definition 0.4.1. Given an affine curve $C_{/k} \subseteq \mathbb{A}^2$ defined by

$$C : f(x,y) = 0,$$

a point $P \in C$ is a **singular point on** C if the two partials of f evaluated at P are zero:

$$\left.\frac{\partial f}{\partial x}\right|_P = \left.\frac{\partial f}{\partial y}\right|_P = 0.$$

Similarly, for a projective curve $C_{/k} \subseteq \mathbb{P}^2$ defined by

$$C : F(X,Y,Z) = 0,$$

a point $P \in C$ is a **singular point on** C if

$$\left.\frac{\partial F}{\partial X}\right|_P = \left.\frac{\partial F}{\partial Y}\right|_P = \left.\frac{\partial F}{\partial Z}\right|_P = 0.$$

In either case, when C has a singular point, we say that C is **singular;** otherwise, we say it is **nonsingular** (or **smooth**).

Example 0.4.1. The curve $C_{/\mathbb{R}} \subseteq \mathbb{P}^2(\mathbb{C})$ defined by

$$F(X,Y,Z) := X^3 + X^2Z + X^2Y - Z^3$$

has a singular point: we check that

$$\frac{\partial F}{\partial X} = 3X^2 + 2XZ + 2XY,$$

$$\frac{\partial F}{\partial Y} = X^2$$

and

$$\frac{\partial F}{\partial Z} = X^2 - 3Z^2.$$

Setting these equal to zero and solving for X, Y and Z shows that C has the singular point $[0:1:0] \in C(\mathbb{R})$, and it is the *only* singular point. (The *singular* singular point?)

Other examples of singular points include the *node* and *cusp* seen below (corresponding to $y^2 = x^3 + x^2$ and $y^2 = x^3$, respectively).

Notes Exercise 0.4.1. Given an affine curve $C_{/k} \subseteq \mathbb{A}^2$, show that a point $(a,b) \in C(k)$ is singular iff $[a:b:1] \in C_H(k)$ is singular. Thus, checking for affine singular points can be done separately from checking for singular points at infinity.

As it turns out, associated to a cubic curve of the form

$$E_{/k} : y^2 = x^3 + Ax + B$$

is an invariant called the *discriminant of E,* defined as $\Delta_E := -16(4A^3 + 27B^2)$. One has that E is an elliptic curve iff E is nonsingular, **iff** $\Delta_E \neq 0$. Exercises 0.4.1 and 0.4.2 explore this invariant.

Notes Exercise 0.4.2. Show that if the *characteristic*[2] of k is $\mathrm{char}(k) = 2$, then the cubic curve

$$C : y^2 = x^3 + Ax + B$$

is always singular.

Exercise 0.4.1. This exercise determines when certain plane curves are nonsingular. Let F be a field of characteristic zero.

a) Show that for a polynomial $f(x) \in F[x]$ and for an integer $n \in \mathbb{Z}^+$, the curve

$$C_{/F} : y^n = f(x)$$

in $\mathbb{A}^2$ has a singular point if and only if $f(x)$ has a *repeated root* in $\overline{F}$, i.e., there exists $x_0 \in \overline{F}$ with $f(x_0) = 0$ and $f'(x_0) = 0$.

[2]Recall that for a field k, there exists a homomorphism $\mathbb{Z} \to k$ via $1 \mapsto 1_k$. Since the kernel is a prime ideal of $\mathbb{Z}$, it is either generated by zero or a prime number. The **characterstic** of k is the non-negative generator of the kernel; it is denoted by $\mathrm{char}(k)$.

b) Given a curve

$$C : y^2 = (x-\alpha)(x-\beta)(x-\gamma)$$

where $\alpha, \beta, \gamma \in \overline{F}$, the *discriminant* of C is

$$\Delta_C := [(\alpha-\beta)(\alpha-\gamma)(\beta-\gamma)]^2.$$

Prove that $\Delta_C = 0$ if and only if C is singular.

In particular, when a cubic polynomial $f(x) \in F[x]$ has no repeated roots, the cubic curve defined by $y^2 = f(x)$ is nonsingular, and in fact is an elliptic curve over F.

Exercise 0.4.2. **Prerequisite: algebraic number theory.**

This exercise extends Exercise 0.4.1, by giving a formula for the discriminant of the polynomial x^3+Ax+B associated to the cubic curve $y^2 = x^3+Ax+B$. For a reference, see pp. 37-38 [MilANT].

Let F be a field of characteristic zero, and K/F an extension of degree n. Then by the primitive element theorem, we can write $K = F(\alpha)$ for some $\alpha \in \overline{F}$. Let $m_\alpha(x)$ be its minimal polynomial; suppose its roots are $\alpha_1 := \alpha, \alpha_2, \ldots, \alpha_n$. Then we have a formula for the discriminant of K/F:

$$\begin{aligned}\Delta_{K/F} &= \Delta(\alpha_1, \ldots, \alpha_n) \\ &= \prod_{1 \le i < j \le n} (\alpha_i - \alpha_j)^2 \\ &= (-1)^{\frac{n(n-1)}{2}} \cdot \mathrm{Nm}_{K/F}(m'_\alpha(\alpha)).\end{aligned}$$

In general, for a polynomial $f \in F[x]$ of degree $n \ge 1$ whose roots in $\overline{F}$ are $\alpha := \alpha_1, \ldots, \alpha_n$, the *discriminant of* f is

$$\Delta(f) := \prod_{1 \le i < j \le n} (\alpha_i - \alpha_j)^2 = (-1)^{\frac{n(n-1)}{2}} \cdot \mathrm{Nm}_{K/F}(f'_\alpha(\alpha)).$$

a. Show that for $n \ge 1$, the discriminant of

$$f(x) := x^n + Ax + B \in F[x]$$

is

$$\Delta(f) = (-1)^{\frac{n(n-1)}{2}}(n^n B^{n-1} + (-1)^{n-1}(n-1)^{n-1}A^n).$$

b. Use part a. and Exercise 0.4.1 to show that a cubic curve

$$E_{/F} : y^2 = x^3 + Ax + B \tag{1}$$

has for its associated polynomial $x^3 + Ax + B$ the discriminant

$$\Delta = -(4A^3 + 27B^2).$$

Remark: This discriminant differs from the usual short Weierstrass form discriminant $\Delta_E := -16(4A^3 + 27B^2)$. The factor of 16 in the latter formula is a useful way to emphasize that over a field of characteristic 2, the curve defined by (1) does *not* define an elliptic curve.

To reiterate, in this chapter we are interested in studying k-rational points on *nonsingular projective cubic plane curves over k.* When such a curve has a k-rational point, we say it is an **elliptic curve over k.**

Remark 0.4.1. This is an important remark: while we have emphasized elliptic curves as being *projective* curves, we will often write them down as *affine* curves $E_{/k}$ in $\mathbb{A}^2$, defined by equations $f(x, y) \in k[x, y]$. This is simply a matter of convention – by Notes Exercise 0.3.4, we know that E embeds into its projective closure E_H. It is the case that E_H has only one more point than E, so the difference between E_H and E is virtually negligible.

0.5. **The definition of an elliptic curve.** Let us recall what an elliptic curve is. For most of these notes, we will focus on projective curves since they are more "complete" than affine curves (in a literal sense).

Definition 0.5.1. Given a field k, an **elliptic curve over k,** denoted $E_{/k}$, is a nonsingular projective plane cubic curve with a fixed k-rational point. Its affinization is given by a cubic equation

$$E : f(x, y) = 0$$

where $f \in k[x, y]$.

In the following exercise, we will see why *irreducible* is not mentioned in the definition of a projective elliptic curve.

Exercise 0.5.1. **Prerequisite: algebraic geometry.**
One has in the usual definition of an *affine* elliptic curve that it must be *irreducible,* i.e., it cannot be the union of two nontrivial plane curves. However, this is superfluous for *projective nonsingular* curves: show that for a nonsingular projective plane curve $C_{/k}$, one has that C is irreducible over $\overline{k}$. (Compare this to Exercise 1.2.1.)

It is often the case that an elliptic curve $E_{/k}$ will be given in a *Weierstrass form:*

- **Short Weierstrass form** is

$$E : y^2 = x^3 + Ax + B,$$

  where $A, B \in k$. This equation can only be nonsingular when $\mathrm{char}(k) \neq 2$.
- **General Weierstrass form** is

$$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6,$$

  with $a_1, a_2, a_3, a_4, a_6 \in k$. This equation can be nonsingular in any characteristic.

Short Weierstrass form is very common, but often times, working with a general Weierstrass form allows us to work with smaller coefficients.

Notes Exercise 0.5.1. Check that an elliptic curve in general Weierstrass form has a single point at infinity, which is $O := [0 : 1 : 0]$.

0.6. **An illustrative example.** In this subsection, we will use the "chord and tangent method" on a specific elliptic curve $E_{/\mathbb{Q}}$ to give an example of the general group law. First, we will use the *chord method* on two rational points $P_1, P_2 \in E(\mathbb{Q})$ to produce a third rational point on E, denoted $R := P_1 * P_2$. We will also use the tangent method on P_1 to produce another rational point on E from it, denoted $S := P_1 * P_1$. The group law for a general planar elliptic curve is this chord and tangent method applied twice, the second time taking the chord/tangent between R or S and the point at infinity $O := [0 : 1 : 0]$.

Example 0.6.1. We will consider the cubic curve $E_{/\mathbb{Q}} : y^2 = x^3 - 7x + 10$. By Exercise 0.4.2, its discriminant is $\Delta_E = -21248 \neq 0$. In particular, the curve E is nonsingular, and is thus an elliptic curve.

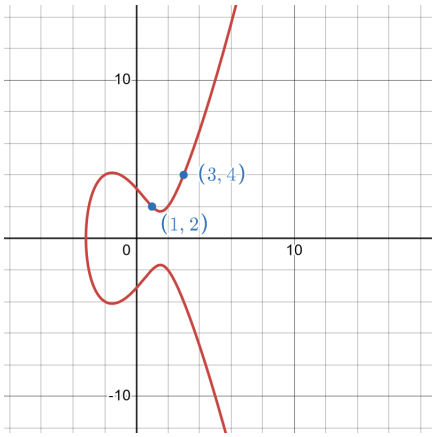


FIGURE 0.6.1. The elliptic curve $E : y^2 = x^3 - 7x + 10$.

Adding two points. We can check that both $P_1 := (1, 2)$ and $P_2 := (3, 4)$ are points in $E(\mathbb{Q})$. Their sum, written $P_1 \oplus P_2$, is determined by a "chord and tangent method" applied twice.

1. *Step 1:* let $L_1 := L_{P_1,P_2}$ be the line through P_1 and P_2. Then its slope is $m = \frac{4-2}{3-1} = 1$, and thus it has the equation
$$L_1 : y - y_1 = m(x - x_1),$$
i.e.,
$$L_1 : y = x + 1.$$
Let's analyze the intersection $L_1 \cap E$. To do this, we'll plug $y = x + 1$ into our equation for E:
$$\begin{aligned} y^2 = x^3 - 7x + 10 &\Rightarrow (x+1)^2 = x^3 - 7x + 10 \\ &\Rightarrow x^3 - x^2 - 9x + 9 = 0 \\ &\Rightarrow x^2(x-1) - 9(x-1) = 0 \\ &\Rightarrow (x^2 - 9)(x-1) = 0 \\ &\Rightarrow (x+3)(x-3)(x-1) = 0. \end{aligned}$$

Thus, there are 3 points in $L_1 \cap E$, each with x-coordinates $x = 1, 3$ and -3, respectively. We know $x = 1$ and $x = 3$ have to be roots of this polynomial, since $P_1, P_2 \in L_1 \cap E$. Thus, let us set $x_3 := -3$. Plugging x_3 into the line L_1 and solving for y, we get $y_3 := x_3 + 1 = -2$. We conclude via the chord method that $R := P_1 * P_2 = (-3, -2)$ is on E and is collinear to P_1 and P_2.

2. *Step 2:* for a second application of the chord method, let us consider the line through R and the point at infinity $O := [0 : 1 : 0]$. Write it as

$$L_2 := L_{R,O} := ax + by = c.$$

Homogenizing it gives

$$L_{2,H} : aX + bY = cZ,$$

a projective line in $\mathbb{P}^2$. Since $O \in L_2$, we have $a \cdot 0 + b \cdot 1 = c \cdot 0$, so that $b = 0$. Thus L_2 has the form

$$L_2 : ax = c$$

which is a *vertical* line. Since $R \in L$, we have $a \cdot -3 = c$. Thus,

$$L_2 : ax = -3a;$$

we can divide by a (why is $a \neq 0$?) and get a new equation for the same line:

$$L_2 : x = -3.$$

Let us analyze $L_2 \cap E$. Plug $x = -3$ into E and get an equation for y:

$$y^2 = (-3)^3 - 7 \cdot (-3) + 10 = 4.$$

Thus, two points on $L_2 \cap E$ are $(-3, \pm 2)$. (Only two affine points appear in $L_2 \cap E$ since the third point is the point at infinity – this is also why we had to solve a *quadratic* equation in y.) Thus, we have constructed a new rational point on E, namely $(-3, 2)$. In fact, this is our "sum" of P_1 and P_2, and we will write it as $P_1 \oplus P_2 := (-3, 2)$.

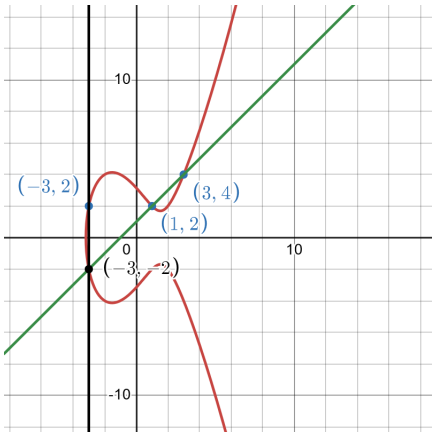


FIGURE 0.6.2. The elliptic curve $E : y^2 = x^3 - 7x + 10$. The initial chord L_1 is green, and the vertical line L_2 is black.

Adding a point to itself. Let's find out how to add $P_1 := (1, 2)$ to itself; this sum is written as $P_1 \oplus P_1$, or simply $2P_1$. We will use the tangent method in the first step.

1. *Step 1:* let L_3 be the *tangent* line through P_1:

$$L_3 : y = m_0(x - 1) + 2$$

where m_0 is the tangent slope of E at P_1. We can compute it with implicit differentiation:

$$\frac{d}{dx}[y^2 = x^3 - 7x + 10] \Rightarrow \frac{dy}{dx} = \frac{3x^2 - 7}{2y},$$

and so

$$m_0 = \left.\frac{dy}{dx}\right|_{(1,2)} = \frac{-4}{4} = -1.$$

Thus,

$$L_3 : y = 3 - x.$$

To analyze $L_3 \cap E$, plug $y = 3 - x$ into $y^2 = x^3 - 7x + 10$ and solve for x:

$$\begin{aligned} y^2 = x^3 - 7x + 10 &\Rightarrow (3 - x)^2 = x^3 - 7x + 10 \\ &\Rightarrow x^3 - x^2 - x + 1 = 0 \\ &\Rightarrow x^2(x - 1) - (x - 1) = 0 \\ &\Rightarrow (x^2 - 1)(x - 1) = 0 \\ &\Rightarrow (x - 1)^2(x + 1) = 0. \end{aligned}$$

As expected, the value $x = 1$ is a root *twice* since $(1, 2)$ has multiplicity two on the tangent line L_3 to E at $(1, 2)$. Thus, we can take $x_3 := -1$ and $y_3 := 3 - x_3 = 4$, and deduce that

$$R := P_1 * P_1 := (-1, 4) \in E(\mathbb{Q}).$$

2. *Step 2:* take the line $L_4 := L_{4,R,O}$ through R and O. As observed before, it should be the vertical line through R. We can check that

$$L_4 : x = -1.$$

Thus, the third point of $L_4 \cap E$ is immediately $(-1, -4)$: to see this, simply note that $y = 4$ must be a root of the quadratic equation $y^2 = (-1)^3 - 7(-1) + 10$, and so the other root must be the negation of $y = 4$. We conclude that the sum of P_1 with itself is $(-1, -4)$, i.e., $2P_1 = (-1, -4)$; by our construction, this point lies on E.

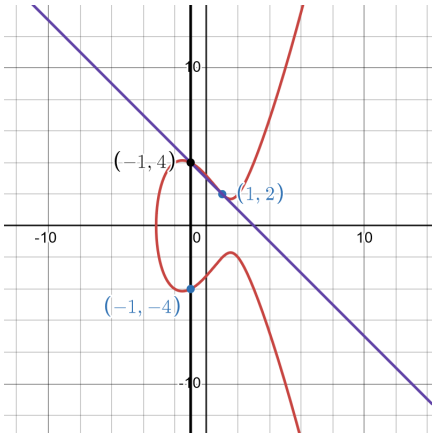


FIGURE 0.6.3. The elliptic curve $E : y^2 = x^3 - 7x + 10$. The initial tangent L_3 is purple, and the vertical line L_4 is black.

0.7. **The group law on an elliptic curve.** Let us describe the general group law on a planar elliptic curve $E_{/k}$. After this, we will see how it simplifies for elliptic curves in short Weierstrass form.

1. **The group law:**
   - i) Fix a k-rational point $O \in E(k)$. Then given two rational points $P_1, P_2 \in E(k)$, define their **sum** $P_1 \oplus P_2$ as follows:
   - ii) First, take the line L_{P_1,P_2} through P_1 and P_2; if $P_1 = P_2$, then take the tangent line to E at P_1 instead. It will intersect the curve at a **k-rational** third point (maybe even at P_1 or P_2). Call this third point $P_1 * P_2$.
   - iii) Then take the line $L_{P_1*P_2,O}$ through $P_1 * P_2$ and O; it will intersect the curve at a **k-rational** third point (maybe even at $P_1 * P_2$ or O). This third point is our sum $P_1 \oplus P_2$.

When E is given in *Weierstrass form,* this group law simplifies. For now, we highlight the case of short Weierstrass form.

2. **The group law, short Weierstrass form:** given an elliptic curve

$$E : y^2 = x^3 + Ax + B$$

with $A, B \in k$:

   - i) There exists a unique point at infinity $[0 : 1 : 0] \in E(k)$. Fixing $O := [0 : 1 : 0]$: given two rational points $P_1, P_2 \in E(k)$, define their sum $P_1 \oplus P_2$ as follows:
   - ii) Take the line L_{P_1,P_2} through P_1 and P_2; if $P_1 = P_2$, take the tangent line to E at P_1 instead. Let the third point of intersection between L_{P_1,P_2} and E be written as $P_1 * P_2$.
   - iii) If $P_1 * P_2$ is affine, then writing $P_1 * P_2 := (x, y)$ one has $P_1 \oplus P_2 = (x, -y)$. Otherwise $P_1 * P_2 = O$, and thus $P_1 \oplus P_2 = O$, due to the fact that O is a *flex point.*

Thus, the second chord/tangent step simplifies in the case of short Weierstrass form, and there is a natural choice of identity element O. In fact, there are formulas for

the first step of the chord and tangent method when working with general or short Weierstrass form: see Exercises 0.7.1 and 0.7.2, respectively.

Remark 0.7.1. Recall that for a curve $C_{/k}$, a point $P \in C$ is a **flex point** if the tangent line L to C at P has *intersection multiplicity* ≥ 3. If C is a nonsingular cubic curve, then this is equivalent to having $L \cap C = \{P\}$. If further C is a nonsingular affine curve over $\mathbb{R}$, then $P \in C(\mathbb{R})$ is a flex point iff the concavity on C changes at P – just like in Calculus 1!

Exercise 0.7.1. Let $E_{/k}$ be an elliptic curve in general Weierstrass form

$$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$

where $a_1, a_2, a_3, a_4, a_6 \in k$. (Note that this includes short Weierstrass form as a special case.)

a. Show that for two points $P_1 := (x_1, y_1), P_2 := (x_2, y_2) \in E(k)$ which are not collinear to $O := [0 : 1 : 0]$, one has the formula

$$P_1 * P_2 = (x_3, y_3) := (m^2 + a_1m - a_2 - x_1 - x_2, mx_3 + b)$$

where $L : y = mx + b$ is the line through P_1 and P_2.

b. Use part a. to further show that

$$P_1 \oplus P_2 = (x_3, -(m + a_1)x_3 - b - a_3).$$

c. In contrast to part a., show that if P_1, P_2 and O are collinear, then

$$P_1 \oplus P_2 = O.$$

d. Prove that for a point $P = (x, y) \in E(k)$, one has

$$-P = (x, -y - a_1x - a_3).$$

Exercise 0.7.2. This exercise proves some formulas for elliptic curves in short Weierstrass form,

$$E_{/k} : y^2 = x^3 + Ax + B.$$

a. Using Exercise 0.7.1, show that for two points $P_1 := (x_1, y_1), P_2 := (x_2, y_2) \in E(k)$ which are not collinear to $O := [0 : 1 : 0]$, one has the formula

$$P_1 \oplus P_2 = (m^2 - x_1 - x_2, -m(m^2 - x_1 - x_2) - b)$$

where $L : y = mx + b$ is the line through P_1 and P_2.

b. Argue that if P_1, P_2 and O are collinear, then $P_2 = -P_1$.

c. Show that for any point $P := (a, b) \in E(k)$, one has the additive inverse

$$-P = (a, -b).$$

The following fact is useful to keep in mind:

Notes Exercise 0.7.1. Prove that the point at infinity $[0 : 1 : 0] \in \mathbb{P}^2$ lies on the projective closure of any vertical line in $\mathbb{A}^2$.

Here is a short list of facts that are useful to keep in mind when computing sums of points on an elliptic curve E for the first time.

1. The tangent line L to E at a point $P \in E$ "contains P twice" (i.e., P has multiplicity two on L).
2. Elliptic curves in short Weierstrass form
$$E : y^2 = x^3 + Ax + B :$$
   - Have exactly one point at infinity, namely $O := [0 : 1 : 0]$;
   - Have that O is a flex point;
   - Have that O lies on every vertical line in $\mathbb{A}^2$.

Now we will sketch a proof that the group law described above indeed defines a group law on the set of rational points on an elliptic curve. To simplify matters, we will assume our fixed rational point O is a flex point. For example, when E is in general Weierstrass form, one has that $O := [0 : 1 : 0] \in E(k)$ is automatically flex. (Another upshot for working with flex points is that there exists a "Collinearity Theorem" for group laws with a flex identity, see Theorem 0.7.4.)

Theorem 0.7.1 (Elliptic curve group law)**.** *Given an elliptic curve $E_{/k}$ with a fixed point $O \in E(k)$, the chord and tangent method described above makes $E(k)$ an abelian group. (We will sometimes write the group as $(E(k), O)$ to emphasize the fixed point.)*

Proof. For simplicity, let us assume that O is a flex point; the general case is left as Exercise 0.7.7. We need to check that $E(k)$ satisfies the definition of an abelian group, which is:

1. $E(k)$ is **closed** under $\oplus$, i.e., $\oplus$ takes $E(k)$ to itself.
2. The binary operation $\oplus$ is **abelian**: $\forall P_1, P_2 \in E(k)$, one has $P_1 \oplus P_2 = P_2 \oplus P_1$.
3. $E(k)$ has an **identity element,** namely the fixed point $O \in E(k)$.
4. $E(k)$ has additive **inverses:** for $P \in E(k)$, there exists $Q \in E(k)$ with
$$P \oplus Q = O$$
(we will write $-P := Q$).
5. The binary operation $\oplus$ is **associative:** $\forall P_1, P_2, P_3 \in E(k)$, one has
$$(P_1 \oplus P_2) \oplus P_3 = P_1 \oplus (P_2 \oplus P_3).$$

Let's prove these:

1. Since P_1 and P_2 are k-rational, so is the third point $P_1 * P_2$ on $L_{P_1,P_2} \cap E$; and since O is also k-rational, so is the third point on $L_{O,R} \cap E$, which by definition is $P_1 \oplus P_2$.
2. For $P_1, P_2 \in E(k)$, the line through P_1 and P_2 is the same as the line through P_2 and P_1, so the first step of the chord and tangent method implies that $P_1 \oplus P_2 = P_2 \oplus P_1$.
3. Given any $P \in E(k)$, we must show that
$$P \oplus O = P.$$
Consider the line $L_{P,O}$; it goes through E at a third point $P * O \in E(k)$. Then consider the line $L_{P*O,O}$: this is the same line as $L_{P,O}$, since the three points P, O and $P * O$ are collinear (any two points determine a line). Thus, the third point on $L_{P*O,O} \cap E$ is P, whence we have $P \oplus O = P$.

4. Given $P \in E(k)$, we want to find $Q \in E(k)$ such that the line through $P * Q$ and O has third point O. Let's try $Q := P * O$, i.e., take our potential inverse of P to be the third point $P * O$ on $L_{P,O}$. We claim that $P \oplus (P * O) = O$:
   i) The first line in the chord and tangent method is $L_{P,P*O}$, which intersects E at the third point O, by definition of $P * O$. Thus $P * (P * O) = O$.
   ii) The second line is $L_{P*O,O} = L_{O,O}$, the tangent line to E at O; and since O is a *flex point,* the third point on $L_{O,O} \cap E$ is O.

   We deduce that $P \oplus (P * O) = O$, whence we conclude that $-P = P * O \in E(k)$.
5. It's sort of tedious to check associativity, so here's an example picture of it:

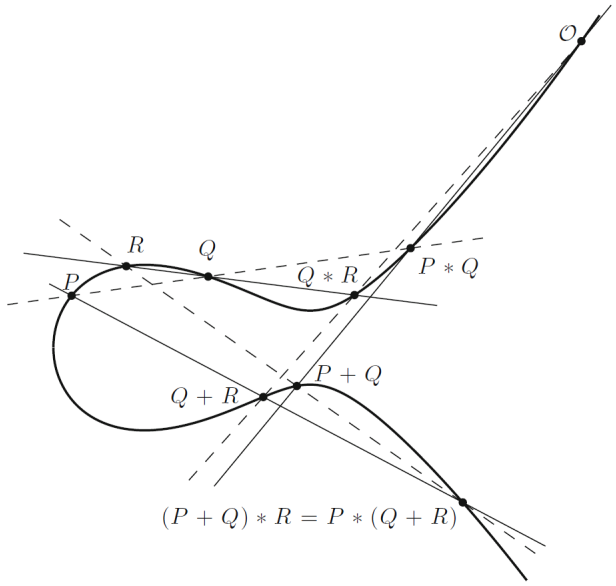


FIGURE 0.7.1. Example of associativity on an elliptic curve [ST15]. □

Remark 0.7.2. From here on out, given a point $P \in E(k)$ and integer $n \in \mathbb{Z}^+$, we will write $nP := \underbrace{P \oplus P \oplus \ldots \oplus P}_{n \text{ times}}$. Similarly, for $n < 0$ we set $nP := \underbrace{-P \oplus -P \oplus \ldots \oplus -P}_{n \text{ times}}$, and $0P := O$.

The group $E(k)$ is called the **Mordell-Weil group of E over k.** We will review its structure very closely in these notes. As it turns out, the **Mordell-Weil Theorem** shows that when $F := k$ is a *number field,* one has that $E(F)$ is a *finitely generated abelian group.* We will prove the Mordell-Weil Theorem later in these notes. For now, here is its statement:

Theorem 0.7.2 (The Mordell-Weil Theorem)**.** *Let $F \subseteq \mathbb{C}$ be a number field, i.e., suppose that $[F : \mathbb{Q}] < \infty$. Then for an elliptic curve $E_{/F}$, its Mordell-Weil group is a **finitely generated abelian group:** that is, there exist $P_1, P_2, \ldots, P_n \in E(F)$ such that for any $P \in E(F)$, one has*

$$P = a_1 P_1 \oplus a_2 P_2 \oplus \ldots \oplus a_n P_n$$

for some $a_1, a_2, \ldots, a_n \in \mathbb{Z}$.

Corollary 0.7.3. *For an elliptic curve* $E_{/F}$ *where* $[F : \mathbb{Q}] < \infty$*, one has*

$$E(F) \cong \mathbb{Z}^r \oplus E(F)[\text{tors}]$$

for some $r := r_{E,F} \geq 0$ *called the* ***rank of*** E ***over*** F*, and where* $E(F)[\text{tors}]$ *is the* ***torsion subgroup*** *of* E *over* F *(i.e., the subgroup of* F*-rational points with finite order).*

The rank and torsion subgroup of an elliptic curve are central objects of research in modern number theory. One goal of these notes is to learn about techniques to compute them.

Example 0.7.1. Consider the elliptic curve $E_{/\mathbb{Q}} : y^2 = x^3 + 5x$. We see that $(0, 0)$ lies on E; in fact, it is an order 2 point (see Exercise 0.7.6). As it turns out, we have $E(\mathbb{Q})[\text{tors}] = \{O, (0, 0)\}$, i.e., the only nontrivial element of the torsion subgroup of E over $\mathbb{Q}$ is $(0, 0)$. Additionally, this curve has rank $r = 1$ over $\mathbb{Q}$, with the point $(20, 90) \in E(\mathbb{Q})$ having infinite order. As a consequence of these two facts (which we take for granted right now), we can conclude that

$$E(\mathbb{Q}) = \langle (20, 90) \rangle \oplus \langle (0, 0) \rangle \cong \mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}.$$

Thus, any point $P \in E(\mathbb{Q})$ has the form

$$P = a(20, 90) \oplus b(0, 0)$$

for some unique $a \in \mathbb{Z}$ and $b \in \mathbb{F}_2$. For example, we have the point $P := \left(\frac{1}{4}, -\frac{9}{8}\right) \in E(\mathbb{Q})$, and we can write

$$P = (20, 90) - (0, 0).$$

See also Figure 0.7.2.

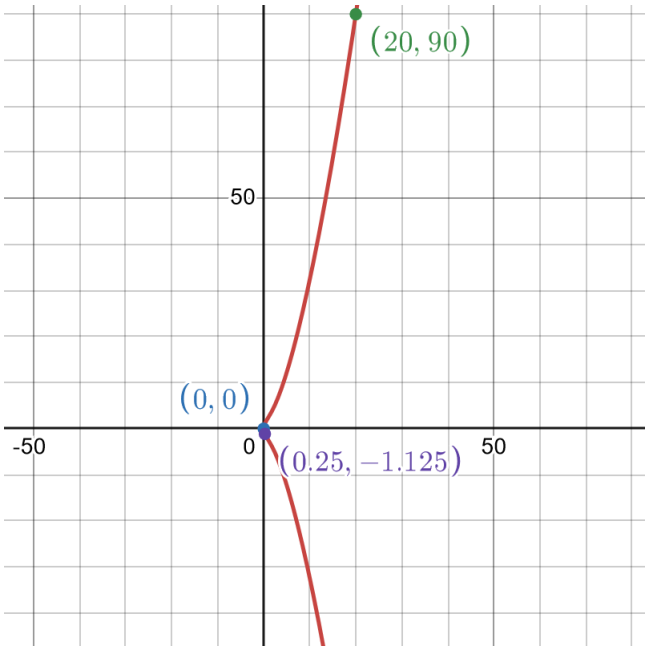


FIGURE 0.7.2. The elliptic curve $E : y^2 = x^3 + 5x$ in $\mathbb{R}^2$.

Example 0.7.2. Here's a pictorial example of a torsion point and its multiples on an elliptic curve:

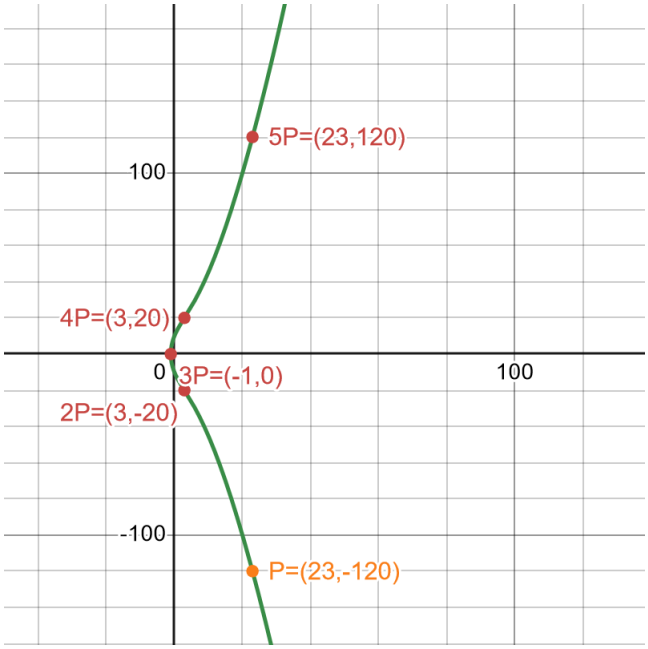


FIGURE 0.7.3. The elliptic curve $E : y^2 = x^3 + 93x + 94$, with NP for $P := (23, -120)$ and $1 \leq N \leq 5$.

Notes Exercise 0.7.2. Without doing any calculations, explain why the point $P := (23, -120)$ on $E : y^2 = x^3 + 93x + 94$ in Figure 0.7.3 is a torsion point, and determine its order.

To wrap this chapter up, let us prove a group-theoretic fact about the sum of three collinear points on an elliptic curve where the identity is flex.

Theorem 0.7.4 (Collinearity Theorem for Flex)**.** *Let $E_{/k}$ be an elliptic curve, and assume that the identity $O \in E(k)$ is a flex point. If $P_1, P_2, P_3 \in E(k)$ are collinear, then one has*

$$P_1 \oplus P_2 \oplus P_3 = O.$$

Proof. It is equivalent to show that

$$P_1 \oplus P_2 = -P_3.$$

Let us go through the chord and tangent method for computing $P_1 \oplus P_2$ and observe what happens.

1. The initial line through P_1 and P_2 passes through a third point on E, written as $P_1 * P_2$. However, the points P_1, P_2 and P_3 are on the same line by assumption, which forces $P_1 * P_2 = P_3$.
2. The second line in the chord and tangent method, which goes through $P_1 * P_2 = P_3$ and O, contains the point $P_1 \oplus P_2$ on E. **Thus P_3, O and $P_1 \oplus P_2$ are collinear.**

With the above in mind, we will show that $(P_1 \oplus P_2) \oplus P_3 = O$. Let us apply the chord and tangent method to $P_1 \oplus P_2$ and P_3:

1. The line through $P_1 \oplus P_2$ and P_3 intersects the curve at a third point $(P_1 \oplus P_2) * P_3$; by the observations above, we know this third point is $(P_1 \oplus P_2) * P_3 = O$.
2. The second line, which is through O and O, intersects E only at O since O is flex. We conclude that $(P_1 \oplus P_2) \oplus P_3 = O$, i.e., $P_1 \oplus P_2 \oplus P_3 = O$. □

Notes Exercise 0.7.3. Let $E_{/k}$ be an elliptic curve with a flex identity $O \in E(k)$. Show that for any point $P \in E(k)$, if there exist $\ell, m, n \in \mathbb{Z}^+$ with $\ell mn \neq 0$ such that $\ell P, mP$ and nP lie on the same line, then P is a torsion point.

Exercise 0.7.3. For the elliptic curve

$$E_{/\mathbb{Q}} : y^2 = x^3 + 17,$$

given points $P_1 := (-2, 3)$, $P_2 := (-1, 4)$ and $P_3 := (2, 5)$ in $E(\mathbb{Q})$, directly use the chord and tangent method to prove the following.

a) $-2P_1 = (8, 23)$.
b) $P_2 \oplus P_3 = \left(-\frac{8}{9}, -\frac{109}{27}\right)$ (which is $\approx (-0.889, -4.037)$).

(You are allowed to use the formula for the inverse of a point, see Exercises 0.7.1 and 0.7.2.)

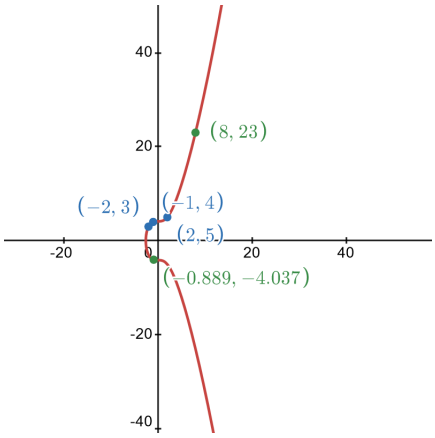


FIGURE 0.7.4. The elliptic curve $E : y^2 = x^3 + 17$.

Exercise 0.7.4. This exercise explores some arithmetic with an elliptic curve not in Weierstrass form.

Consider the cubic curve

$$E_{/\mathbb{Q}} : x^3 + y^3 = 1.$$

a) Write down the projective closure E_H of E. Show that $O := [1 : -1 : 0]$ is the only real point at infinity on E. Also show that E has exactly three points at infinity over $\mathbb{C}$.
b) Show that E_H is nonsingular. Deduce that E_H is a projective elliptic curve.
c) Thus E is an elliptic curve over $\mathbb{Q}$. Prove that for any point $P = (a, b) \in E(\mathbb{C})$ with $a \neq b$, the inverse of P is

$$-P = (b, a).$$

(You may assume that O is a flex point.)
d) For any point $P = (a, a) \in E(\mathbb{C})$, show that P has order two.
e) (Optional) Explain why E has no positive rational points.

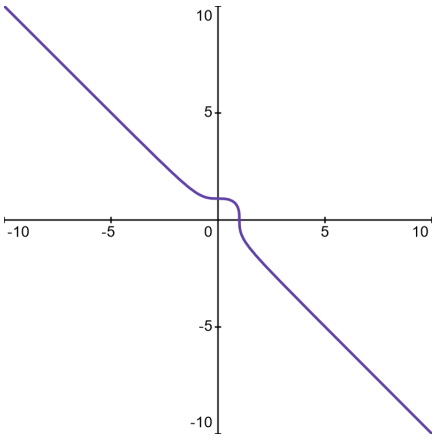


FIGURE 0.7.5. The elliptic curve $E : x^3 + y^3 = 1$.

Exercise 0.7.5. Consider the elliptic curve

$$E : y^2 + y = x^3.$$

a. Using the picture below, guess the real flex points of E.
b. With proof, determine the real flex points of E.

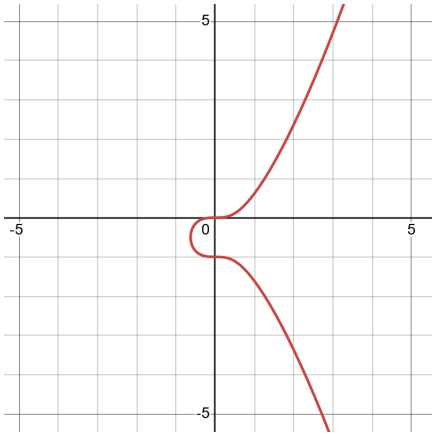


FIGURE 0.7.6. The elliptic curve $E : y^2 + y = x^3$.

Exercise 0.7.6. Let k be a field and $E_{/k}$ an elliptic curve in general Weierstrass form. This exercise will describe the points on E of order 2 and 3, under suitable assumptions.

a. Prove that the points on E of order dividing 2 are precisely the points with vertical tangent lines.
b. Further assume that $\text{char}(k) \neq 2$, and that E is given in short Weierstrass form,

$$E : y^2 = x^3 + Ax + B.$$

Show that the points of order 2 on E have the form $(\alpha, 0)$ where α is a root of $x^3 + Ax + B$.
c. Back to general Weierstrass form: prove that the points on E of order dividing 3 are precisely the flex points of E.

Exercise 0.7.7.

a. Given a planar elliptic curve $E_{/k}$ and a point $O \in E(k)$ *that is not necessarily flex,* show that the chord and tangent method makes $(E(k), O)$ an abelian group. (You can skip showing associativity.)
b. Consider the elliptic curve $E : y^2 = x^3 - 7x + 10$ from Example 0.6.1. We showed that for $P_1 := (1, 2)$ and $P_2 := (3, 4)$, one has $P_1 \oplus P_2 = (-3, 2)$ and $2P_1 = (-1, -4)$. Compute $P_1 \oplus P_2$ and $2P_1$ in the group $(E(k), P_2)$.

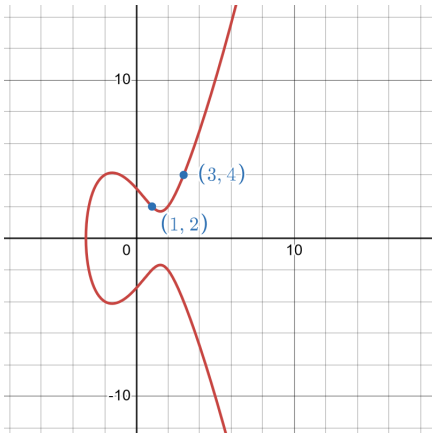


FIGURE 0.7.7. The elliptic curve $E : y^2 = x^3 - 7x + 10$.

Exercise 0.7.8. Show that for a planar elliptic curve $E_{/k}$ and two fixed points $O_1, O_2 \in E(k)$, the groups $(E(k), O_1)$ and $(E(k), O_2)$ are isomorphic.

1. Algebraic Varieties

For the rest of these notes, we will be following Silverman's book on elliptic curves [Sil09]; we will refer to sections as "chapters" and subsections as "sections".

This chapter will be a review of relevant topics from an introductory algebraic geometry class. We will generalize the definition of affine and projective curves. The upshot to using algebraic geometry is that we can understand elliptic curves much better. Additionally, studying elliptic curves from this more high-brow perspective makes it easier to study other geometric objects of number-theoretic interest down the road (such as *abelian varieties*).

If you haven't taken an algebraic geometry class yet, don't worry – this chapter will be important in setting up the geometry of plane curves in the next chapter, but you can black box the proofs of those results and still get a sense of the algebra and arithmetic of elliptic curves quite well.

Throughout these notes, we let k denote a **perfect field,** i.e., every algebraic extension of k is separable; in our eventual applications, we will let k be an algebraic extension of $\mathbb{Q}$ or $\mathbb{F}_p$, so assuming that k is perfect isn't too big of a deal. We will also let $\overline{k}$ denote a fixed algebraic closure of k (we sometimes let $\overline{k}$ also denote an algebraically closed field containing k instead).

1.1. Affine varieties.

We will start by defining the sets from algebraic geometry we are most interested in: *varieties.* The first type of variety for us is an *affine variety.*

Definition 1.1.1.

- For $n \in \mathbb{Z}^+$, define *affine n-space* as $\mathbb{A}^n := \mathbb{A}^n(\overline{k}) := \overline{k}^n$. For an extension ℓ/k, we also have *affine n-space over ℓ,* which is $\mathbb{A}^n(\ell) := \ell^n$.
- Fix an ideal $I \subseteq \overline{k}[x_1, \ldots, x_n]$. Then the **algebraic set of I** (over $\overline{k}$) is
$$V_I := \{P \in \mathbb{A}^n : \forall f \in I, f(P) = 0\}.$$
These are the points in $\mathbb{A}^n$ which are solutions to every polynomial in I.
- Say a subset $V \subseteq \mathbb{A}^n$ is an **affine variety defined over k,** written as $V_{/k}$, if there exists an ideal $I \subseteq k[x_1, \ldots, x_n]$ such that $V_I = V$ and I is *still prime* in $\overline{k}[x_1, \ldots, x_n]$.
  - Sometimes, we will say V is an affine *n-variety* to emphasize which affine n-space $\mathbb{A}^n$ we're viewing V in.

When $n = 2$, we say that $V_{/k}$ is an **affine algebraic curve over k.**

Thus, an affine variety over k is a zero set of polynomial equations with coefficients in k, with some *irreducibility conditions* on the ideal generating the set (see the next exercise). Recall that $\mathbb{A}^n$ has the *Zariski topology,* which is the coarsest topology for which algebraic sets are closed (this also serves as a definition).

Exercise 1.1.1. **Prerequisite: algebraic geometry.**
Show that an algebraic set $V_I \subseteq \mathbb{A}^n$ is irreducible with respect to the Zariski topology iff I is a prime ideal in $\overline{k}[x_1, \ldots, x_n]$. (See also Exercises 0.5.1 and 1.2.1.)

Recall that the Hilbert Basis Theorem says every ideal $I \subseteq k[x_1, \ldots, x_n]$ is *finitely generated,* i.e., has the form $I = (f_1, \ldots, f_m)$ where each $f_i \in k[x_1, \ldots, x_n]$. The following exercise then simplifies the definition of the corresponding algebraic set V_I.

Notes Exercise 1.1.1. Show that if $I = (f_1, \ldots, f_m) \subseteq k[x_1, \ldots, x_n]$, then

$$V_I = V_{f_1,\ldots,f_m} := \{P \in \mathbb{A}^n : \forall 1 \leq i \leq n,\ f_i(P) = 0\}.$$

Thus, every affine k-variety in $\mathbb{A}^n$ has the form $V_{f_1,\ldots,f_m}$ for some $f_i \in k[x_1, \ldots, x_n]$. We will often write varieties as

$$V : f_1(x_1, \ldots, x_n) = \ldots = f_n(x_1, \ldots, x_n) = 0.$$

In these notes, we are interested in *rational* points on varieties, which leads us to the following definition.

Definition 1.1.2. Given a variety $V_{/k} \subseteq \mathbb{A}^n$, we define the **set of k-rational points of V** as

$$V(k) := V \cap \mathbb{A}^n(k).$$

Furthermore, if the polynomials $f_i \in k[x_1, \ldots, x_n]$ which define V have coefficients in a subring $R \subseteq k$, then we also have the **set of R-integral points of V,** defined as

$$V(R) := V(k) \cap R^n.$$

There is an alternative but important definition of k-rational points on a variety $V_{/k}$, defined by an action of the **absolute Galois group** $G_k := \mathrm{Gal}(\overline{k}/k)$.[3]

Definition 1.1.3. The absolute Galois group G_k acts on $\mathbb{A}^n$ coordinate-wise: for all points $P := (a_1, \ldots, a_n) \in \mathbb{A}^n$ and for all $\sigma \in G_k$, one has

$$\sigma(P) := (\sigma(a_1), \ldots, \sigma(a_n)).$$

Notes Exercise 1.1.2. Show that for a variety $V_{/k}$, there is an action of G_k on V: for all $P \in V$, one has for all $\sigma \in G_k$ that

$$\sigma(P) \in V.$$

Furthermore, we have $P \in V(k)$ if and only if $\forall \sigma \in G_k$, one has $\sigma(P) = P$, and so the k-rational points in V are precisely those points fixed by the action of G_k.

What is the upshot to this group action definition of a rational point? There are quite a few benefits to describing rational points this way. Here is one: we will see later in these notes that this action takes torsion points on an elliptic curve to torsion points, and thus it can be used to described the rationality of torsion points in terms of the group theory of invertible matrices (keyword: *Galois representations*).

[3]Recall that $\overline{k}/k$ is an *infinite* Galois extension, i.e., normal and separable with infinite degree. Elements $\sigma \in G_k$ are automorphisms $\sigma\colon \overline{k} \xrightarrow{\sim} \overline{k}$ which fix k; these automorphisms are defined on *every algebraic number over k.* There is a great set of notes which contains a good amount of details pertaining to infinite Galois theory, due to Conrad: `https://ctnt-summer.math.uconn.edu/wp-content/uploads/sites/1632/2020/06/CTNT-InfGaloisTheory.pdf`. We won't need to know too much fine details about infinite Galois theory for these notes: just note that it packages together the information of *all* finite Galois extensions of k in a compatible way. G_k is a profinite group, in particular, an inverse limit of finite Galois groups.

Example 1.1.1. Here are some examples of affine varieties:

- If $f(x,y) := x - y \in \mathbb{R}[x,y]$ then $V_f(\mathbb{R}) = \{(a,b) \in \mathbb{R}^2 : a = b\}$; we can also write
$$V_{/\mathbb{R}} : y = x.$$
This is simply the line in $\mathbb{R}^2$ through the origin with slope 1.
- For $g(x,y,z) := x^2 + y^2 - z^2 \in \mathbb{R}[x,y,z]$, we have that $V_g(\mathbb{R})$ is a 3-D cone pointed at the origin, also reflected across the x,y-plane – use 3D desmos to draw it! (This variety is also called a *surface*.)

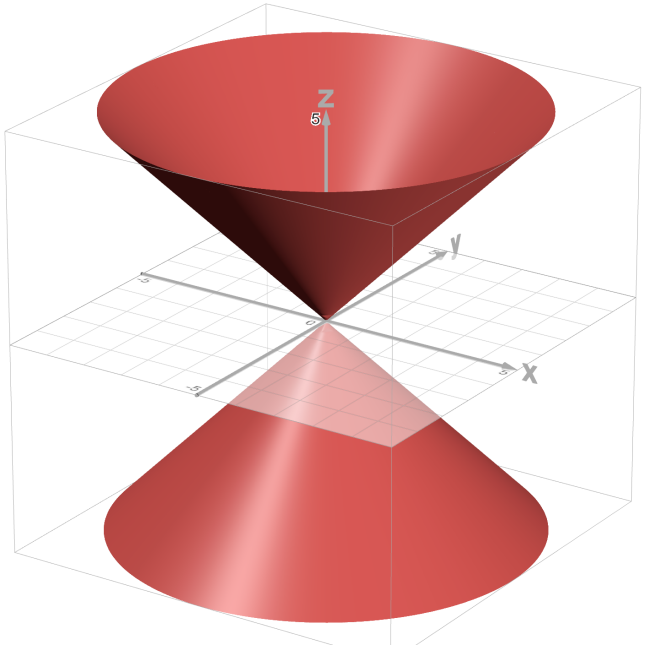


FIGURE 1.1.1. The variety $V_g : x^2 + y^2 = z^2$.

- If $V \subseteq \mathbb{A}^2(\mathbb{R})$ is the set of points
$$V_{/\mathbb{R}} = \{(a,b) \in \mathbb{R}^2 : a^2 + b^2 = 1\},$$
then V is the unit circle in $\mathbb{R}^2$ at the origin, defined by $h(x,y) := x^2 + y^2 - 1$. Also observe that $h \in \mathbb{Z}[x,y]$, and so we can study both $V(\mathbb{Z})$ and $V(\mathbb{Q})$. We have $V(\mathbb{Z}) = \{(\pm 1, 0), (0, \pm 1)\}$, whereas $\#V(\mathbb{Q}) = \infty$, due to e.g. the existence of infinitely many Pythagorean triples.
- Consider the cubic curve
$$E_{/\mathbb{Q}} : y^2 = x^3 - 2x + 1.$$
Its discriminant is $\Delta_E = 80 \neq 0$, and is thus an elliptic curve (see Exercise 0.4.1). We can draw a picture of it over $\mathbb{R}$:

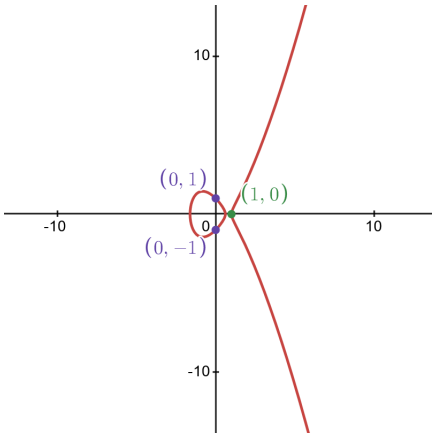


FIGURE 1.1.2. The variety $E : y^2 = x^3 - 2x + 1$.

As it turns out, we have $E(\mathbb{Q}) = \{O, (0, \pm 1), (1, 0)\}$. However, realizing E as lying over $\mathbb{Q}(\sqrt{2})$, we find instead that

$$E(\mathbb{Q}(\sqrt{2})) = \langle P \rangle \oplus \{O, (0, \pm 1), (1, 0)\},$$

where $P := (\sqrt{2} + 2, 2\sqrt{2} + 3) \in E(\mathbb{Q}(\sqrt{2}))$ has infinite order. On the other hand, we have $E(\mathbb{Q}(\sqrt{3})) = E(\mathbb{Q}) = \{O, (0, \pm 1), (1, 0)\}$. Studying $E(K)$ as $K/\mathbb{Q}$ varies is an extremely interesting question.

- We can also realize the same elliptic curve as a complex curve:

$$E_{/\mathbb{C}} : y^2 = x^3 - 2x + 1.$$

Then its picture is different: it is a *complex torus.* Over $\mathbb{C}$, we have $E[\text{tors}] \subseteq E(\mathbb{C})$, and in fact $\text{rank}(E(\mathbb{C})) = \#\mathbb{C}$ (see `https://math.stackexchange.com/questions/1577405/elliptic-curve-over-algebraically-closed-field-of-characteristic-0-has-a-non-t`).

- We can also realize E as an elliptic curve over $\mathbb{F}_{71}$ since $\Delta_E \not\equiv 0 \pmod{71}$. We can picture it using `https://graui.de/code/elliptic2/`. (Note that over finite fields $\mathbb{F}$, we have for any elliptic curve $E_{/\mathbb{F}}$ that $E(\mathbb{F}) = E(\mathbb{F})[\text{tors}]$.)

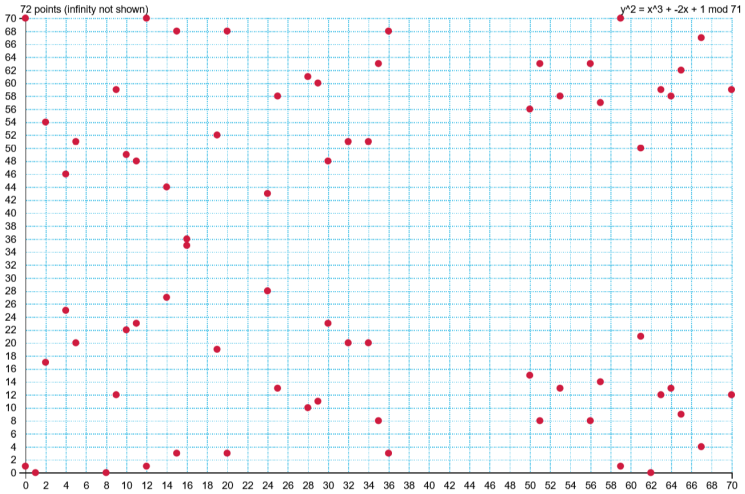


FIGURE 1.1.3. The variety $E_{/\mathbb{F}_{71}} : y^2 = x^3 - 2x + 1$.

In conclusion: the picture of E can change a lot when viewed over different fields!

Remark 1.1.1. Something we took for granted in these examples is that these algebraic sets were *varieties,* i.e., their defining equations generated prime ideals in $\overline{k}[x, y]$. By Exercise 1.1.1, this is equivalent to the algebraic set being irreducible. However, it will be enough to know that the *projective closure* of the variety is nonsingular, by Exercise 0.5.1 (this will be discussed in the next section).

For a variety $V_{/k}$ with a fixed point $P \in V$, if P is not already k-rational, then it is natural to ask when P "becomes rational." This leads us to the following definition.

Definition 1.1.4. Given an affine n-variety $V_{/k}$ and a point $P = (a_1, \ldots, a_n) \in V$, the **field of definition of P,** written as $k(P)$, is

$$k(P) := k(a_1, \ldots, a_n).$$

Notes Exercise 1.1.3. Show that for a variety $V_{/k}$ and a point $P \in V$, the field of definition $k(P)$ is a finite extension of k.

Next, let us recall the coordinate ring and function field of a variety. Understanding which continuous functions are defined (even almost everywhere) on a variety is important, since they characterize the variety up to different notions of equivalence.

Definition 1.1.5. Given an affine variety $V_{/k} := V_{I/k}$ in $\mathbb{A}^n$, its **coordinate ring over k** is

$$k[V] := k[x_1, \ldots, x_n]/I.$$

Since I is prime, we know that $k[V]$ is a domain. Its fraction field, denoted by $k(V) := \mathrm{ff}(k[V])$, is called the **function field of V over k.** Elements of $\overline{k}(V)$ are called *rational functions on V over k.* Without qualification, the rings $\overline{k}[V]$ and $\overline{k}(V)$ will be called the coordinate ring and function field of V, respectively.

Example 1.1.2. Consider $V := \mathbb{A}^n$. Then $V = V_{(0)}$, and thus its coordinate ring is $\overline{k}[V] = \overline{k}[x_1, \ldots, x_n]$, and has function field $\overline{k}(V) = \overline{k}(x_1, \ldots, x_n)$.

Another example is the parabola

$$C_{/\mathbb{Q}} : y = x^2.$$

We can check that that C is a curve in two ways: either proving directly that $(y - x^2) \subseteq \overline{\mathbb{Q}}[x, y]$ is prime, or checking that the projective closure $C_H : YZ = X^2$ is nonsingular (we will discuss the notion of projective closure in the next section). In any case, the parabola has a coordinate ring

$$\mathbb{Q}[C] := \frac{\mathbb{Q}[x, y]}{(y - x^2)}$$

over $\mathbb{Q}$. This ring is isomorphic to $\mathbb{Q}[x]$ under the map $\overline{p(x, y)} \mapsto p(x, x^2)$. Its function field over $\mathbb{Q}$ is then

$$\mathbb{Q}(C) \cong \mathbb{Q}(x).$$

This is an example of a *rational curve* (i.e., its projective closure is *isomorphic* to $\mathbb{P}^1$ over its base field). This is equivalent to the *genus* of C being 0, since C has a rational point $(0, 0) \in C(\mathbb{Q})$. We will define some of these terms in this chapter and the following one.

Here is an important invariant of varieties.

Definition 1.1.6. For an affine variety $V_{/k}$, the **dimension of** V is the transcendence degree of the field extension $\overline{k}(V)/\overline{k}$.[4] We will denote it by $\dim(V)$.

When a variety $V \subseteq \mathbb{A}^n$ has dimension one, we call V an affine **curve.** Compare this to our current definition of curves.

Example 1.1.3. The variety $\mathbb{A}^n$ has dimension n, since $\overline{k}(\mathbb{A}^n) = \overline{k}(x_1, \ldots, x_n)$ has transcendence degree n over $\overline{k}$. The affine curve

$$C_{/\mathbb{Q}} : y = x^2$$

has dimension 1, since $\overline{\mathbb{Q}}(C) \cong \overline{\mathbb{Q}}(x)$ has transcendence degree 1 over $\overline{\mathbb{Q}}$. (This agrees with our new definition of a curve.)

The following exercise is important when considering singularities on curves (which we will do in a moment, in Example 1.1.4).

Exercise 1.1.2. Show that for a projective n-variety $V_{/k} \subseteq \mathbb{P}^n$ defined by a single non-constant homogeneous polynomial

$$V : F(X_0, X_1, \ldots, X_n) = 0,$$

one has $\dim(V) = n - 1$. Such varieties are called *hypersurfaces.* (For more on projective hypersurfaces, see [Sil09, Exercise 1.11].)

[4]Recall that for a field extension ℓ/k, the *transcendence degree of* ℓ/k is the largest possible size of any *algebraically independent* subset of ℓ/k (such a subset's elements are not the simultaneous roots of any nonzero polynomial over k).

Here is another important concept we will review for affine varieties, which is that of *nonsingularity.*

Definition 1.1.7. Fix an affine n-variety $V_{/k}$; say it is defined by $f_1, \dots, f_m \in k[x_1, \dots, x_n]$. Then for a point $P \in V$, we say that V is **nonsingular at** P (or **smooth at** P) if the matrix

$$\left(\left. \frac{\partial f_i}{\partial x_j} \right|_P \right)_{1 \le i \le m}^{1 \le j \le n}$$

has rank $n - \dim(V)$. Say V is **nonsingular** (or **smooth**) if it is smooth at every point $P \in V$.

Example 1.1.4. An important example is when $V_{/k}$ is defined by one polynomial equation: $V = V_f$ where $f \in k[x_1, \dots, x_n]$. Then there is $i = 1$ row above, and this nonsingularity condition is equivalent to the $1 \times n$ row matrix

$$\left[\left. \frac{\partial f}{\partial x_1} \right|_P, \left. \frac{\partial f}{\partial x_2} \right|_P, \dots, \left. \frac{\partial f}{\partial x_n} \right|_P \right]$$

having rank $n - (n-1) = 1$ (see Exercise 1.1.2). However, a row matrix automatically has rank 1 if and only if it is a nonzero matrix.[5] Thus $P \in V$ is singular iff for all $1 \le i \le n$ one has

$$\left. \frac{\partial f}{\partial x_i} \right|_P = 0.$$

Here is an alternative definition of nonsingularity in terms of functions, which can be useful (both practically and theoretically).

Definition 1.1.8. For an affine n-variety $V_{/k}$ and a point $P \in V$, define the ideal

$$M_P := \{ f \in \overline{k}[V] : f(P) = 0 \}.$$

Then M_P is maximal, and in fact $M_P/(M_P)^2$ is a finite dimensional $\overline{k}$-vector space (also called the *cotangent space of* P). Say that V is **nonsingular at** P (or **smooth at** P) if

$$\dim_{\overline{k}}(M_P/(M_P)^2) = \dim(V).$$

If you would like to challenge yourself:

Exercise 1.1.3. [Sil09, Exercise 1.3] Show that for an affine hypersurface

$$V_{/k} : f(x_1, x_2, \dots, x_n) = 0,$$

our two definitions of nonsingularity at a point are equivalent. More precisely, for a point $P \in V$, the $1 \times n$ matrix

$$\left(\frac{\partial f}{\partial x_i} \right)_{1 \le j \le n}$$

has rank $n - 1$ iff $\dim_{\overline{k}}(M_P/M_P^2) = n - 1$.

[5]Note that the row rank is equal to the column rank; here, the columns are elements of k, so the column rank is also 1 iff the row matrix is nonzero.

(*Hint:* define the *tangent plane of* V *at* P as

$$T := \left\{ (y_1, y_2, \ldots, y_n) \in \mathbb{A}^n : \sum_{i=1}^{n} \left(\frac{\partial f}{\partial x_i}\bigg|_P \right) \cdot y_i = 0 \right\}.$$

Show that the map

$$M_P/M_P^2 \times T \to \overline{k},\ (g, y) \mapsto \sum_{i=1}^{n} \left(\frac{\partial g}{\partial x_i}\bigg|_P \right) \cdot y_i$$

is a well-defined perfect pairing of $\overline{k}$-vector spaces.

Example 1.1.5. Here is an example with checking whether a point is singular with both definitions. Consider the curves

$$C_1 : y^2 = x^3 + x$$

and

$$C_2 : y^2 = x^3 + x^2.$$

They are pictured in Figure 1.1.4.

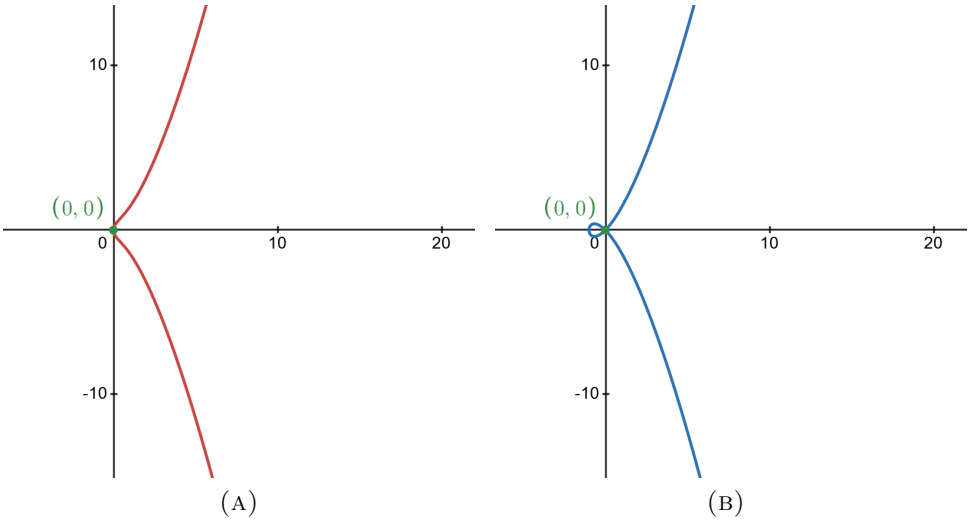


FIGURE 1.1.4. The curves $C_1 : y^2 = x^3 + x$ and $C_2 : y^2 = x^3 + x^2$.

Let $F(x, y) := y^2 - (x^3 + x)$ and $G(x, y) := y^2 - (x^3 + x^2)$ be the defining equations for C_1 and C_2, respectively. Let us check for singular points using the partial derivative definition: since $\frac{\partial F}{\partial x} = -3x^2 - 1 = 0$ and $\frac{\partial F}{\partial y} = 0$ imply that $x^2 = -\frac{1}{3}$ and $y = 0$ respectively, we deduce that C_1 is nonsingular since $\left(\pm\frac{i}{\sqrt{3}}, 0\right) \notin C_1(\mathbb{C})$. On the other hand, checking both $\frac{\partial G}{\partial x} = -3x^2 + 2x = 0$ and $\frac{\partial F}{\partial y} = 2y = 0$, we see that $(0, 0) \in C_2$ is a singular point.

Next, let's check whether $P := (0, 0)$ is singular on C_1 and C_2 with the second definition (which has its utilities in understanding the local ring of both C_1 and C_2 at

P which, in general, which is useful for applications we will see later). For this, we need to compute the ideal $M_P \subseteq \mathbb{C}[C_i]$ of vanishing functions at P, and then the dimension of M_P/M_P^2 over $\mathbb{C}$. Writing $\overline{f}$ for the coset of an element $f \in \mathbb{C}[x,y]$ in $\mathbb{C}[C_i]$, in both cases we have $M_P = (\overline{x}, \overline{y})\mathbb{C}[C_i]$ (since $\overline{x}, \overline{y}$ are in M_P and they are minimal in degree); this implies that $M_P^2 = (\overline{x}^2, \overline{xy}, \overline{y}^2)\mathbb{C}[C_i]$. Thus, the set

$$\{\overline{x} + M_P^2, \overline{y} + M_P^2\}$$

generates M_P/M_P^2 over $\mathbb{C}$ in both cases. *However,* in $\mathbb{C}[C_1] := \frac{\mathbb{C}[x,y]}{(y^2-(x^3+x))}$ we have $\overline{y}^2 = \overline{x}^3 + \overline{x}$, so that $\overline{x} = \overline{y}^2 - \overline{x}^3$, and thus

$$\overline{x} + M_P^2 = (\overline{y}^2 - \overline{x}^3) + M_P^2 = 0 + M_P^2,$$

since $\overline{y}^2 \in M_P^2$ and $\overline{x} \cdot \overline{x}^2 = \overline{x}^3 \in M_P^2$. Since $\overline{y} \notin M_P^2$, we conclude that $\dim_{\mathbb{C}}(M_P/M_P^2) = 1$, and thus $\dim_{\mathbb{C}}(M_P/M_P^2) = \dim(C_1)$, whence we conclude that P is nonsingular on C_1. However, we only have the relation $\overline{x}^2 = \overline{y}^2 - \overline{x}^3$ in $\mathbb{C}[C_2]$, which implies that $\{\overline{x} + M_P^2, \overline{y} + M_P^2\}$ stays $\mathbb{C}$-linearly independent in M_P/M_P^2. We conclude that $\dim_{\mathbb{C}}(M_P/M_P^2) = 2 > \dim(C_1)$, and thus P is singular on C_2.

Finally, given a point $P \in V$, we can localize $k[V]$ at M_P. Explicitly, this localization, called the **local ring of V at P,** is

$$\begin{aligned}\overline{k}[V]_P := \overline{k}[V]_{M_P} :&= \{f \in \overline{k}(V) : f \text{ is defined at } P\} \\ &= \left\{\frac{f}{g} \in \overline{k}(V) : f, g \in \overline{k}[V] \text{ with } g(P) \neq 0\right\}.\end{aligned}$$

Thus $\overline{k}[V]_P$ is the subring of rational functions in $\overline{k}(V)$ defined at P; such functions are also said to be *regular* at P. Explicitly, the localization $\overline{k}[V]_P$ is created by inverting regular functions on C which are nonzero at P.

To summarize some function definitions:

- An affine variety $V_{/k}$ gets a coordinate ring $\overline{k}[V]$, which is essentially the ring of polynomial functions on V.
- It also gets a function field $\overline{k}(V)$, which is the ring of rational functions on V, which are fractions of polynomial functions on V (in analogy to meromorphic functions on a complex manifold).
- For each point $P \in V$, we have a local subring $\overline{k}[V]_P \subseteq \overline{k}(V)$, where elements of $\overline{k}[V]_P$ are regular at P, i.e., defined at P.

1.2. **Projective varieties.** In this section, we will describe some basic definitions for projective varieties. In these notes, the algebraic geometry we do will be for projective varieties, for the most part – as we will see in the next chapter, projective curves are *complete,* which makes them a lot nicer to work with than affine curves in general. However, local properties for projective varieties can be reduced to affine computations, so it is good to know how to work with both types of varieties.

Definition 1.2.1.

- For $n \in \mathbb{Z}^+$, define *projective n-space* (over $\overline{k}$) as

$$\mathbb{P}^n := \mathbb{P}^n(\overline{k}) := \{P \neq (0, 0, \ldots, 0) \in \mathbb{A}^{n+1}\}/\sim,$$

where for $P, Q \in \mathbb{A}^{n+1}$ one has $P \sim Q$ iff $\exists \lambda \in \overline{k}^\times$ with $P = \lambda Q$. Thus, points in $\mathbb{P}^n$, written as $[a_0 : a_1 : \ldots : a_n]$, are equivalence classes of points in $\mathbb{A}^{n+1}$.

- An ideal $J \subseteq k[x_0, x_1, \ldots, x_n]$ is **homogeneous** if it is generated by *homogeneous polynomials,* which are polynomials $F(X_0, X_1, \ldots, X_n) \in k[X_0, X_1, \ldots, X_n]$ with "homogeneity in their monomial degrees." That is, there exists $d \in \mathbb{Z}_{\geq 0}$, called the *total degree* of F, such that for all points $(a_0, a_1, \ldots, a_n) \in \mathbb{A}^{n+1}$ and for all $\lambda \in \overline{k}^\times$, one has
$$F(\lambda a_0, \lambda a_1, \ldots, \lambda a_n) = \lambda^d \cdot F(a_0, a_1, \ldots, a_n).$$
- For a homogeneous ideal $J \subseteq \overline{k}[X_0, X_1, \ldots, X_n]$, the **projective set of** J (over $\overline{k}$) is
$$V_J := \{P \in \mathbb{P}^n : \forall F \in J, F(P) = 0\}.$$
If J is a prime ideal, we say that V is a **projective variety.**
- A projective variety $V \subseteq \mathbb{P}^n$ is **defined over** k if there exists a homogeneous ideal $J \subseteq k[X_0, X_1, \ldots, X_n]$ that is prime over $\overline{k}$, with $V = V_J$. In this case, we write $V_{/k} := V_J/k$.

Notes Exercise 1.2.1. In analogy to Notes Exercise 0.3.2, show that the "zero locus" of a homogeneous polynomial is well-defined: i.e., for any homogeneous $F \in k[X_0, X_1, \ldots, X_n]$, one has for $(a_0, a_1, \ldots, a_n) \in \mathbb{A}^{n+1}$ that
$$F(a_0, a_1, \ldots, a_n) = 0$$
iff for all $\lambda \in \overline{k}^\times$,
$$F(\lambda a_0, \lambda a_1, \ldots, \lambda a_n) = 0.$$
Thus, the expression
$$F([a_0 : a_1 : \ldots : a_n]) = 0$$
for $[a_0 : a_1 : \ldots : a_n] \in \mathbb{P}^n$ makes sense.

Notes Exercise 1.2.2. Show that a polynomial $F \in k[X_0, X_1, \ldots, X_n]$ of total degree d is homogeneous iff it can be written as
$$F = \sum_{e_0 + e_1 + \ldots + e_n = d} \alpha_{e_0, e_1, \ldots, e_n} \cdot X_0^{e_0} X_1^{e_1} \cdots X_n^{e_n}$$
for some $\alpha_{e_0, e_1, \ldots, e_n} \in k$.

Even with the equivalence class definition of $\mathbb{P}^n$, it still makes sense to talk about *rational* projective points.

Definition 1.2.2. A point $P \in \mathbb{P}^n$ is said to be k**-rational** if it can be written as
$$P = [a_0 : a_1 : \ldots : a_n]$$
where each $a_i \in k$.

For an alternative definition, note that G_k acts on $\mathbb{P}^n$ coordinatewise: for $P := [a_0 : a_1 : \ldots : a_n] \in \mathbb{P}^n$, one has
$$\sigma(P) := [\sigma(a_0) : \sigma(a_1) : \ldots : \sigma(a_n)].$$
Then say that a point $P \in \mathbb{P}^n$ is k**-rational** if for all $\sigma \in G_k$ one has $\sigma(P) = P$.

Notes Exercise 1.2.3. Check that the action above is well-defined. Then show that both definitions of rationality are equivalent.

These definitions extend to rational points on a *projective variety* $V_{/k}$.

Notes Exercise 1.2.4. Show that for a projective variety $V_{/k} \subseteq \mathbb{P}^n$, one has for $P \in V$ and $\sigma \in G_k$ that $\sigma(P) \in V$.

Example 1.2.1. Here are some examples of projective varieties.

- A *line* in $\mathbb{P}^2$ has the form
$$L : aX + bY + cZ = 0$$
where not all of a, b and c are zero. This assumption implies the line is non-singular, and so it is a projective variety. If $a, b, c \in k$, then V is defined over k.
- More generally, a *hyperplane* in $\mathbb{P}^n$ is given by an equation
$$H : a_0X_0 + a_1X_1 + \ldots + a_nX_n = 0$$
where not all a_i are zero.
- The equation
$$E_{/k} : Y^2Z = X^3 + AXZ^2 + BZ^3$$
defines a projective elliptic curve when E is nonsingular (which is equivalent to $\Delta_E := -16(4A^3 + 27B^2) \neq 0$ in k).

Next, let us discuss the connection between affine and projective varieties. For $0 \leq i \leq n$, dehomogenizing the i'th coordinate of $\mathbb{P}^{n+1}$ gives a bijection to $\mathbb{A}^n$: if we define the (open) projective subset
$$U(i) := \{[a_0 : a_1 : \ldots : a_n] \in \mathbb{P}^n : a_i \neq 0\} = \mathbb{P}^n \smallsetminus V_{X_i},$$
then for any $P \in U(i)$ we can uniquely write $P = [a_0 : a_1 : \ldots : \underbrace{1}_{i\text{'th coordinate}} : \ldots : a_n]$ for some $a_i \in \overline{k}$. This defines a map
$$\varphi_i \colon U(i) \to \mathbb{A}^n$$
via
$$P \mapsto (a_0, a_1, \ldots, a_{i-1}, a_{i+1}, \ldots, a_n)\,.$$
This is a bijection, with inverse $\mathbb{A}^n \to U(i)$ given by
$$(a_1, a_2, \ldots, a_n) \mapsto [a_1 : a_2 : \ldots : a_{i-1} : 1 : a_{i+1} : \ldots : a_n].$$
For a point $P \in U(i)$, we will write $P_i := \varphi_i(P)$. Thus, there are (at least) $n+1$ copies of $\mathbb{A}^n$ in $\mathbb{P}^n$! This gives several ways to projectively close affine varieties, each with respect to a projective coordinate X_i.

Example 1.2.2. We previously saw that we can embed $\mathbb{A}^2$ into $\mathbb{P}^2$ via $(a, b) \mapsto [a : b : 1]$. This is a special case of the above, where we take $U(Z) := \{[a : b : c] \in \mathbb{P}^2 : c \neq 0\}$.

In analogy to this example and the earlier lectures, we can "projectively close" affine varieties $V \subseteq \mathbb{A}^n$ to turn them into projective varieties in $\mathbb{P}^n$, based on which coordinate we homogenize along. When we had $n = 2$, we chose the coordinate Z from X, Y, Z.

Definition 1.2.3. Given an integer $0 \leq i \leq n$ and a polynomial $f \in \overline{k}[x_0, x_1, \ldots, x_{i-1}, x_{i+1}, \ldots, x_n]$ (say of degree d), we can **homogenize f w.r.t. X_i:**

$$F(X_0, X_1, \ldots, X_n) := f^{(i)} := X_i^d f\left(\frac{X_0}{X_i}, \frac{X_1}{X_i}, \ldots, \frac{X_{i-1}}{X_i}, \frac{X_{i+1}}{X_i}, \ldots, \frac{X_n}{X_i}\right).$$

This is in analogy to homogenizing $f \in \overline{k}[x, y]$ into $F \in \overline{k}[X, Y, Z]$ via

$$F(X, Y, Z) := Z^d f\left(\frac{X}{Z}, \frac{Y}{Z}\right).$$

Conversely, given homogeneous $G \in \overline{k}[X_0, \ldots, X_n]$, we can **dehomogenize G w.r.t. X_i:**

$$g(x_0, x_1, \ldots, x_{i-1}, x_{i+1}, \ldots, x_n) := G(x_0, x_1, \ldots, x_{i-1}, 1, x_{i+1}, \ldots, x_n).$$

Now, for a fixed $0 \leq i \leq n$, given an affine variety $V := V_I \subseteq \mathbb{A}^n$, the **projective closure of V w.r.t. X_i** is the projective variety $V_i \subseteq \mathbb{P}^n$ defined by the ideal

$$I_i := \langle f^{(i)} : f \in I \rangle \overline{k}[X_0, X_1, \ldots, X_n].$$

Conversely, given a projective variety $V \subseteq \mathbb{P}^n$ and a coordinate X_i, we say that $V_i := V_{X_i} := U(i) \cap V$ is an **affine patch of V at X_i.** Points in $V \smallsetminus V_i$ are called **points at infinity w.r.t. X_i.**

It is clear that a projective variety $V \subseteq \mathbb{P}^n$ satisfies

$$V = \bigcup_{i=0}^{n} V_i.$$

As it turns out, each nonempty affine patch V_i has projective closure *isomorphic* to V.

Notes Exercise 1.2.5. Show that if a projective variety $V \subseteq \mathbb{P}^n$ is defined over k, then so is any nonempty affine patch $V_i \subseteq \mathbb{A}^n$.

The following exercise is overdue: it concerns irreducibility of a variety and its projective closure.

Exercise 1.2.1. **Prerequisite: algebraic geometry.**
Using the Zariski topology, show that an affine algebraic set $C \subseteq \mathbb{A}^n$ is irreducible iff its projective closure $C_H \subseteq \mathbb{P}^n$ is irreducible, and thus C is an affine variety iff C_H is a projective variety. (See also Exercise 0.5.1 and 1.1.1.)

Remark 1.2.1. We will often work with projective varieties implicitly, but write out their equation in affine coordinates, i.e., study the variety in one of its affine patches. For example, we will usually write elliptic curves in general Weierstrass form

$$E : y^2 + a_1 ax + a_3 y = x^3 + a_2 x^2 + a_4 x + a_6,$$

with the understanding that it is a projective curve (which is important since it has the hidden point at infinity $O := [0 : 1 : 0]$).

To wrap this section up, we will define a few projective variety invariants. First, we will describe the function field of a projective variety $V_{/k} \subseteq \mathbb{P}^n$ over k, which explicitly realizes it as a subfield of $k(X_0, X_1, \ldots, X_n)$.

Definition 1.2.4. For a projective variety $V_{/k} := V_J/k \subseteq \mathbb{P}^n$, the **function field of** V **over** k**,** denoted $k(V)$, is defined as the following subfield of $k(X_0, X_1, \ldots, X_n)$:

$$k(V) = \left\{ f \in k(X_0, X_1, \ldots, X_n) : \exists \text{homogeneous } F, G \in k[X_0, \ldots, X_n] \text{ of equal degree with } G \notin J \text{ and } f = \frac{F}{G} \right\} / \sim,$$

where $\frac{F_1}{G_1} \sim \frac{F_2}{G_2}$ iff $F_1G_2 - F_2G_1 \in J$. Elements of $k(V)$ are called *rational functions on* V*.*

As an example, the function field of $\mathbb{P}^n$ over $\mathbb{Q}$ is $\mathbb{Q}(\mathbb{P}^n) = \mathbb{Q}(X_0, X_1, \ldots, X_n)$. Thus, all function fields $\mathbb{Q}(V)$ of projective varieties $V_{/\mathbb{Q}} \subseteq \mathbb{P}^n$ are subfields of $\mathbb{Q}(\mathbb{P}^n)$.

Next, we will define some local invariants of a function field; this will involve an alternative but equivalent definition for $k(V)$.

Definition 1.2.5. Let $V_{/k} \subseteq \mathbb{P}^n$ be a projective variety; fix an affine patch $V_i \neq \emptyset$. Then the **function field of** V **over** k is $k(V) := k(V_i)$. Also, the **dimension of** V is $\dim(V_i)$. It can be shown that each $k(V_i)$ is k-isomorphic to each other, and so $k(V)$ is well-defined up to k-isomorphism.

Furthermore, fix $P \in V$; Suppose that $P \in V_i$. Say that V is **nonsingular** (or **smooth**) at P if V_i is nonsingular at P_i. The **local ring** of V at P over k, denoted $k[V]_P$, is defined as the local ring $k[V_i]_{P_i}$. A function $f \in \overline{k}[V]_P$ is said to be **regular,** or **defined,** at P.

Remark 1.2.2. Let us briefly explain how to connect the two definitions of the function field of a projective variety $V_{/k} \subseteq \mathbb{P}^n$. For clarity, we will do this in the planar case ($n = 3$), and with respect to the last variable $X_2 =: Z$.

Given a variety $V_{/k} := V_J/k \subseteq \mathbb{P}^2$, we have defined $k(V)$ as functions $f := \frac{F(X,Y,Z)}{G(X,Y,Z)} \in k(X, Y, Z)$ where $F, G \in k[X, Y, Z]$ are homogeneous of equal degree, and $G \notin J$, with a particular equivalence relation on $k(V)$. Assume that the Z-coordinate patch $V_Z := V \cap U(Z) \neq 0$. Then we have an *isomorphism* $U(Z) \cong \mathbb{A}^2$, and so V_Z can be viewed as an affine variety. Let us give coordinates x, y to $\mathbb{A}^2$; explicitly, we can take $x := \frac{X}{Z}$ and $y := \frac{Y}{Z}$. Then we have that φ induces a rational function $\varphi_Z := \frac{F(x,y,1)}{G(x,y,1)} \in k(V_Z)$; this is analogous to dehomogenization, since on this patch we have $Z = 1$.

Conversely, given a rational function $\psi := \frac{f(x,y)}{g(x,y)} \in k(V_Z)$, we can realize ψ as a rational function ψ^Z on V via the identifications $x \mapsto \frac{X}{Z}$ and $y \mapsto \frac{Y}{Z}$:

$$\psi^Z := \frac{f\left(\frac{X}{Z}, \frac{Y}{Z}\right)}{g\left(\frac{X}{Z}, \frac{Y}{Z}\right)}.$$

Even if $\deg(f) \neq \deg(g)$, one always has that ψ^Z can be written in the form $\frac{F'(X,Y,Z)}{G'(X,Y,Z)}$, where $F', G' \in k[X, Y, Z]$ are homogeneous *of equal degree.* (Convince yourself of this!)

As an example, consider the projective elliptic curve $E_{/\mathbb{Q}} : Y^2Z = X^3 + XZ^2$. This has the usual affine patch $E_Z : y^2 = x^3 + x$ (we previously wrote E_h instead of E_Z). We see that $\mathbb{Q}(E_Z) = \text{ff}\left(\frac{\mathbb{Q}[x,y]}{(y^2-(x^3+x))}\right)$. A rational function $\frac{f(x,y)}{g(x,y)} \in \mathbb{Q}(E_Z)$ can be realized as a rational function on E via identifying $x \mapsto \frac{X}{Z}$ and $y \mapsto \frac{Y}{Z}$; For example, the rational function $x^2/y \in \mathbb{Q}(E_Z)$ maps to $(\frac{X^2}{Z^2})/(\frac{Y}{Z}) = \frac{X^2}{YZ} \in \mathbb{Q}(E)$.

For a projective variety $V_{/k} \subseteq \mathbb{P}^n$, understanding how to identify rational functions in $k(V)$ with affine rational functions in $k(V_i)$ is important when performing "local" calculations on V, i.e., calculations at a point $P \in V$. This includes, for example, understanding ramification points under morphisms of projective varieties (which we will do in the next chapter).

Exercise 1.2.2. Prove that for a projective variety $V_{/k} \subseteq \mathbb{P}^n$:

a. $k(V)$ is well-defined;
b. $\dim(V)$ is well-defined;
c. for at least one $0 \leq i \leq n$, one can have $V_i = \emptyset$.

1.3. **Morphisms of varieties.** In this section, we will review algebraic maps between varieties. For most of these notes, we will focus on projective varieties since they are more "complete" than affine varieties (in a literal sense!). However, much of the definitions ahead also apply to affine objects with some adjustments.

We start with our first definition of a *rational map* (a nice map defined "almost everywhere").

Definition 1.3.1 (Definition 1 of a *rational map*)**.** Given two projective varieties $V_{1/k} \subseteq \mathbb{P}^m$ and $V_{2/k} \subseteq \mathbb{P}^n$, a **rational map** from V_1 to V_2 is a map

$$\phi \colon V_1 \dashrightarrow V_2$$

defined at all but finitely many points in V_1, where ϕ is given by *rational functions* in $\overline{k}(V_1)$, i.e., we can write

$$\phi = [f_0 : f_1 : \ldots : f_n]$$

for some rational functions $f_i \in \overline{k}(V_1)$. We say that ϕ is k**-rational** if $\exists \lambda \in \overline{k}(V_1)^\times$ such that each $\lambda \cdot f_i \in k(V_1)$. (Note that ϕ and $\lambda \cdot \phi$ are the same map on projective points, where they are defined.)

A subtlety here is that the rational functions f_i need not be defined at every point of V_1, since they can be expressed as quotients of homogeneous polynomials (see e.g. Definition 1.2.4). This is why we write $\phi \colon V_1 \dashrightarrow V_2$ with a dotted arrow.

Next is the notion of a rational map being defined at a point. Despite initial observations about where a rational map ϕ might not be defined, it may be possible to scale ϕ by a *rational function* and have it be defined at a point.

Definition 1.3.2 (Definition 1 of a *regular point*)**.** Given two projective varieties $V_1/k \subseteq \mathbb{P}^m$ and $V_2/k \subseteq \mathbb{P}^n$, a rational map $\phi \colon V_1 \dashrightarrow V_2$ and a point $P \in V_1$, we say that ϕ is **regular** (or **defined**) at P if there exists $g \in \overline{k}(V_1)$ such that:

i. each $g \cdot f_i$ is defined at P;
ii. for some j we have $(g \cdot f_j)(P) \neq 0$.

In such a case, we set

$$\phi(P) := ((g \cdot f_0)(P) : (g \cdot f_1)(P) : \ldots : (g \cdot f_n)(P)).$$

If ϕ is regular at every point in V_1, then we say that ϕ is a **regular function,** or a **morphism,** and we write $\phi \colon V_1 \to V_2$. If ϕ is k-rational, then we call ϕ a k**-rational morphism.**

Remark 1.3.1. Let us quickly note that the rational function g in the definition of "regular at P" can vary for different choices of P!

There is an equivalent definition for rational maps and regularity that [Sil09] also uses; it follows from the definitions above, by the fact that we can clear the denominators of rational functions in $\overline{k}(V_1)$ to get homogeneous polynomials in $\overline{k}[X_0, X_1, \ldots, X_n]$. Generally speaking, the first definition usually comes up in proof applications, whereas the second definition is helpful for exercise applications.

Definition 1.3.3 (Definition 2 of a *rational map*)**.** Given two projective varieties $V_1/k := V_{J_1}/k \subseteq \mathbb{P}^m$ and $V_2/k := V_{J_2}/k \subseteq \mathbb{P}^n$, a **rational map** from V_1 to V_2 is a map

$$\phi \colon V_1 \dashrightarrow V_2$$

defined at all but finitely many points in V_1, where ϕ is given by *homogeneous polynomials* in $\overline{k}(V_1)$, i.e., we can write

$$\phi = [F_0 : F_1 : \ldots : F_n]$$

for some homogeneous polynomials $F_i \in \overline{k}[X_0, X_1, \ldots, X_m]$ of equal degree, not all in J_1. We say that ϕ is k**-rational** if $\exists \lambda \in \overline{k}(V_1)^\times$ such that each $\lambda \cdot F_i \in k[X_0, X_1, \ldots, X_n]$.

Remark 1.3.2. In the above definition, the F_i need equal degrees with each other to be well-defined on projective points, and we require that not all F_i lie in J_1 since otherwise ϕ would be undefined at every point in V_1.

With this alternate definition of a rational map, we also have an alternate definition of regular points.

Definition 1.3.4 (Definition 2 of a *regular point*)**.** Given two projective varieties $V_1/k := V_{J_1}/k \subseteq \mathbb{P}^m$ and $V_2/k := V_{J_2}/k \subseteq \mathbb{P}^n$, as well as a rational map $\phi \colon V_1 \dashrightarrow V_2$ and a point $P \in V_1$, writing

$$\phi = (F_0 : F_1 : \ldots : F_n)$$

for homogeneous $F_i \in \overline{k}[X_0, X_1, \ldots, X_n]$ of equal degree, we say that ϕ is **regular** (or **defined**) at P if there exist homogeneous polynomials $G_0, G_1, \ldots, G_n \in \overline{k}[X_0, X_1, \ldots, X_n]$ of equal degree such that:

i. at least one $G_i(P) \neq 0$;
ii. for all pairs $0 \leq i, j \leq n$, we have

$$F_i \cdot G_j \equiv F_j \cdot G_i \pmod{J_1}. \tag{2}$$

When ϕ is regular at P as above, we define

$$\phi(P) := [G_0(P) : G_1(P) : \ldots : G_n(P)].$$

If ϕ is regular at every point in V_1, then we say that ϕ is a **regular function,** or **morphism,** and we write $\phi \colon V_1 \to V_2$. If ϕ is also k-rational, we call ϕ a k**-morphism.**

Remark 1.3.3. The latter condition (2) implies that as functions on V_1, we have

$$\frac{F_i}{F_j} = \frac{G_i}{G_j}$$

at all points where these quotients are defined. This implies that for any point $P \in V_1$ and index $0 \leq j \leq n$ where both $F_j(P) \neq 0$ and $G_j(P) \neq 0$, we can express the value $\phi(P)$ as

$$\begin{aligned}
\phi(P) :&= [F_0(P) : \ldots : F_j(P) : \ldots : F_n(P)] \\
&= \left[\frac{F_0(P)}{F_j(P)} : \ldots : 1 : \ldots : \frac{F_n(P)}{F_j(P)}\right] \\
&= \left[\frac{G_0(P)}{G_j(P)} : \ldots : 1 : \ldots : \frac{G_n(P)}{G_j(P)}\right] \qquad \text{(by Condition (2))} \\
&= [G_0(P) : \ldots : G_j(P) : \ldots : G_n(P)],
\end{aligned}$$

so that $\phi(P)$ is well-defined, i.e.,

$$\phi(P) = [F_0 : F_1 : \ldots : F_n](P) := [G_0(P) : G_1(P) : \ldots : G_n(P)],$$

where the latter value $[G_0(P) : G_1(P) : \ldots : G_n(P)]$ makes sense.

Example 1.3.1. Consider the map $\phi\colon \mathbb{P}^1 \dashrightarrow \mathbb{P}^2$ defined by

$$\phi([a : b]) := [a^2 : ab : b^2].$$

By the second definition, this is a rational map, written as

$$\phi = [X^2 : XY : Y^2].$$

This is clearly defined over k. It is also defined at every point (i.e., $(X^2, XY, Y^2) = (0, 0, 0) \Rightarrow (X, Y) = 0$, and $[0 : 0]$ is not a point on $\mathbb{P}^1$), so it is a k-morphism.

Definition 1.3.5. Given projective varieties $V_1/k \subseteq \mathbb{P}^m$ and $V_2/k \subseteq \mathbb{P}^n$, we say that a morphism $\phi\colon V_1 \to V_2$ is an **isomorphism** if there exists a morphism $\psi\colon V_2 \to V_1$ with $\psi \circ \phi = 1_{V_1}$ and $\phi \circ \psi = 1_{V_2}$. We say that ϕ is a *k-isomorphism* if both ϕ and ψ are defined over k.

Example 1.3.2. Consider the projective curve

$$V_{/\mathbb{Q}} : X^2 + Y^2 = Z^2.$$

Note that $V_{/\mathbb{R}}$ is the projective closure of the unit circle in $\mathbb{R}^2$. Consider the map

$$\phi\colon V \dashrightarrow \mathbb{P}^1$$

defined via

$$\phi([X : Y : Z]) := [X + Z : Y].$$

This is a rational map, defined over $\mathbb{Q}$. It is regular at any point $P \in V(\overline{\mathbb{Q}})$ such that $\phi(P) \neq (0, 0)$. Thus, it is regular at all points *except possibly* those $[X : Y : Z] \in V(\overline{\mathbb{Q}})$ where $X + Z = Y = 0$. Such a point is $[X : Y : Z] = [X : 0 : -X] = [-1 : 0 : 1]$.

We claim that ϕ is defined at $P := [-1 : 0 : 1]$. When attempting to compute $\phi(P)$, we know by the second definition of regularity that we are allowed to change $\phi = [X + Z : Y]$ into $\phi = [G_0(X, Y, Z) : G_1(X, Y, Z)]$ such that

$$(X + Z) \cdot G_1 \equiv Y \cdot G_0 \pmod{(X^2 + Y^2 - Z^2)}$$

where $G_0(P) \neq 0$ or $G_1(P) \neq 0$. This amounts to solving a congruence: since

$$X^2 - Z^2 = (X+Z)(X-Z) \equiv Y^2 \pmod{(X^2+Y^2-Z^2)},$$

we see that $G_0 := Y$ and $G_1 := (X-Z)$ works; furthermore, we have $G_1(P) = -2 \neq 0$. We deduce that ϕ is regular at P, with the value $\phi(P) = [G_0(P) : G_1(P)] = [0:1]$. We conclude that ϕ is a k-morphism.

Notes Exercise 1.3.1. Continuing the example above, show that the rational map

$$\psi\colon \mathbb{P}^1 \dashrightarrow V$$

defined by

$$\psi([S:T]) := [S^2 - T^2 : 2ST : S^2 + T^2]$$

is regular and inverse to ϕ. Conclude that $\phi\colon V \to \mathbb{P}^1$ is a $\mathbb{Q}$-isomorphism.

In the next chapter, we will see that for any two curves C_1 and C_2 where C_1 is *smooth,* one has that any rational map $\phi\colon C_1 \to C_2$ is defined everywhere, i.e., is a morphism.

Exercise 1.3.1. [Sil09, Exercise 1.4] Let $V_{/\mathbb{Q}}$ be the projective variety

$$V : 5X^2 + 6XY + 2Y^2 = 2YZ + Z^2.$$

Prove that $V(\mathbb{Q}) = \emptyset$.

Exercise 1.3.2. [Sil09, Exercise 1.6] Let $V \subseteq \mathbb{P}^2$ be the variety

$$V : Y^2Z = X^3 + Z^3.$$

Show that the map

$$\phi\colon V \dashrightarrow \mathbb{P}^2,\ \phi = [X^2 : XY : Z^2]$$

is a morphism. (Notice that ϕ does not extend to a morphism $\phi\colon \mathbb{P}^2 \to \mathbb{P}^2$.)

Exercise 1.3.3. [Sil09, Exercise 1.7] Let $V \subseteq \mathbb{P}^2$ be the variety

$$V : Y^2Z = X^3,$$

and let ϕ be the rational map

$$\phi\colon \mathbb{P}^1 \dashrightarrow V,\ \phi = [S^2T, S^3, T^3].$$

a. Show that ϕ is a morphism.
b. Find a rational map $\psi\colon V \dashrightarrow \mathbb{P}^1$ such that $\psi \circ \phi$ and $\phi \circ \psi$ are the identity wherever they are defined.
c. Is ϕ an isomorphism?

Exercise 1.3.4. [Sil09, Exercise 1.10] For each prime $p \geq 3$, let $V_p \subseteq \mathbb{P}^2$ be the variety given by the equation

$$V_p : X^2 + Y^2 = pZ^2.$$

a. Prove that V_p is isomorphic to $\mathbb{P}^1$ over $\mathbb{Q}$ if and only if $p \equiv 1 \pmod 4$.
b. Prove that for $p \equiv 3 \pmod 4$, no two of the V_p's are isomorphic over $\mathbb{Q}$.

2. Algebraic Curves

In this chapter, we closely study **curves,** which are defined as one-dimensional varieties (projective or affine). This includes not only elliptic curves, but also curves of arbitrary *genus* (a term we will define later in this chapter). We will continue to assume that k is a perfect field, and that $\overline{k}$ is an algebraic closure of k (or sometimes an algebraically closed field containing k).

Just as Silverman [Sil09] does, we will often cite proofs of algebraic-geometric results from standard textbooks such as [Sha13] and [Har77]; if we state a result from [Sil09] but do not cite a proof from [Sha13] or [Har77], this means that [Sil09] provides a proof. While we are not assuming a background in algebraic geometry for these notes, it would take up too much time to prove everything that we discuss; thus, we will prove some things and cite proofs for others.

2.1. **Curves.** Recall that a **curve** is a projective or affine variety of dimension one; for us, it will often be projective. We will write C to denote $C_{/\overline{k}}$, with the understanding that it is defined over some finite extension of k (often just k).

We usually focus on *smooth* curves. A particularly nice property holds for functions on a curve defined at smooth points, which makes analyzing them more consistent:

Proposition 2.1.1. [Sil09, Proposition II.1.1] *Let C be a curve and $P \in C$ a smooth point. Then $\overline{k}[C]_P$ is a discrete valuation ring.*

Proof. This follows from the fact that M_P/M_P^2 is a one-dimensional vector space over $\overline{k}$, along with a general commutative algebra result (see Exercise 2.1.1). □

Exercise 2.1.1. [Sil09, Exercise 2.1] Let R be a Noetherian local domain that is not a field, let $M \subseteq R$ be its maximal ideal and set $k := R/M$ its residue field. Show that the following are equivalent:

a. R is a discrete valuation ring;
b. M is principal;
c. $\dim_k M/M^2 = 1$.

(For us, this exercise is applied to the local ring $\overline{k}[C]_P$ at a smooth point P on a curve C.)

Remark 2.1.1. Recall that a **discrete valuation** on a field K is a surjective map

$$v\colon K \to \mathbb{Z} \cup \{\infty\}$$

such that for all $\alpha, \beta \in K$ we have:

1. $v(\alpha \cdot \beta) = v(\alpha) + v(\beta)$;
2. $v(\alpha + \beta) \geq \min\{v(\alpha) + v(\beta)\}$, with equality if $v(\alpha) \neq v(\beta)$;
3. $v(\alpha) = \infty$ iff $\alpha = 0$.

The set $R := \{\alpha \in K : v(\alpha) \geq 0\}$ is called the **discrete valuation ring for v.** Its maximal ideal is $M := \{\alpha \in K : v(\alpha) > 0\}$.

Notes Exercise 2.1.1. Suppose that $v\colon K \to \mathbb{Z} \cup \{\infty\}$ is a discrete valuation. Prove the *domination principle:* for $\alpha, \beta \in K$, if $v(\alpha) \neq v(\beta)$ then $v(\alpha+\beta) = \min\{v(\alpha), v(\beta)\}$.

Definition 2.1.1. Let C be a curve and $P \in C$ a smooth point. By Proposition 2.1.1, we know that $\overline{k}[C]_P$ is a DVR. The **normalized (discrete) valuation** on $\overline{k}[C]_P$, written as $v_P \colon \overline{k}[C]_P \to \mathbb{Z}_{\geq 0} \cup \{\infty\}$, is given by

$$v_P(f) := \sup\{d \in \mathbb{Z} : f \in M_P^d\};$$

Equivalently, $v_P(f)$ is the largest exponent $e \in \mathbb{Z}_{\geq 0}$ for which M_P^e divides (f) in $\overline{k}[C]$. Alternatively, writing $M_P = (t)$, we have $v_P := v_t$, where $v_t(f) := d \in \mathbb{Z}_{\geq 0}$ is such that $t^d \parallel f$. We call t a **uniformizer** for C at P.

The valuation on $\overline{k}[C]_P$ extends to a discrete valuation

$$v \colon \overline{k}(C) \to \mathbb{Z} \cup \{\infty\}$$

via $v_P(f/g) := v_P(f) - v_P(g)$ (noting that $\mathrm{ff}(\overline{k}[C]_P) = \overline{k}(C)$); then $\overline{k}[C]_P$ is the discrete valuation ring for v_P.

For $f \in \overline{k}(C)$, we call the value $v_P(f)$ the **order (of vanishing) of f at P.** If $v_P(f) > 0$, we say that P is a *zero* of f. If $v_P(f) < 0$, then we say that P is a *pole* of f, and we set $f(P) := \infty$. When $v_P(f) \geq 0$, we say that f is **regular** at P, and we can evaluate $f(P)$.

Here is a result on the finiteness of zeroes and poles for a rational function on a smooth curve.

Proposition 2.1.2. [Sil09, Proposition II.1.2] *Let C be a smooth curve and $f \in \overline{k}(C)^\times$. Then f has finitely many zeroes and poles; furthermore, if f has no poles, then $f \in \overline{k}^\times$.*

Proof. See [Har77, Lemma I.6.5], [Har77, Lemma II.6.1] or [Sha13, Chapter 3, §1.1] for the first part. For the second part, see [Har77, Theorem I.3.4a] or [Sha13, Chapter 1, §5.2, Corollary 1.1]. □

Notes Exercise 2.1.2. Show that for a curve C and a smooth point $P \in C$, a rational function $f \in \overline{k}(C)$ has a zero of order $n > 0$ at a smooth point $P \in C$ iff $1/f$ has a pole of order $n < 0$ at P.

Example 2.1.1. Let us reconsider the curves from Example 1.1.5:

$$C_1 : y^2 = x^3 + x$$

and

$$C_2 : y^2 = x^3 + x^2.$$

They are pictured in the the x, y-plane in Figure 7.2.1.

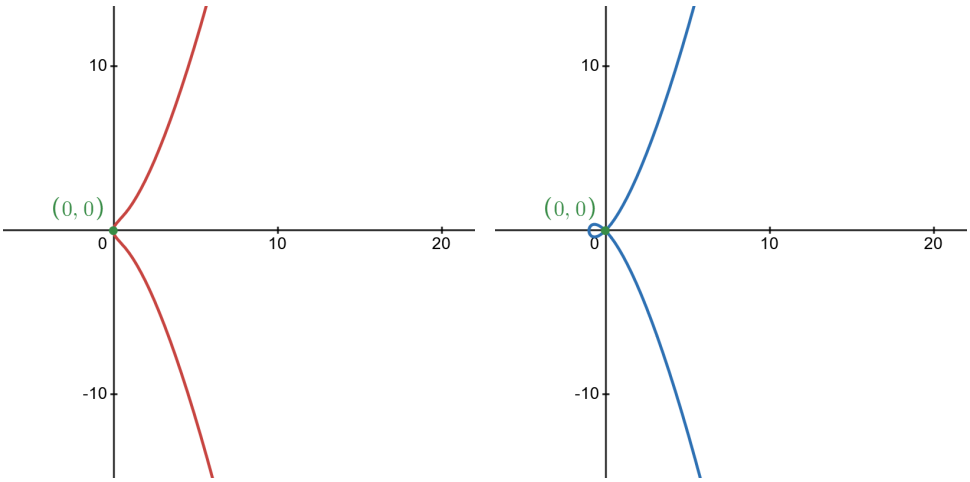


FIGURE 2.1.1. The curves $C_1 : y^2 = x^3 + x$ and $C_2 : y^2 = x^3 + x^2$.

Previously, we have shown that that $P := (0, 0)$ is on both curves, and that C_1 is nonsingular, whereas C_2 is singular only at P. Thus, by Exercise 2.1.1 we know that $\overline{k}[C_1]_P$ is a DVR, whereas $\overline{k}[C_2]_P$ is not.

We noted that in $\overline{k}[C_1] := \frac{\overline{k}[x,y]}{(y^2-(x^3+x))}$, one has $M_P = (\overline{x}, \overline{y})$ (recall that M_P is the ideal of functions in $\overline{k}[C_1]$ which have a zero at P). We claim that $\overline{x} \in (\overline{y})\overline{k}[C_1]_P$: by definition of the localization $\overline{k}[C_1]_P$, it is equivalent to show that there exists a function $f \in \overline{k}(C_1)$ that is both regular and nonzero at P, such that $\overline{x} = \overline{y} \cdot f$. Since $\overline{y}^2 = \overline{x}^3 + \overline{x} = \overline{x} \cdot (\overline{x}^2 + 1)$, observing that $(\overline{x}^2 + 1)$ is both regular and nonzero at P, we find that $\overline{x} = \overline{y}^2 \cdot \frac{1}{\overline{x}^2+1}$ in $\overline{k}[C_1]_P$. We deduce that $\overline{y}$ is a uniformizer for $\overline{k}[C_1]_P$, i.e., $v_P = v_{\overline{y}}$. This helps with computing the order of vanishing at P for rational functions on C_1.

Here are some examples: by knowing that $\overline{y}$ is a uniformizer at P, we get $v_P(\overline{y}) = 1$. On the other hand, to compute $v_P(\overline{x})$, we first observe that

$$\overline{x} = \overline{y}^2 - \overline{x}^3$$

in $\overline{k}[C_1]$. Since $v_P(\overline{y}^2) = 2v_P(\overline{y}) = 2$ and $v_P(\overline{x}^3) = 3v_P(\overline{x}) \geq 3$ (noting that x vanishes at P, and so $v_P(\overline{x}) \geq 1$), we deduce that

$$v_P(\overline{x}) = \min\{v_P(\overline{y}^2), v_P(\overline{x}^3)\} = 2$$

by Notes Exercise 2.1.1. Additionally,

$$v_P(2\overline{y}^2 - \overline{x}) = 2.$$

To see this, note that $2\overline{y}^2 - \overline{x} = 2\overline{x}^3 + \overline{x} = \overline{x} \cdot (2\overline{x}^2 + 1)$, and then $v_P(\overline{x}) = 2$, while $v_P(2\overline{x}^2 + 1) = 0$ since $2\overline{x}^2 + 1$ is both defined and nonzero at P. Note that these computations were done on their Z-affine patches, and still hold for the corresponding projective curves since smoothness and order of vanishing at a point is a local property.

(See also Remark 1.2.2 on analyzing rational functions with affine patches.) These "local variables", such as $x := \frac{X}{Z}$ and $y := \frac{Y}{Z}$ above, are sometimes called **local parameters.**

In these notes, we will come across fields K with positive characteristic (specifically, finite fields and function fields of curves over finite fields). In these situations, we will want to know when the field extensions L/K we are dealing with are *separable* (i.e., irreducible polynomials over L have distinct roots in $\overline{K}$). This proposition will help make some things simpler for us towards this end, especially when analyzing *differentials* on a curve.

Proposition 2.1.3. [Sil09, Proposition II.1.4] *Let $C_{/k}$ be a curve, and $t \in k(C)$ a uniformizer at a smooth point $P \in C(k)$. Then $k(C)/k(t)$ is separable.*

2.2. **Maps between curves.** In this section, we will study maps between curves, their properties and the connection to function fields of curves.

Here is an important result which says that a rational map from a smooth curve is regular, i.e., is defined at every single point.

Proposition 2.2.1. [Sil09, Proposition II.2.1] *Let C be a curve and $V \subseteq \mathbb{P}^n$ a projective variety. Let $P \in C$ be a smooth point, and let $\phi\colon C \dashrightarrow \mathbb{P}^n$ be a rational map. Then ϕ is regular at P. In particular, if C is smooth then ϕ is a morphism.*

Proof. Let us write $\phi = [f_0 : f_1 : \ldots : f_n]$ for rational functions $f_i \in \overline{k}(C)$ (definition 1 of a rational map, see Definition 1.3.1). Since C is smooth at P, we can fix a uniformizer $t \in \overline{k}(C)$ at P.

Let us set $m := \min_{0\leq i\leq n} v_P(f_i)$; fix $0 \leq j \leq n$ with $m = v_P(f_j)$. Then $m \in \mathbb{Z}$, and for each $0 \leq i \leq n$ one has $v_P(t^{-m} \cdot f_i) = -m + v_P(f_i) \geq 0$; thus, every $t^{-m} \cdot f_i$ is regular at P. Furthermore, since $v_P(t^{-m} \cdot f_j) = 0$, we know that $(t^{-m} \cdot f_j)(P) \neq 0$. We conclude that ϕ is regular at P (definition 1 of a regular point, see Definition 1.3.2). □

Example 2.2.1. Rational functions on a smooth curve $C_{/k}$ can be realized as rational maps from C to $\mathbb{P}^1$ defined over k. To see this, let $f \in k(C)$ be a rational function. Then f induces a rational map via

$$\phi\colon C \dashrightarrow \mathbb{P}^1,\ \phi(P) := [f(P) : 1],$$

which is defined over k. By Proposition 2.2.1, this is a morphism (possibly constant); the proof shows that

$$\phi(P) = \begin{cases} [f(P) : 1] & \text{if } f \text{ is regular at } P, \\ [1 : 0] & \text{if } f \text{ has a pole at } P. \end{cases}$$

Conversely, given a k-morphism $\phi\colon C \dashrightarrow \mathbb{P}^1$, writing $\phi = [f_0 : f_1]$ with $f_0, f_1 \in k(C)$:

- if $f_1 = 0$, then $\phi = [1 : 0]$ is a constant morphism, denoted by ∞;
- if $f_1 \neq 0$, then $\phi = \left[\frac{f_0}{f_1} : 1\right]$, where $\frac{f_0}{f_1} \in k(C)$.

Thus, we have a $1-1$ correspondence

$$k(C) \cup \{\infty\} \leftrightarrow \{k\text{-morphisms } C \to \mathbb{P}^1\}.$$

These two sets are often identified with each other.

Here is a theorem of theoretical significance, which concerns morphisms of curves.

Theorem 2.2.2. [Sil09, Theorem II.2.3] *Let $\phi\colon C_1 \to C_2$ be a morphism of curves. Then either ϕ is constant, or ϕ is surjective.*

Proof. see [Har77, Proposition II.6.8] or [Sha13, Chapter 1, §5.3, Theorem 1.12]. □

For the rest of these notes, unless otherwise stated we will assume our morphisms are nonconstant. Now we will study an important correspondence between morphisms of curves, and extensions of function fields. Given two curves $C_{1/k}$ and $C_{2/k}$, if $\phi\colon C_1 \to C_2$ is a k-morphism, then ϕ induces an injective homomorphism $\phi^*\colon k(C_2) \hookrightarrow k(C_1)$ via precomposition:

$$\phi^*(f) := f \circ \phi.$$

Observe that ϕ^* fixes k. This field homomorphism ϕ^* is often called the *pullback of ϕ.*

Theorem 2.2.3. [Sil09, Theorem II.2.4] *Let C_1/k and C_2/k be curves.*

a. *If $\phi\colon C_1 \to C_2$ is a k-morphism, then $k(C_1)$ is a finite extension of $\phi^*(k(C_2))$.*
b. *If $\iota\colon k(C_2) \hookrightarrow k(C_1)$ is an injection fixing k, then $\exists!$ k-morphism $\phi\colon C_1 \to C_2$ such that $\phi^* = \iota$.*
c. *For any subfield $\mathbb{K} \subseteq k(C_1)$ with $[k(C_1) : \mathbb{K}] < \infty$, there exists a smooth curve C_3/k, unique up to k-isomorphism, and a k-morphism $\phi\colon C_1 \to C_3$ with $\phi^*(k(C_3)) = \mathbb{K}$.*

Proof. Part a. is proven in [Har77, Proposition II.6.8], whereas part c. is in [Har77, Corollary I.6.12] (in the case where $k = \overline{k}$).

Let us prove part b.: we start with an injection $\iota\colon k(C_2) \hookrightarrow k(C_1)$. Let us write $C_1/k \subseteq \mathbb{P}^m$ and $C_2/k \subseteq \mathbb{P}^n$, and without loss of generality, assume that $C_2 \not\subseteq V_{X_n}$ (i.e., assume there exists a point in C_2 with nonzero X_n-coordinate). Observe that each coordinate $X_i \in k(C_2)$ gives a rational function $\iota(X_i) \in k(C_1)$. Let us define a map $\phi\colon C_1 \to C_2$ via

$$\phi := [\iota(X_0) : \iota(X_1) : \ldots : \iota(X_n)] = \left[\iota\left(\frac{X_0}{X_n}\right) : \iota\left(\frac{X_1}{X_n}\right) : \ldots : 1\right].$$

Note that ϕ is nonconstant. Otherwise, each $\iota\left(\frac{X_i}{X_n}\right) = \alpha_i$ for some $\alpha_i \in k$, and thus (applying ι^{-1} to both sides) we get $X_i = \alpha_i \cdot X_n$ for all $0 \leq i < n$. This would imply that $k(X_0, X_1, \ldots, X_n) = k(X_n)$, and thus from $k(C_2) \subseteq k(X_0, X_1, \ldots, X_n)$, we would be forced to have $k(C_2) = k(X_n)$, contradicting that $C_2 \not\subseteq V_{X_n}$.

Thus ϕ is a rational map (by Definition 1.3.1). It is defined over k since ι fixes k and each $\frac{X_i}{X_n} \in k(C_2)$. In particular, ϕ is a k-morphism. Furthermore, we check that $\phi^* = \iota$: for $f \in k(C_2)$, we have

$$\phi^*(f) := f \circ \phi = f(\iota(X_0), \ldots, \iota(X_n)) = \iota(f(X_0, \ldots, X_n)) = \iota(f)$$

since f is defined over k.

We can also check that ϕ is unique: if $\psi\colon C_1 \to C_2$ is another k-morphism with $\psi^* = \iota$, then we have for each $0 \leq i \leq n$ that

$$\psi^*\left(\frac{X_i}{X_n}\right) = \iota\left(\frac{X_i}{X_n}\right) = \frac{\iota(X_i)}{\iota(X_n)}.$$

If we write $\psi = [f_0 : f_1 : \ldots : f_n]$ with each $f_i \in k(C_1)$, then we *also* have for each $0 \leq i \leq n$ that

$$\psi^*\left(\frac{X_i}{X_n}\right) := \frac{f_i}{f_n},$$

since X_i and X_n are the i'th and n'th coordinates of ψ, respectively. We thus have

$$\frac{f_i}{f_n} = \frac{\iota(X_i)}{\iota(X_n)},$$

and so

$$\psi = \left[\frac{f_0}{f_n} : \ldots : \frac{f_{n-1}}{f_n} : 1\right] = \left[\frac{X_0}{X_n} : \ldots : \frac{X_{n-1}}{X_n} : 1\right] = \phi. \qquad \square$$

We have just demonstrated some of the correspondence between smooth curves over k, and function fields of transcendence degree 1 over k. As it turns out, for a field k, the category $\mathscr{C}$ whose objects are smooth curves C over k and whose maps are k-morphisms, is equivalent to the category $\mathscr{K}$ whose objects K are finitely generated field extensions of k of transcendence degree 1 with $K \cap \overline{k} = k$, and whose maps are injections fixing k. This correspondence is very important, as it allows one to study properties of morphisms between curves using field theory.

Definition 2.2.1. Let $\phi\colon C_1 \to C_2$ be a k-morphism of smooth curves (so C_1, C_2 and ϕ are defined over k). If ϕ is constant, define its **degree** as $\deg \phi := 0$. Otherwise, say that ϕ is a **finite map,** and that its **degree** is

$$\deg \phi := [k(C_1) : \phi^*(k(C_2))].$$

Say that ϕ is **separable/inseparable/purely inseparable** if the field extension $k(C_1)/\phi^*(k(C_2))$ is separable/inseparable/purely inseparable. Denote the separable and inseparable degrees of the extension $k(C_1)/\phi^*(k(C_2))$ by $\deg_s \phi$ and $\deg_i \phi$, respectively.

Corollary 2.2.4. [Sil09, Corollary II.2.4.1] *Let $\phi\colon C_1 \to C_2$ be a k-morphism of smooth curves. Then ϕ is an isomorphism if* $\deg \phi = 1$.

Given a k-morphism $\phi\colon C_1 \to C_2$ of curves, we saw that we have an induced injection $\phi^*\colon k(C_2) \hookrightarrow k(C_1)$. There is also a "dual map" $k(C_1) \to k(C_2)$ analogous to a norm map.

Definition 2.2.2. Given a k-morphism $\phi\colon C_1 \to C_2$ of curves, we can define the **norm map relative to** ϕ: written as

$$\phi_*\colon k(C_1) \to k(C_2),$$

this is defined via

$$\phi_*(f) := (\phi^*)^{-1}(\mathrm{Nm}_{k(C_1)/\phi^*(k(C_2))}(f))$$

(i.e., given $f \in k(C_1)$, writing $\mathrm{Nm}(f) = \phi^*(g)$ for some unique $g \in k(C_2)$, we set $\phi_*(f) := g$).

The next type of behavior we want to isolate is that of a *ramified point* under a morphism.

Definition 2.2.3. Let $\phi\colon C_1 \to C_2$ be a morphism of smooth curves. For $P \in C_1$, the **ramification index of ϕ at P** is

$$e_\phi(P) := v_P(\phi^*(t_{\phi(P)})),$$

where $t_{\phi(P)} \in k(C_2)$ is a uniformizer at $\phi(P)$ (so $v_{\phi(P)}(t_{\phi(P)}) = 1$). We note that $e_\phi(P) \geq 1$, since $\phi^*(t_{\phi(P)})$ vanishes at P. Say that ϕ is **unramified at** P if $e_\phi(P) = 1$; otherwise, say that ϕ is **ramified at** P**.** if ϕ is unramified at all $P \in C_1$, say that ϕ is **unramified.**

Proposition 2.2.5. [Sil09, Proposition II.2.6] *Let $\phi\colon C_1 \to C_2$ be a morphism of smooth curves.*

a. For all $Q \in C_2$,

$$\sum_{P \in \phi^{-1}(Q)} e_\phi(P) = \deg \phi.$$

b. For all but finitely many $Q \in C_2$,

$$\#\phi^{-1}(Q) = \deg_s(\phi).$$

c. Let $\psi\colon C_2 \to C_3$ be another morphism of smooth curves. Then for all $P \in C_1$,

$$e_{\psi\circ\phi}(P) = e_\phi(P) \cdot e_\psi(\phi(P)).$$

Proof. For part a., see e.g. [Har77, Proposition II.6.9], and for b., see [Har77, Proposition II.6.8].

We will prove part c. Let $t_{\phi(P)}$ and $t_{(\psi\circ\phi)(P)}$ be uniformizers at $\phi(P) \in C_2$ and $(\psi \circ \phi)(P) \in C_3$, respectively. By definition, for points $Q \in C_2$ we have

$$e_\psi(Q) := v_Q(\psi^*(t_{\psi(Q)})).$$

When $Q = \phi(P)$, we thus have

$$e_\psi(\phi(P)) = v_{\phi(P)}(\psi^*(t_{(\psi\circ\phi)(P)})).$$

In particular, the functions $t_{\phi(P)}^{e_\psi(\phi(P))}$ and $\psi^*(t_{(\psi\circ\phi)(P)})$ have the same order at $\phi(P)$ (note that $t_{\phi(P)}$ has order 1 at $\phi(P)$). Applying ϕ^* to both functions and taking orders at P then shows that

$$e_\psi(\phi(P)) \cdot v_P(\phi^*(t_{\phi(P)})) = v_P(\phi^*(\psi^*(t_{(\psi\circ\phi)(P)}))),$$

i.e.,

$$e_\psi(\phi(P)) \cdot e_\phi(P) = v_P((\psi \circ \phi)^*(t_{(\psi\circ\phi)(P)})),$$

i.e.,

$$e_\psi(\phi(P)) \cdot e_\phi(P) = e_{\psi\circ\phi}(P). \qquad \square$$

It is worth noting that part a. of the proposition implies that for a morphism $\phi\colon C_1 \to C_2$, if a point $Q \in C_2$ is such that $\#\phi^{-1}(Q) < \deg \phi$, then ϕ is ramified at a point above Q. This can be phrased as a corollary.

Corollary 2.2.6. [Sil09, Corollary II.2.7] *A morphism $\phi\colon C_1 \to C_2$ of smooth curves is unramified if and only if $\#\phi^{-1}(Q) = \deg\phi$ for all $Q \in C_2$.*

Remark 2.2.1. Our notion of ramification in morphisms is closely related to ramification in number fields. For example, given a number field extension K/F, part a. of Proposition 2.2.5 is analogous to the *efg theorem:* for a nonzero prime ideal $\mathfrak{P} \subseteq F$, writing $\mathfrak{P} = \prod_{i=1}^{g} \mathfrak{Q}_i^{e_i}$ in the ring of integers $\mathcal{O}_K$ where the $\mathfrak{Q}_i$ are the distinct prime ideals above $\mathfrak{P}$, one has

$$\sum_{i=1}^{g} e_i f_i = [K : F],$$

where each $f_i := [\mathcal{O}_K/\mathfrak{Q}_i : \mathcal{O}_F/\mathfrak{P}]$ is the inertial degree of $\mathfrak{Q}_i$ over $\mathfrak{P}$. Part b. of the proposition is analogous to the fact that finitely many prime ideals ramify in K/F, and part c. is identical to transitivity of ramification indices in towers of extensions $L/K/F$. Both concepts of ramification are connected by the theory of Dedekind domains, and the fact that the extensions $k(C_1)/\phi^*(k(C_2))$ and K/F are finite. For more on arithmetic geometry and algebraic number theory from the perspective of Dedekind domains, see e.g. Lorenzini's "An invitation to arithmetic geometry" [Lor96].

Here is an example in which we compute ramification indices under a morphism of curves. This is an example of applying local techniques to analyze projective varieties.

Example 2.2.2. Consider the $\mathbb{Q}$-morphism $\phi\colon \mathbb{P}^1 \dashrightarrow \mathbb{P}^1$ defined by

$$\phi([X : Y]) := [X^3(X - Y)^2 : Y^5].$$

We claim that ϕ is ramified at the point $P := [0 : 1]$. To prove this, we can do the following: determine a uniformizer t at $\phi(P)$; pull this uniformizer back to a rational function $f_t := \phi^*(t)$ on $\mathbb{P}^1$ under ϕ; compute a uniformizer s at P on the first $\mathbb{P}^1$; and then compute $v_s(f_t)$, showing that this valuation is > 1. Since both curves are the same, our uniformizer analysis is simplified.

Give the coordinates X, Y to $\mathbb{P}^1$. Since $\phi(P) = [0 : 1]$ is in the affine patch $U(Y)$ of $\mathbb{P}^1$, we can compute the uniformizer of $\phi(P)$ in $U(Y)$ (locally). In this patch, we have that P corresponds to the point $P_Y := 0$ on $\mathbb{A}^1$; the coordinate ring of $U(Y)$ is $\overline{\mathbb{Q}}[t]$, where $t := \frac{X}{Y}$. It is clear that the maximal ideal M_{P_Y} is generated by (t), i.e., t is a uniformizer at P_Y. This corresponds to the rational function $\frac{X}{Y} \in \overline{\mathbb{Q}}(\mathbb{P}^1)$, which is a uniformizer at P.

Next, we observe that $\phi^*\left(\frac{X}{Y}\right) = \frac{X^3(X-Y)^2}{Y^5}$. Since $\phi(P) = P$, the preceding paragraph implies that $\frac{X}{Y}$ is a uniformizer at P. Thus, to compute $e_\phi(P)$, we must compute the valuation $v_{X/Y}\left(\frac{X^3(X-Y)^2}{Y^5}\right)$. Since

$$\frac{X^3(X-Y)^2}{Y^5} = \left(\frac{X}{Y}\right)^3 \cdot \left(\frac{X-Y}{Y}\right)^2,$$

with $\frac{X-Y}{Y}$ defined and nonzero at P, we check that

$$v_{X/Y}\left(\frac{X^3(X-Y)^2}{Y^5}\right) = v_{X/Y}\left(\left(\frac{X}{Y}\right)^3\right) + v_{X/Y}\left(\left(\frac{X-Y}{Y}\right)^2\right) = 3 + 0 = 3.$$

We conclude that $e_\phi(P) = 3$, whence ϕ is ramified at P.

Notes Exercise 2.2.1. In the example above, show that ϕ is also ramified at $Q := [1:1] \in \mathbb{P}^1$, and compute $e_\phi(Q)$ directly.

To wrap this section up, we will briefly discuss the *Frobenius morphism.* This is an important morphism defined on varieties which always shows up when k has positive characteristic. (We will discuss the Frobenius morphism more in the next chapter.)

Definition 2.2.4. Let $p := \text{char}(k) > 0$, and fix a power $q := p^r$ of p. Given a polynomial $F \in k[X_0, \ldots, X_n]$, let $F^{(q)}$ be the polynomial obtained by raising the coefficients of F to the q'th power.

Given a curve $C_{/k}$ defined by homogeneous F, we obtain a new curve $C^{(q)}$ defined by $F^{(q)}$, also defined over k. The map

$$F_q \colon C \to C^{(q)}$$

via

$$F_q([x_0 : x_1 : \ldots : x_n]) := [x_0^q : x_1^q : \ldots : x_n^q]$$

is called the **q-power Frobenius morphism.**

Notes Exercise 2.2.2. Verify that q-power Frobenius maps C to $C^{(q)}$.

Here are some basic properties of the q-power Frobenius morphism.

Proposition 2.2.7. [Sil09, Proposition II.2.11] *Let $p := \text{char}(k) > 0$, and fix a power $q := p^r > 1$. Let $C_{/k}$ be a curve, and let $F_q \colon C \to C^{(q)}$ be q-power Frobenius.*

a. $F_q^*(k(C^{(q)})) = k(C)^q := \{f^q : f \in k(C)\}$;
b. F_q *is purely inseparable;*
c. $\deg(F_q) = q$.

(We are assuming that k is perfect here; if k is not perfect, then b. and c. still hold, but a. must be modified.)

For some properties of purely inseparable extensions, see Exercise 2.2.3.

Corollary 2.2.8. [Sil09, Corollary II.2.12] *When $p := \text{char}(k) > 0$, every morphism $\psi \colon C_1 \to C_2$ factors as*

$$C_1 \xrightarrow{F_q} C_1^{(q)} \xrightarrow{\lambda} C_2$$

where F_q is the q-power Frobenius morphism for $q := \deg_i(\psi)$, and λ is a separable morphism.

Exercise 2.2.1. Consider the elliptic curve

$$E_{/\mathbb{Q}} : Y^2Z = X^3 + Z^3.$$

We have a $\mathbb{Q}$-morphism $\phi \colon E \to \mathbb{P}^1$ given by projection,

$$\phi := [X : Z].$$

a. Prove that $[\mathbb{Q}(E) : \phi^*(\mathbb{Q}(\mathbb{P}^1))] = 2$.
b. Prove that ϕ is ramified at $P := [-1 : 0 : 1]$.
c. Argue that P is the only ramified point of ϕ above $\phi(P)$.

d. (Optional) Using visuals, explain what ϕ being ramified at P means in this example.

(*Hint for all parts:* do things locally!)

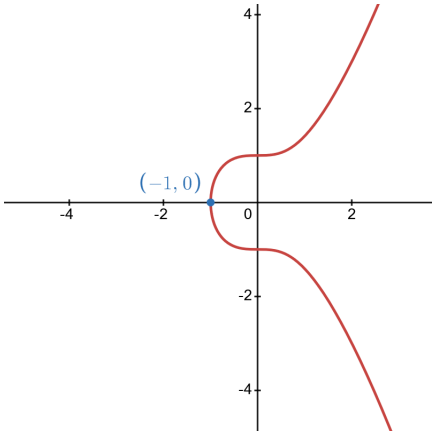


FIGURE 2.2.1. The elliptic curve $E : y^2 = x^3 + 1$.

Exercise 2.2.2. [Sil09, Exercise 2.2] Let $\phi\colon C_1 \to C_2$ be a morphism of smooth curves. Let $g \in \overline{k}(C_2)^\times$, and let $P \in C_1$. Prove that

$$v_P(\phi^*(g)) = e_\phi(P) \cdot v_{\phi(P)}(g).$$

Exercise 2.2.3. This exercise proves some properties about the Frobenius morphism; see also Proposition 2.2.7 ([Sil09, Proposition II.2.11]). It also serves as a review of inseparable extensions.

Recall that an algebraic field extension K/F is **separable** if for any element $\alpha \in K$, the minimal polynomial $m(x) \in F[x]$ of α over F has no repeated roots; this is equivalent to $\gcd(m(x), m'(x)) = 1$. If all elements $\alpha \in K$ have minimal polynomials over F with repeated roots, then K/F is said to be **purely inseparable.**

a. Show that if K/F is not separable, then $\mathrm{char}(K)=\mathrm{char}(F) > 0$.
b. Show that the following are equivalent:
   1. K is purely inseparable over F;
   2. for all $\alpha \in K$, there exists $n \geq 0$ with $\alpha^{p^n} \in F$;
   3. each $\alpha \in K$ has a minimal polynomial over F of the form $x^{p^n} - a$ for some $n \in \mathbb{Z}_{\geq 0}$ and some $a \in F$.

Let k be a field with $p := \mathrm{char}(k) > 0$. Fix a power $q := p^r$, as well as a curve $C_{/k}$. Prove the following:

c. $F_q^*(k(C^{(q)})) = k(C)^q := \{f^q : f \in k(C)\}$.
d. F_q is purely inseparable.
e. $\deg(F_q) = q$.

For more on separable and inseparable extensions, see these notes from Conrad: `https://kconrad.math.uconn.edu/blurbs/galoistheory/separable1.pdf`.

2.3. **Divisors.** In this section, we will study *divisors* of curves. Understanding the divisors on an elliptic curve is very important: it will allow us to describe the group law on an elliptic curve in terms of their divisors, which will be useful for us when understanding their morphisms.

Definition 2.3.1. For a given curve C, the **divisor group of** C is the free abelian group $\mathrm{Div}(C)$ generated by the points of C. Its elements are called **divisors,** which have the form

$$D = \sum_{P \in C} n_P \cdot (P),$$

where each $n_P \in \mathbb{Z}$, and $n_P = 0$ for all but finitely many $P \in C$.

Each divisor $D \in \mathrm{Div}(C)$ has a well-defined **degree:** if

$$D = \sum_{P \in C} n_P \cdot (P),$$

then

$$\deg(D) := \sum_{P \in C} n_P.$$

We let $\mathrm{Div}^0(C)$ denote the **degree** 0 **divisor group of** C**,** consisting of divisors $D \in \mathrm{Div}(C)$ with $\deg(D) = 0$.

Finally, if C is defined over k, then there is a natural action of $G_k := \mathrm{Gal}(\overline{k}/k)$ on $\mathrm{Div}(C)$: for each $\sigma \in G_k$ and $D := \sum_{P \in C} n_P \cdot (P) \in \mathrm{Div}(C)$, we set

$$\sigma(D) := \sum_{P \in C} n_P \cdot (\sigma(P))$$

(also see Notes Exercise 1.2.4). Say that a divisor $D \in \mathrm{Div}(C)$ is **defined over** k**,** or is k**-rational,** if D is fixed under this action, i.e., $\forall \sigma \in G_k$ we have $\sigma(D) = D$. We denote the group of k-rational divisors of C by $\mathrm{Div}_k(C)$; we have a similar definition for $\mathrm{Div}^0_k(C)$.

Remark 2.3.1. Note that for a curve $C_{/k}$, a k-rational point $P \in C(k)$ induces a k-rational divisor $(P) \in \mathrm{Div}_k(C)$. *However,* there can also be rational divisors which are not a sum of k-rational points! See the notes exercise below.

Notes Exercise 2.3.1. Consider the curve $C_{/\mathbb{Q}} : y = x^2 - 5$. Show that the divisor $D := ((\sqrt{5}, 0) + (-\sqrt{5}, 0))$ is $\mathbb{Q}$-rational.

We can also associate divisors to rational functions on a smooth curve.

Definition 2.3.2. Let C be a smooth curve and $f \in \overline{k}(C)$. Then f has an associated divisor, given by its order of vanishing at points:

$$\mathrm{div}(f) := \sum_{P \in C} v_p(f) \cdot (P).$$

This sum is finite since f has finitely many zeros and poles, see Proposition 2.1.2 ([Sil09, Proposition II.1.2]).

Notes Exercise 2.3.2. If C is a curve defined over k, then show that for $\sigma \in G_k$ we have

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

Deduce that for $f \in k(C)$, one has $\operatorname{div}(f) \in \operatorname{Div}_k(C)$.

Notes Exercise 2.3.3. Show that the map $\operatorname{div}\colon \overline{k}(C)^\times \to \operatorname{Div}(C)$ is a homomorphism.

The above notes exercise is in analogy to sending an element of a number field to its fractional ideal. In fact, this analogy goes much farther, see Notes Exercise 2.3.6.

Here are facts about divisors of rational functions on a smooth curve.

Proposition 2.3.1. [Sil09, Proposition II.3.1] *Let C be a smooth curve and $f \in \overline{k}(C)^\times$.*

a. One has $\operatorname{div}(f) = 0$ iff $f \in \overline{k}^\times$.
b. $\deg(\operatorname{div}(f)) = 0$.

Proof. For part b., we cite [Har77, Corollary II.6.10]. For part a., observe that if $\deg(f) = 0$, then f has no poles, and thus the corresponding morphism $\phi\colon C \to \mathbb{P}^1$ via

$$\phi(P) = \begin{cases} [f(P) : 1] & \text{if } f \text{ is regular at } P, \\ [1 : 0] & \text{if } f \text{ has a pole at } P \end{cases}$$

misses $[1 : 0]$, hence is not surjective. But then Theorem 2.2.2 ([Sil09, Theorem II.2.3]) implies that this map is constant, and thus $f \in \overline{k}^\times$. The converse is clear. □

Here is an important example of computing divisors on an elliptic curve.

Example 2.3.1. Assume that $\operatorname{char}(k) \neq 2$, and consider an elliptic curve of the form

$$E : y^2 = (x - e_1)(x - e_2)(x - e_3)$$

where $e_1, e_2, e_3 \in \overline{k}$ are distinct. Our coordinate ring of E (on the affine patch E_Z, where $Z \neq 0$) is

$$\overline{k}[E] := \frac{\overline{k}[x, y]}{(y^2 - (x - e_1)(x - e_2)(x - e_3))}.$$

(For this example, and for the rest of these notes, we will simply write x instead of $\overline{x}$, etc.)

Let us compute $\operatorname{div}(y)$. For $P \notin \{(e_1, 0), (e_2, 0), (e_3, 0), O\}$, it can be checked that $y(P) \neq 0$ since P has nonzero y-coordinate, and thus $v_P(y) = 0$.

For each $1 \leq i \leq 3$, we claim that y is a uniformizer at $P_i := (e_i, 0)$. To show this, we must show for $M_{P_i} := (x - e_i, y) \subseteq \overline{k}[E]$ that $M_{P_i}\overline{k}[E]_{P_i} = (y)\overline{k}[E]_{P_i}$. Equivalently, we must show there exists a rational function $f \in \overline{k}(E)$ defined and nonzero at P_i, such that $x - e_i = y \cdot f$. Let us write $f := (x - e_j)(x - e_k)$ where $j, k \in \{1, 2, 3\}$ do not equal i. Then in $\overline{k}[E]$, we have $y^2 = (x - e_i) \cdot f$; since $f(P_i) = (e_i - e_j)(e_i - e_k) \neq 0$, we find that f is defined and nonzero at P_i, and thus is invertible in $\overline{k}[E]_{P_i}$. We deduce that M_{P_i} is generated by y in the local ring $\overline{k}[E]_{P_i}$, whence y is a uniformizer at P_i, i.e., $v_{P_i}(y) = 1$.

Finally, to compute $v_O(y)$, we must find a uniformizer at $O := [0:1:0]$. We will do this on an affine patch where O is contained in; since

$$E : Y^2Z = (X - e_1Z)(X - e_2Z)(X - e_3Z),$$

we have that O corresponds to $(0,0)$ in the affine patch $E_Y := E \cap U(Y)$. Thus,

$$M_O = (x', z') \subseteq \overline{k}[E_Y] := \frac{\overline{k}[x', z']}{(z' - (x' - e_1z')(x' - e_2z')(x' - e_3z'))}$$

where $x' := \frac{X}{Y}$ and $z' := \frac{Z}{Y}$. We see that x' is a uniformizer at O, by checking that $x' \notin M_O^2 = (x'^2, x'z', z'^2)$.

Let us also compute $v_O(z')$. Since each $x' - e_iz' \in M_O$ and $z' = (x' - e_1z')(x' - e_2z')(x' - e_3z')$ in $\overline{k}[E_Y]$, it follows that $z' \in M_O^3$, i.e., $v_O(z') \geq 3$. Using the defining equation, one can write

$$x'^3 = z' \cdot (1 + ax'^2 - bx'z' + cz'^2)$$

for some $a, b, c \in k(e_1, e_2, e_3)$. Since $(1 + ax'^2 - bx'z' + cz'^2)$ is defined and nonzero at O, this implies that $3v_O(x') = v_O(z')$. We thus have $v_O(z') = 3$. This also implies that $v_O(x' - e_iz') = 1$.

The uniformizer x' on E_Y above corresponds to $\frac{X}{Y} \in \overline{k}(E)$. Therefore, on E_Z we have

$$v_O(y) := v_{X/Y}\left(\frac{Y}{Z}\right).$$

To compute this, we note that the relation

$$Y^2Z = (X - e_1Z)(X - e_2Z)(X - e_3Z)$$

gives

$$\frac{Z}{Y} = \prod_{i=1}^{3}\left(\frac{X - e_iZ}{Y}\right).$$

Taking valuations gives

$$v_{X/Y}\left(\frac{Y}{Z}\right) = -\sum_{i=1}^{3} v_{X/Y}\left(\frac{X - e_iZ}{Y}\right).$$

Since each $v_{X/Y}\left(\frac{X-e_iZ}{Y}\right) = v_O(x' - e_iz') = 1$, we conclude that $v_O(y) = -3$. In particular, we conclude with

$$\mathrm{div}(y) = (P_1) + (P_2) + (P_3) - 3(O).$$

Notes Exercise 2.3.4. Continuing the above example, show that for each $1 \leq i \leq 3$ one has $v_O(x - e_i) = -2$. What is $v_O(x)$?

Definition 2.3.3. Let C be a smooth curve. Say a divisor $D \in \mathrm{Div}(C)$ is **principal** if $D = \mathrm{div}(f)$ for some $f \in \overline{k}(C)^\times$. By Proposition 2.3.1, the subset of principal divisors of C forms subgroup of $\mathrm{Div}^0(C)$, denoted by $\mathrm{Prin}(C)$.

The **divisor class group** (or **Picard group**) of C is

$$\mathrm{Pic}(C) := \mathrm{Div}(C)/\mathrm{Prin}(C).$$

We say that two divisors $D_1, D_2 \in \mathrm{Div}(C)$ are **linearly equivalent,** and write $D_1 \sim D_2$, if $D_1 - D_2 \in \mathrm{Prin}(C)$, i.e., if $D_1 = D_2 + \mathrm{div}(f)$ for some $f \in \overline{k}(C)^\times$.

Since $\mathrm{Prin}(C) \subseteq \mathrm{Div}^0(C)$, we can also define the **degree 0 divisor class group** (or **degree 0 Picard group**):

$$\mathrm{Pic}^0(C) := \mathrm{Div}^0(C)/\mathrm{Prin}(C).$$

$\mathrm{Pic}^0(C)$ is also sometimes called the **Jacobian of C.**

Finally, suppose that the curve C is defined over k. Then we let $\mathrm{Pic}_k(C)$ denote the subgroup of $\mathrm{Pic}(C)$ fixed by G_k.

The kernel of $\deg\colon \mathrm{Div}(C) \to \mathbb{Z}$ contains $\mathrm{Prin}(C)$, by Proposition 2.3.1. Thus, it descends to a homomorphism on the quotient,

$$\deg\colon \mathrm{Pic}(C) \to \mathbb{Z}.$$

Notes Exercise 2.3.5. Show that for a curve C, the degree map $\deg\colon \mathrm{Pic}(C) \to \mathbb{Z}$ is surjective.

Example 2.3.2. We will show that $\mathrm{Div}^0(\mathbb{P}^1) = \mathrm{Prin}(\mathbb{P}^1)$, i.e., that every degree 0 divisor on $\mathbb{P}^1$ is principal. Give coordinates X, Y to $\mathbb{P}^1$. Observe that any point $P_a := [a : 1] \in \mathbb{P}^1$ has uniformizer $\frac{aY-X}{Y}$; for the remaining point $\infty := [1 : 0] \in \mathbb{P}^1$, we have the uniformizer $\frac{Y}{X}$.

Let $D \in \mathrm{Div}^0(\mathbb{P}^1)$, and write

$$D = n_\infty \cdot (\infty) + \prod_{P_a := [a:1] \in \mathbb{P}^1} n_P \cdot (P)$$

where $\sum_{P \in \mathbb{P}^1} n_P = 0$. We see that the rational function

$$f := \left(\frac{Y}{X}\right)^{n_\infty} \cdot \prod_{P_a := [a:1] \in \mathbb{P}^1} \left(\frac{aY - X}{Y}\right)^{n_{P_a}}$$

satisfies $\mathrm{div}(f) = D$, whence D is principal. (Note that $\sum_{P \in \mathbb{P}^1} n_P = 0$ is a necessary condition for f to be a rational function.)

This shows that the degree map $\deg\colon \mathrm{Pic}(\mathbb{P}^1) \to \mathbb{Z}$ is an injection; combined with Notes Exercise 2.3.5, it is thus an isomorphism $\deg\colon \mathrm{Pic}(\mathbb{P}^1) \xrightarrow{\sim} \mathbb{Z}$. As it turns out, the converse is also true: if C is a smooth curve and $\mathrm{Pic}(C) \cong \mathbb{Z}$, then $C \cong \mathbb{P}^1$.

The following notes exercise provides another analogy to algebraic number theory.

Notes Exercise 2.3.6. Show that for a smooth curve C, there exists an exact sequence

$$1 \to \overline{k}^\times \to \overline{k}(C)^\times \xrightarrow{\mathrm{div}} \mathrm{Div}^0(C) \to \mathrm{Pic}^0(C) \to 0.$$

(This is in direct analogy to the following: for a number field F with integer ring $\mathcal{O}_F$, one has

$$1 \to \mathcal{O}_F^\times \to F^\times \to \mathcal{I}_F \to \mathrm{Cl}(\mathcal{O}_F) \to 1,$$

where $\mathcal{I}_F$ is the monoid of fractional ideals of F and $\mathrm{Cl}(\mathcal{O}_F)$ is its ideal class group.

We will wrap this section up with a description of the interaction between divisors and (induced maps on function fields from) morphisms.

Definition 2.3.4. Given a morphism $\phi\colon C_1 \to C_2$ of smooth curves, we have the pullback homomorphism $\phi^*\colon \overline{k}(C_2) \hookrightarrow \overline{k}(C_1)$. This in turn induces a homomorphism

$$\phi^*\colon \mathrm{Div}(C_2) \to \mathrm{Div}(C_1)$$

via

$$\phi^*((Q)) := \sum_{P \in \phi^{-1}(Q)} e_\phi(P) \cdot (P),$$

and extending linearly. Similarly, the norm map relative to ϕ, denoted as $\phi_*\colon \overline{k}(C_1) \to \overline{k}(C_2)$, induces a homomorphism

$$\phi_*\colon \mathrm{Div}(C_1) \to \mathrm{Div}(C_2)$$

via

$$\phi_*((P)) := (\phi(P)),$$

and extending linearly.

Proposition 2.3.2. [Sil09, Proposition II.3.6] *Let $\phi\colon C_1 \to C_2$ be a morphism of smooth curves.*

a. $\deg(\phi^*(D)) = \deg\phi \cdot \deg(D)$, *for all* $D \in \mathrm{Div}(C_2)$;
b. $\phi^*(\mathrm{div}(f)) = \mathrm{div}(\phi^*(f))$, *for all* $f \in \overline{k}(C_2)^\times$;
c. $\deg(\phi_*(D)) = \deg(D)$, *for all* $D \in \overline{k}(C_1)$;
d. $\phi_*(\mathrm{div}(f)) = \mathrm{div}(\phi_*(f))$, *for all* $f \in \overline{k}(C_1)^\times$;
e. $\phi_* \circ \phi^*(D) = \deg(\phi) \cdot D$ *for all* $D \in \mathrm{Div}(C_2)$;
f. if $\psi\colon C_2 \to C_3$ *is a morphism of smooth curves, then*

$$(\psi \circ \phi)^* = \phi^* \circ \psi^*$$

and

$$(\psi \circ \phi)_* = \psi_* \circ \phi_*.$$

Proof. The proofs for parts a., c., e. and f. are relatively straightforward. For example, in part a., we can assume that $D = (Q)$ for some $Q \in C_2$. Then by definition, $\phi^*(D) := \sum_{P \in \phi^{-1}(Q)} e_\phi(P) \cdot (P)$. Thus,

$$\deg(\phi^*(D)) = \sum_{P \in \phi^{-1}(Q)} e_\phi(P),$$

which equals $\deg(\phi)$ by the "efg theorem" for curves, see Proposition 2.2.5 ([Sil09, Proposition II.2.6]).

For part b., use Exercise 2.2.2 ([Sil09, Exercise 2.2]). Part d. is a norm result from algebraic number theory, see e.g. [Lan94, Chapter 1, Proposition 22]. □

Remark 2.3.2. By the proposition above, both ϕ^* and ϕ_* take principal divisors to principal divisors, and degree 0 divisors to degree 0 divisors. Thus, they induce maps on the degree 0 Picard groups:

$$\phi^*\colon \mathrm{Pic}^0(C_2) \to \mathrm{Pic}^0(C_1)$$

and

$$\phi_*\colon \mathrm{Pic}^0(C_1) \to \mathrm{Pic}^0(C_2).$$

As we will see in the next chapter, for an elliptic curve (E, O), the group $(E(\overline{k}), O)$ is in bijection with $\mathrm{Pic}^0(E)$; and when E is in Weierstrass form, these two groups are isomorphic in a natural way.

Notes Exercise 2.3.7. Use the proposition above to prove Proposition 2.3.1.b ([Sil09, Proposition II.3.1]): that for a smooth curve C and rational function $f \in \overline{k}(C)^\times$, one has $\deg(\mathrm{div}(f)) = 0$.

2.4. **Differentials.** In this section, we will define and list properties of *differentials* on curves. They will help "linearize" problems for us (like what is done in calculus), and help determine which morphisms are separable. Note that inseparable field extensions can appear when studying function fields of positive characteristic, so in particular, when studying curves over positive characteristic fields.

Definition 2.4.1. Let C be a smooth curve. Then the **space of (meromorphic) differential forms on** C, denoted Ω_C, is the $\overline{k}(C)$-vector space generated by formal symbols dx, where $x \in \overline{k}(C)$, subject to the following relations:

1. $d(x + y) = dx + dy$ for all $x, y \in \overline{k}(C)$;
2. $d(xy) = xdy + ydx$ for all $x, y \in \overline{k}(C)$;
3. $da = 0$ for all $a \in \overline{k}$.

The symbols dx are called **differentials,** or **differential forms.**

Clearly, the relations above mimic the usual derivative rules for addition, products and constants. The following notes exercise explores this connection further:

Notes Exercise 2.4.1. Show that for $f \in \overline{k}(C)^\times$:

1. one has $d(f^{-1}) = -f^{-2}df$;
2. for $n \neq 0 \in \mathbb{Z}$, one has $d(f^n) = nf^{n-1}df$;
3. for $g \in \overline{k}(C)^\times$, one has

$$d\left(\frac{f}{g}\right) = \frac{gdf - fdg}{g^2}.$$

Example 2.4.1. Consider the elliptic curve

$$E : y^2 = x^3 + x.$$

Then the differential of the rational function $\frac{x^2}{y} \in \mathbb{Q}(E)$ is

$$d\left(\frac{x^2}{y}\right) = \frac{yd(x^2) - x^2dy}{y^2} = \frac{2xydx - x^2dy}{y^2}.$$

(Note that $\frac{x^2}{y}$ corresponds to the rational function $\frac{X^2}{YZ}$ on the affine patch E_Z; we will often write out rational functions on this patch.)

Notes Exercise 2.4.2. Show that for a curve C in coordinates X, Y, Z with nonempty affine patch C_Z, one has that every differential form df can be expressed as a $\overline{k}(C)$-linear combination of dx and dy, where $x := \frac{X}{Z}$ and $y := \frac{Y}{Z}$. This explains the frequent use of notation dx and dy for arbitrary differentials, instead of df. (The next proposition will state something stronger.)

Given a morphism $\phi\colon C_1 \to C_2$ of smooth curves, the pullback homomorphism $\phi^*\colon \overline{k}(C_2) \hookrightarrow \overline{k}(C_1)$ induces a linear map between differential spaces:

$$\phi^*\colon \Omega_{C_2} \to \Omega_{C_1},$$

via

$$\phi^*\left(\sum f_i dx_i\right) := \sum \phi^*(f_i) d(\phi^*(x_i)).$$

The following proposition will use differentials to determine when a morphism $\phi\colon C_1 \to C_2$ is separable.

Proposition 2.4.1. [Sil09, Proposition II.4.2] *Let C be a smooth curve.*

a. *Ω_C is a one-dimensional $\overline{k}(C)$-vector space.*
b. *Let $f \in \overline{k}(C)$. Then $\{df\}$ is a $\overline{k}(C)$-basis for Ω_C if and only if $\overline{k}(C)/\overline{k}(f)$ is a finite separable extension.*
c. *Let $\phi\colon C_1 \to C_2$ be a morphism of smooth curves. Then ϕ is separable if and only if the pullback $\phi^*\colon \Omega_{C_2} \to \Omega_{C_1}$ is injective, i.e., is nonzero.*

Proof. Parts a. and b. are proven in e.g. [Sha13, Chapter 3, §5.4, Theorem 3.19] and [Sha13, Chapter 3, §5.4, Theorem 3.20], respectively.

We will prove part c. Using parts a. and b., fix an element $y \in \overline{k}(C_2)$ such that Ω_{C_2} has $\overline{k}(C_2)$-basis $\{dy\}$, with $\overline{k}(C_2)/\overline{k}(y)$ a separable extension. Then

$$\begin{aligned}
\phi^*\colon \Omega_{C_2} \to \Omega_{C_1} \text{ is injective} &\Leftrightarrow \phi^*(dy) \neq 0 \\
&\Leftrightarrow d(\phi^*(y)) \neq 0 && \text{(by definition of } \phi^* \text{ on } \Omega_{C_1}) \\
&\Leftrightarrow \{d(\phi^*(y))\} \text{ is a basis for } \Omega_{C_1} && \text{(from a.)} \\
&\Leftrightarrow \overline{k}(C_1)/\overline{k}(\phi^*(y)) \text{ is separable} && \text{(from b.).}
\end{aligned}$$

However, we are also assuming that $\overline{k}(C_2)/\overline{k}(y)$ is separable, and thus so is the image $\phi^*(\overline{k}(C_2))/\phi^*(\overline{k}(y)) = \phi^*(\overline{k}(C_2))/\overline{k}(\phi^*(y))$ after applying ϕ^*. In particular, we deduce that

$$\phi^*\colon \Omega_{C_2} \to \Omega_{C_1} \text{ is injective} \Leftrightarrow \overline{k}(C_1)/\phi^*(\overline{k}(C_2))$$

is separable (since separable degree is transitive), which by definition is iff $\phi\colon C_1 \to C_2$ is separable. □

The next proposition concerns properties of differentials dt where $t \in \overline{k}(C)$ is a uniformizer at a fixed point $P \in C$.

Proposition 2.4.2. [Sil09, Proposition II.4.3] *Let C be a smooth curve, let $P \in C$ and let $t \in \overline{k}(C)$ be a uniformizer at P.*

a. *For all differentials $\omega \in \Omega_C$, $\exists! g \in \overline{k}(C)$, depending on ω and t, such that*

$$\omega = g \cdot dt.$$

We denote $\frac{\omega}{dt} := g$.
b. *If $f \in \overline{k}(C)$ is regular at P, then so is $\frac{df}{dt}$.*

c. *For $\omega \neq 0 \in \Omega_C$, the value*
$$v_P\left(\frac{\omega}{dt}\right)$$
depends only on ω and P, and is independent of t. This value is called the ***order of*** *ω* ***at*** *P,* *and is denoted $v_P(\omega)$.*

d. *Let $x, f \in \overline{k}(C)$ with $x(P) = 0$, and let $p :=$char(k). Then*
- *$v_P(fdx) = v_P(f) + v_P(x) - 1$ if $p = 0$ or $p \nmid v_P(x)$,*
- *$v_P(fdx) \geq v_P(f) + v_P(x)$ if $p > 0$ and $p \mid v_P(x)$.*

e. *Let $\omega \neq 0 \in \Omega_C$. Then $v_P(\omega) = 0$ for all but finitely many $P \in C$.*

Proof. For part b., see [Har77, Comment after Proposition IV.2.1]. Observe that part a. follows from the previous proposition combined with Proposition 2.1.3 ([Sil09, Proposition II.1.4]). More precisely, in part a., we know that $\overline{k}(C)/\overline{k}(t)$ is separable; thus, by Proposition 2.4.1, we have that $\{dt\}$ is a $\overline{k}(C)$-basis for Ω_C, so that for any $\omega \in \Omega_C$ we can write $\omega = g \cdot dt$ for some unique $g \in \overline{k}(C)$. The other parts are proven in [Sil09]. □

By the above proposition, for any differential $\omega \in \Omega_C$, each point $P \in C$ and uniformizer $t \in \overline{k}(C)$ at P, there exists an associated rational function $\frac{\omega}{dt} := g_{\omega,t} \in \overline{k}(C)$, where $\omega = g_{\omega,t} \cdot dt$; there also exists a valuation $v_P(\omega) := v_P\left(\frac{\omega}{dt}\right) := v_P(g_{\omega,t})$ which is independent of t. Thus, there is a **divisor associated to ω,** defined as
$$\text{div}(\omega) := \sum_{P \in C} v_P(\omega) \cdot (P) \in \text{Div}(C).$$

Say a differential $\omega \in \Omega_C$ is **regular** (or **holomorphic**) if $v_P(\omega) \geq 0$ for all $P \in C$. Say ω is **nonvanishing** if $v_P(\omega) \leq 0$ for all $P \in C$.

Since Ω_C is a one-dimensional $\overline{k}(C)$-vector space, for any two nonzero differentials $\omega_1, \omega_2 \in \Omega_C$, there exists $f \in \overline{k}(C)^\times$ with $\omega_2 = f \cdot \omega_1$. It follows that
$$\text{div}(\omega_2) = \text{div}(f) + \text{div}(\omega_1),$$
and thus $\omega_2 \sim \omega_1$ in Div(C). This leads us to the following definition.

Definition 2.4.2. For a smooth curve C, the **canonical divisor class on** C is the coset $[\text{div}(\omega)] := \text{div}(\omega) + \text{Prin}(C) \in \text{Pic}(C)$ for any nonzero differential $\omega \in \Omega_C$. Any divisor in $[\text{div}(\omega)]$ is called a **canonical divisor,** written as K_C.

Therefore, for any smooth curve C, the canonical divisor class of C is the *unique* equivalence class in Pic(C) of divisors of differentials on C. This explains the use of the word canonical.

Example 2.4.2. Here is an example in which we compute the divisor of a differential on $\mathbb{P}^1$; thus, this computes a canonical divisor $K_{\mathbb{P}^1}$ of $\mathbb{P}^1$. Give $\mathbb{P}^1$ coordinates X, Y. On the affine patch $\mathbb{P}^1_Y := U(Y) = \{[a : b] \in \mathbb{P}^1 : b \neq 0\}$, we have the coordinate $t := \frac{X}{Y}$, and on the patch $\mathbb{P}^1_X$, we have the coordinate $s := \frac{Y}{X}$. Observe that $s = \frac{1}{t}$. We can write $\mathbb{P}^1 = \mathbb{P}^1_Y \sqcup \{\infty\}$, where $\infty := [1 : 0]$.

Let us compute div(dt); to do this, for each point $P \in \mathbb{P}^1$ we need to find a uniformizer $t_P \in \overline{k}(\mathbb{P}^1)$ at P, and then compute $v_P(g_P)$ where $g_P \in \overline{k}(\mathbb{P}^1)$ satisfies $dt = g_P \cdot d(t_P)$. Given a point $P_a := [a : 1] \in \mathbb{P}^1_Y$, we can check that a uniformizer at P_a is $t - a$. Next,

to determine $g \in \overline{k}(\mathbb{P}^1)$ such that $dt = g \cdot d(t-a)$, we observe that $d(t-a) = dt$; in particular, we can take $g := 1$. It follows that $v_{P_a}(dt) := v_{P_a}(1) = 0$.

For the point at infinity $\infty := [1:0] \in \mathbb{P}^1_X$, a uniformizer at ∞ is $s := \frac{1}{t}$. Thus, we need to find $g \in \overline{k}(\mathbb{P}^1)$ such that

$$dt = g \cdot d\left(\frac{1}{t}\right).$$

We know by Notes Exercise 2.4.1 that $dt\left(\frac{1}{t}\right) = -t^{-2} \cdot dt$; this means we must solve

$$dt = -gt^{-2} \cdot dt.$$

We see that $g := -t^2$ works. We deduce that $v_\infty(dt) := v_\infty(-t^2) = 2v_\infty(t) = -2$ (note that $\frac{1}{t}$ is a uniformizer at ∞).

We conclude that $\operatorname{div}(dt) = -2(\infty)$; this shows that dt is not holomorphic, as it is strictly nonvanishing. By definition, it follows that this is a canonical divisor on $\mathbb{P}^1$. Furthermore, since any nonzero differential $\omega \in \Omega_C$ satisfies $\deg(\operatorname{div}(\omega)) = \deg(dt) = -2$, we conclude that no differential on $\mathbb{P}^1$ is holomorphic.

We will wrap this section up with an example where we compute the canonical divisor of an elliptic curve.

Example 2.4.3. Let $\operatorname{char}(k) \neq 2$, and consider the elliptic curve

$$E : y^2 = (x-e_1)(x-e_2)(x-e_3)$$

where $e_1, e_2, e_3 \in \overline{k}$ are distinct. (We considered divisors on this curve in Example 2.3.1.)

We claim that the canonical divisor *class* $[K_E]$ of E is trivial: i.e., there exists a nonzero differential $\omega \in \Omega_C$ with $\operatorname{div}(\omega) = 0$. This is equivalent to the existence of a trivial canonical divisor, i.e., a differential which is both holomorphic and nonvanishing.

We claim that $\operatorname{div}\left(\frac{dx}{y}\right) = 0$. From Example 2.3.1, we know that $\operatorname{div}(y) = (P_1) + (P_2) + (P_3) - 3(O)$, so it suffices to show that $\operatorname{div}(dx) = \operatorname{div}(y) = (P_1)+(P_2)+(P_3)-3(O)$.

From the relation

$$y^2 = (x-e_1)(x-e_2)(x-e_3),$$

we have

$$2y \cdot dy = [(x-e_2)(x-e_3) + (x-e_1)(x-e_3) + (x-e_1)(x-e_2)]dx,$$

and thus

$$2y \cdot dy = dx \cdot \sum_{i \neq j} (x-e_i)(x-e_j). \tag{3}$$

We can use this to help compute $v_P(dx)$ for certain points $P \in E$.

We will focus on computing $v_{P_i}(dx)$ for each $P_i := (e_i, 0)$, as well as $v_O(dx)$ (we leave the other computations for $v_P(dx)$ as an exercise). Observe that by (3), we have

$$v_{P_i}(dx) = v_{P_i}(2y) + v_{P_i}(dy) - v_{P_i}\left(\sum_{j \neq k} (x-e_j)(x-e_k)\right).$$

As can be checked, we have that $x - e_j$ is a uniformizer at P_i when $j = i$, and $x - e_j$ is defined and nonzero at P_i when $j \neq i$. Thus, the valuation of the latter sum is zero (see Notes Exercise 2.1.1, the "domination principle" of valuations). Thus, we have

$$v_{P_i}(dx) = v_{P_i}(2y) + v_{P_i}(dy).$$

By Example 2.3.1, we know that y is a uniformizer at P_i, and so this simplifies to

$$v_{P_i}(dx) = 1 + v_{P_i}(dy).$$

To compute $v_{P_i}(dy)$, we need to compute $v_{P_i}(g)$ where $dy = g \cdot dt_{P_i}$ with t_{P_i} a uniformizer at P_i. However, y is a uniformizer at P_i, and so we may take $g := 1$ and deduce that $v_{P_i}(dy) = 0$. We conclude that

$$v_{P_i}(dx) = 1.$$

To compute $v_O(dx)$, we need to fix a uniformizer t_O at O, and then find $g \in \overline{k}(E)$ for which $dx = g \cdot dt_O$. We found in Example 2.3.1 that $x' := \frac{X}{Y}$ is a uniformizer at O; this function corresponds to $\frac{x}{y} \in \overline{k}(E_Z)$. Thus, to compute $v_O(dx)$, we need to solve for g in

$$dx = g \cdot d\left(\frac{x}{y}\right).$$

We know by Notes Exercise 2.4.1 that

$$d\left(\frac{x}{y}\right) = \frac{ydx - xdy}{y^2}.$$

Expanding this and using (3) to substitute dy out, we find that

$$d\left(\frac{x}{y}\right) = \frac{2y^2 - x\sum_{i\neq j}(x - e_i)(x - e_j)}{2y^3} \cdot dx,$$

and so we can take

$$g := \frac{2y^3}{2y^2 - x\sum_{i\neq j}(x - e_i)(x - e_j)}.$$

We deduce that

$$v_O(dx) = v_O(2y^3) - v_O\left(2y^2 - x\sum_{i\neq j}(x - e_i)(x - e_j))\right).$$

Since $v_O(y) = -3$ (Example 2.3.1), as well as $v_O(x) = -2$ and each $v_O(x - e_i) = -2$ (Notes Exercise 2.3.4), we have

$$v_O(dx) = -9 - (-6) = -3.$$

We conclude that a canonical divisor of E is

$$\operatorname{div}(dx) = (P_1) + (P_2) + (P_3) - 3(O).$$

We deduce from $\operatorname{div}(dx) = \operatorname{div}(y)$ that

$$\operatorname{div}\left(\frac{dx}{y}\right) = 0.$$

Therefore, all canonical divisors are trivial up to linear equivalence.

2.5. **The Riemann-Roch Theorem.** We conclude this chapter with an important theorem called the *Riemann-Roch Theorem.* This theorem will guarantee the existence of rational functions on a smooth curve, with a prescribed set of zeroes and poles. We will see in Chapter 3 that it will imply any elliptic curve has a defining equation in general Weierstrass form.

We begin with a few definitions. Throughout this section, C denotes a smooth curve.

Definition 2.5.1. Say a divisor $D = \sum_{P \in C} n_P \cdot (P) \in \mathrm{Div}(C)$ is **positive,** or **effective,** if each $n_P \geq 0$; in this case, we will write

$$D \geq 0.$$

For two divisors $D_1, D_2 \in \mathrm{Div}(C)$, we write

$$D_1 \geq D_2$$

if $D_1 - D_2 \geq 0$.

Notes Exercise 2.5.1. Show that if $D_1 \geq D_2$, then $\deg(D_1) \geq \deg(D_2)$. Show that the converse need not hold.

Example 2.5.1. Let $f \in \overline{k}(C)$ be a rational function that is regular everywhere except at a point $P \in C$, with a pole of order at most n at P. This is equivalent to

$$\mathrm{div}(f) \geq -n \cdot (P).$$

Similarly, for a point $Q \in C$, if

$$\mathrm{div}(f) \geq (Q) - n \cdot (P),$$

then f has a zero at Q as well. Thus, these inequalities can be used to describe zeroes and poles of rational functions.

Definition 2.5.2. Given a divisor $D \in \mathrm{Div}(C)$, the **Riemann-Roch space associated to** D is

$$\mathcal{L}(D) := \{f \in \overline{k}(C)^\times : \mathrm{div}(f) \geq -D\} \cup \{0\}.$$

Each Riemann-Roch space $\mathcal{L}(D)$ is a $\overline{k}$-vector space; let us set

$$\ell(D) := \dim_{\overline{k}}(\mathcal{L}(D)).$$

Remark 2.5.1. Intuitively, $\mathcal{L}(D)$ is the collection of rational functions on C whose order of vanishing at points is "no worse" than those which appear in D.

Proposition 2.5.1. [Sil09, Proposition II.5.2] *Let* $D \in \mathrm{Div}(C)$.

a. If $\deg(D) < 0$, *then*

$$\mathcal{L}(D) = 0,$$

and thus $\ell(D) = 0$.

b. $\mathcal{L}(D)$ *is finite-dimensional over* $\overline{k}$.

c. If $D' \in \mathrm{Div}(C)$ *is linearly equivalent to* D, *then*

$$\mathcal{L}(D') \cong \mathcal{L}(D),$$

and thus $\ell(D') = \ell(D)$.

Proof.

a. Let $f \in \mathcal{L}(D)$. For contradiction, suppose $f \neq 0$. Then by Proposition 2.3.1 ([Sil09, Proposition II.3.1]), we have $\deg(\operatorname{div}(f)) = 0$. But since $f \in \mathcal{L}(D)$, we know that
$$\operatorname{div}(f) \geq -D,$$
and thus
$$0 = \deg(\operatorname{div}(f)) \geq \deg(-D) = -\deg(D) > 0,$$
which is impossible. Thus, $f = 0$.
b. See [Har77, Theorem II.5.19], or Exercise 2.5.1.
c. Since $D \sim D'$, we can write $D' = D + \operatorname{div}(g)$ for some $g \in \operatorname{Div}(C)$. Then we have a $\overline{k}$-isomorphism
$$\mathcal{L}(D') \to \mathcal{L}(D)$$
via
$$f \mapsto fg.$$ □

Notes Exercise 2.5.2. Check that the map in part c. is an isomorphism.

Example 2.5.2. Let's study $\mathcal{L}(K_C)$ associated to a canonical divisor K_C. Fix any nonzero differential $\omega_0 \in \Omega_C$; then we can take $K_C := \operatorname{div}(\omega_0)$. For any $f \in \overline{k}(C)^\times$, we have $f \in \mathcal{L}(K_C)$ if and only if
$$\operatorname{div}(f) \geq -K_C = -\operatorname{div}(\omega_0),$$
iff $\operatorname{div}(f\omega_0) \geq 0$, iff $f\omega_0$ is holomorphic. Noting that every element of Ω_C has the form $f\omega_0$, we conclude a $\overline{k}$-isomorphism of vector spaces,
$$\mathcal{L}(K_C) \cong \{\omega \in \Omega_C : \omega \text{ is holomorphic}\}.$$
The dimension $\ell(K_C)$ is an important invariant of C, and shows up in the Riemann-Roch theorem.

Here is the main theorem of this section.

Theorem 2.5.2 (The Riemann-Roch Theorem)**.** [Sil09, Theorem II.5.4] *Let K_C be a canonical divisor on C. Then there exists an integer $g \in \mathbb{Z}_{\geq 0}$, called the* genus *of g, such that for all divisors $D \in \operatorname{Div}(C)$,*
$$\ell(D) - \ell(K_C - D) = \deg(D) - g + 1. \tag{4}$$

Proof. A fancy proof using Serre duality is given in [Har77, Theorem IV.1.3]. For a nice set of notes on Weil's proof of Riemann-Roch (and a nice set of notes on algebraic curves from an algebraic perspective), see "Algebraic curves: an algebraic approach" by Clark [ClaAAA, Theorem 2.11]. □

A number of useful corollaries follow from Riemann-Roch.

Corollary 2.5.3. [Sil09, Corollary II.5.5]

a. $\ell(K_C) = g$.
b. $\deg(K_C) = 2g - 2$.
c. If $\deg(D) > 2g - 2$, *then*
$$\ell(D) = \deg(D) - g + 1.$$

Proof.

a. Taking $D := 0$ in Equation (4), we get
$$\ell(0) - \ell(K_C) = -g + 1,$$
i.e.,
$$\ell(K_C) = g - 1 + \ell(0).$$
However, we have
$$\mathcal{L}(0) = \{f \in \overline{k}(C)^\times : \mathrm{div}(f) \geq 0\} \cup \{0\} = \overline{k}$$
since any rational function without poles is constant, see Proposition 2.1.2 ([Sil09, Proposition II.1.2]). Thus $\ell(0) = 1$, and so (4) simplifies to
$$\ell(K_C) = g.$$

b. Taking $D := K_C$ in (4), we have
$$\ell(K_C) - \ell(0) = \deg(K_C) - g + 1,$$
i.e.,
$$\deg(K_C) = \ell(K_C) + g - 2$$
By part a., we have $\ell(K_C) = g$, hence we deduce that
$$\deg(K_C) = 2g - 2.$$

c. If $\deg(D) > 2g - 2$, then part b. implies $\deg(D) > \deg(K_C)$, so that $\deg(K_C - D) < 0$. Then Proposition 2.5.1 implies that $\ell(K_C - D) = 0$. Thus, (4) becomes
$$\ell(D) = \deg(D) - g + 1. \qquad \square$$

The above corollary shows that each smooth curve C has a well-defined **genus:** this is $g := g(C) := \ell(K_C)$, where $K_C \in \mathrm{Div}(C)$ is a canonical divisor of C.

We now explore the consequences of Riemann-Roch in two examples where we have previously computed canonical divisors. Note that the choice of canonical divisor K_C does not change $\ell(K_C)$, and thus does not change $\ell(K_C - D)$.

Example 2.5.3. In Example 2.4.2, we showed that we have the canonical divisor $K_{\mathbb{P}^1} := \mathrm{div}(dt) = -2 \cdot (\infty)$, where $\infty := [1 : 0]$. Thus, there are no holomorphic differentials on $\mathbb{P}^1$, i.e., $\mathcal{L}(K_{\mathbb{P}^1}) = 0$, i.e., $\ell(K_{\mathbb{P}^1}) = 0$. Therefore, $\mathbb{P}^1$ has genus $g := g(\mathbb{P}^1) = 0$. By Riemann-Roch, this implies that for any $D \in \mathrm{Div}(\mathbb{P}^1)$,
$$\ell(D) - \ell(-2 \cdot (\infty) - D) = \deg(D) + 1.$$
Furthermore, if $\deg(D) > -2 = \deg(K_C)$, then $\ell(-2 \cdot (\infty) - D) = 0$ by part c. of Corollary 2.5.3, and so this becomes
$$\ell(D) = \deg(D) + 1.$$

Example 2.5.4. Let $\mathrm{char}(k) \neq 2$, and consider the elliptic curve
$$E : y^2 = (x - e_1)(x - e_2)(x - e_3)$$
where $e_1, e_2, e_3 \in \overline{k}$ are distinct. We have shown in Example 2.4.3 that we have the canonical divisor $\mathrm{div}\left(\frac{dx}{y}\right) = 0$. It follows that we can take $K_C := \mathrm{div}\left(\frac{dx}{y}\right) = 0$.

Thus, Riemann-Roch implies that $g := g(E) = \ell(0) = 1$, i.e., elliptic curves in short Weierstrass form have genus one. Part c. of Corollary 2.5.3 also implies that if $\deg(D) > 0$, then

$$\ell(D) = \deg(D).$$

Here are several special cases of Riemann-Roch spaces for E:

- Let $P \in E$. Then by the above, $\ell((P)) = 1$. Since $\overline{k} \subseteq \mathcal{L}((P))$, we deduce that $\mathcal{L}((P)) = \overline{k}$. We conclude that there are no rational functions on E with a single pole, and which has order 1. (In general, poles of order 1 are called *simple poles*.)
- For $O := [0 : 1 : 0]$, we have $\ell(2(O)) = 2$. In Notes Exercise 2.3.4, we have shown that the coordinate function $x \in \overline{k}(E)$ has $v_O(x) = -2$. In fact, one can show that x has no other poles, and so $\operatorname{div}(x) \geq -2(O)$, thus $x \in \mathcal{L}(2(O))$. From $\ell(2(O)) = 2$, we conclude that $\mathcal{L}(2(O))$ has $\overline{k}$-basis $\{1, x\}$.
- We also have $\ell(3(O)) = 3$. In Example 2.3.1, we have shown that the coordinate function $y \in \overline{k}(E)$ has $v_O(y) = -3$. One can check that y has no other poles, and thus $y \in \mathcal{L}(3(O))$. It follows that $\{1, x, y\}$ is a basis for $\mathcal{L}(3(O))$.
- We can show that $1, x, y, x^2, xy, y^2, x^3 \in \mathcal{L}(6(O))$; these are 7 rational functions in a 6-dimensional $\overline{k}$-vector space, and so they are $\overline{k}$-linearly dependent. However, we already know this, due to the relation

$$y^2 = (x - e_1)(x - e_2)(x - e_3).$$

The following result says that if C and D are defined over k, then so is $\mathcal{L}(D)$. (This will be useful when we construct Weierstrass equations for "abstract elliptic curves" defined over k in the next chapter.)

Proposition 2.5.4. [Sil09, Proposition II.5.8] *Let C be defined over k and $D \in \operatorname{Div}_k(C)$. Then $\mathcal{L}(D)$ has a $\overline{k}$-basis of rational functions in $k(C)$.*

We wrap this chapter up with a result which relates the genera of two curves connected by a morphism.

Theorem 2.5.5 (Riemann-Hurwitz)**.** [Sil09, Theorem II.5.9] *Let $\phi\colon C_1 \to C_2$ be a separable morphism of smooth curves, and set $g_1 := g(C_1)$ and $g_2 := g(C_2)$. Then*

$$2g_1 - 2 \geq \deg \phi \cdot (2g_2 - 2) + \sum_{P \in C_1} (e_\phi(P) - 1).$$

Furthermore, equality holds if and only if one of the following conditions is true:

a. $\operatorname{char}(k) = 0$.
b. $\operatorname{char}(k) > 0$, *but does not divide $e_\phi(P)$ for any $P \in C_1$.*

Exercise 2.5.1. [Sil09, Exercise 2.4] Let C be a smooth curve and $D \in \operatorname{Div}(C)$. Without using Riemann-Roch, prove the following:

a. $\mathcal{L}(D)$ is a $\overline{k}$-vector space.
b. If $\deg(D) \geq 0$, then

$$\ell(D) \leq \deg(D) + 1.$$

Exercise 2.5.2. [Sil09, Exercise 2.5] Let C be a smooth curve. Prove that the following are equivalent (over $\overline{k}$):

a. C is isomorphic to $\mathbb{P}^1$.
b. C has genus 0.
c. There exist distinct points $P, Q \in C$ with $(P) \sim (Q)$.

Exercise 2.5.3. [Sil09, Exercise 2.6] Let C be a smooth curve of genus one, and fix a base point $P_0 \in C$.

a. Prove that for all $P, Q \in C$ there exists a unique $R \in C$ such that
$$(P) + (Q) \sim (R) + (P_0).$$
Denote this point R by $\sigma(P, Q)$.
b. Prove that the map $\sigma\colon C \times C \to C$ makes C into an abelian group with identity element P_0.
c. Define a map
$$\kappa\colon C \to \mathrm{Pic}^0(C)$$
via
$$P \mapsto [(P) - (P_0)].$$
Prove that κ is a bijection, and thus κ can be used to make C into a group via the rule
$$P + Q := \kappa^{-1}(\kappa(P) + \kappa(Q)).$$
d. Prove that the group operations on C defined in parts b. and c. are the same.

Exercise 2.5.4. [Sil09, Exercise 2.7] Let $F(X, Y, Z) \in k[X, Y, Z]$ be a homogeneous polynomial of degree $d \geq 1$, and assume that the curve $C \subseteq \mathbb{P}^2$ defined by
$$C : F(X, Y, Z) = 0$$
is nonsingular. Prove that
$$g(C) = \frac{(d-1)(d-2)}{2}.$$
(*Hint:* one way to do this is to define a map $C \to \mathbb{P}^1$ and use Riemann-Hurwitz. Another way is to cleverly construct a nonzero differential ω on C, and then use the fact that $\deg(\mathrm{div}(\omega)) = 2g(C) - 2$.)

Exercise 2.5.5. [Sil09, Exercise 2.8] Let $\phi\colon C_1 \to C_2$ be a separable morphism of smooth curves.

a. Prove that $g(C_1) \geq g(C_2)$.
b. Prove that if C_1 and C_2 have the same genus g, then one of the following is true:
   i. $g = 0$.
   ii. $g = 1$ and ϕ is unramified.
   iii. $g \geq 2$ and ϕ is an isomorphism.

Exercise 2.5.6. [Sil09, Exercise 2.13] Let $C_{/k}$ be a smooth curve.

a. Prove that the following sequence is exact:
$$1 \to k^\times \to k(C)^\times \to \mathrm{Div}_k^0(C) \to \mathrm{Pic}_k^0(C).$$

b. Suppose that C has genus one and $C(k) \neq \emptyset$. Prove that the map

$$\mathrm{Div}_k^0(C) \to \mathrm{Pic}_k^0(C)$$

is surjective.

Exercise 2.5.7. [Sil09, Exercise 2.14] For this exercise, we assume that $\mathrm{char}(k) \neq 2$. Let $f(x) \in k[x]$ be a polynomial of degree $d \geq 1$ with nonzero discriminant (see Exercise 0.4.2), let C_0/k be the affine curve given by the equation

$$C_0 : y^2 = f(x) := a_0x^d + a_1x^{d-1} + \ldots + a_{d-1}x + a_d,$$

and let g be the unique integer satisfying $d - 3 < 2g \leq d - 1$.

a. Let C be the closure of the image of C_0 via the map

$$[1 : x : x^2 : \ldots : x^{g+1} : y] \colon C_0 \to \mathbb{P}^{g+2}.$$

Prove that C is smooth, and that the affine piece C_{X_0} is isomorphic to C_0. The curve C is called a *hyperelliptic curve.*

b. Let

$$f^*(v) := v^{2g+2} f\left(\frac{1}{v}\right) := \begin{cases} a_0 + a_1v + \ldots + a_{d-1}v^{d-1} + a_dv^d & \text{if } d \text{ is even,} \\ a_0v + a_1v^2 + \ldots + a_{d-1}v^d + a_dv^{d+1} & \text{if } d \text{ is odd.} \end{cases}$$

Show that C consists of two affine pieces

$$C_0 : y^2 = f(x)$$

and

$$C_1 : w^2 = f^*(v),$$

"glued together" via the maps

$$C_0 \to C_1$$

where

$$(x, y) \mapsto \left(\frac{1}{x}, \frac{y}{x^{g+1}}\right),$$

and

$$C_1 \to C_0$$

where

$$(v, w) \mapsto \left(\frac{1}{v}, \frac{w}{v^{g+1}}\right).$$

c. Calculate the divisor of the differential $\frac{dx}{y}$ on C and use the result to show that C has genus g. Check your answer by applying Riemann-Hurwitz to the map $[1 : x] \colon C \to \mathbb{P}^1$. (Note that Exercise 2.5.4 does not apply, since $C \not\subseteq \mathbb{P}^2$.)

d. Find a basis for the holomorphic differentials on C. (*Hint:* consider the set of differential forms $\{x^i \frac{dx}{y} : i = 0, 1, 2, \ldots\}$. How many elements in this set are holomorphic?)

3. The Geometry of Elliptic Curves

In this chapter, we will study the *geometry* of elliptic curves, which mostly concerns their properties over an algebraically closed field $\overline{k}$. This chapter sets up the foundational theory of elliptic curves, and will apply what we've learned from Chapters 1 and 2. We will continue to assume that our base fields k are perfect.

Recall our original definition of an elliptic curve:

Definition 3.0.1. An **elliptic curve** E is a smooth plane cubic curve $E \subseteq \mathbb{P}^2$ with a fixed point. Thus, in e.g. the x, y-plane it can be written as

$$E : f(x, y) = 0.$$

Say E is *defined over* k if you can choose $f \in k[x, y]$ and the fixed point from k^2.

Here is another definition of an elliptic curve; it is a "coordinate-free" definition.

Definition 3.0.2. An **abstract elliptic curve** E is a smooth curve of genus one with a fixed base point $O \in E$. Say E is *defined over* k if E is defined over k as a curve and $O \in E(k)$.

The first definition implies the second one, see Exercise 2.5.4. As we will see in §3.3, these two definitions are equivalent up to k-isomorphism. In fact, we will show more: if E is an abstract elliptic curve, then there exists an equation for E in $\mathbb{P}^2$ *in general Weierstrass form.* Thus, we are led to first study elliptic curves in Weierstrass form.

3.1. Weierstrass Equations.

In this section, we will define some invariants for elliptic curves in Weierstrass form. As we will see in §3.3, any elliptic curve has a defining equation in Weierstrass form, and if $\mathrm{char}(k) \neq 2, 3$, then they have an equation in short Weierstrass form. Thus, understanding invariants of Weierstrass equations will be useful.

Recall the following definition:

Definition 3.1.1. Say a cubic curve $C \subseteq \mathbb{P}^2$ is in *(general) Weierstrass form* if it is given by an equation

$$C : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$

where $a_1, a_2, a_3, a_4, a_6 \in \overline{k}$. Say C is in *short Weierstrass form* if it is given by

$$C : y^2 = x^3 + Ax + B$$

where $A, B \in \overline{k}$. In either case, say C is *defined over* k if the coefficients lie in k.

When $\mathrm{char}(k) \neq 2$, we can make a linear change of variables to simplify a general Weierstrass equation: given a curve

$$C : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6,$$

we can take $y := \frac{1}{2}(y' - a_1x - a_3)$ to get a new defining equation in coordinates x and y':

$$C := y'^2 = 4x^3 + b_2x^2 + 2b_4x + b_6$$

where $b_2 := a_1^2 + 4a_2$, $b_4 := 2a_4 + a_1a_3$ and $b_6 := a_3^2 + 4a_6$. If we also assume $\mathrm{char}(k) \neq 3$, then we can make a further linear change of variables to get C into short Weierstrass

form: taking $x := \frac{x'-3b_2}{36}$ and $y' := \frac{y''}{108}$, we get an equation for C in coordinates x' and y'', via

$$C : y''^2 = x'^3 - 27c_4x' - 54c_6$$

where $c_4 := b_2^2 - 24b_4$ and $c_6 := -b_2^3 + 36b_2b_4 - 216b_6$.

Notes Exercise 3.1.1. Double-check that for a curve $C_{/k} \subseteq \mathbb{P}^2$ given by

$$C : f(x, y) = 0,$$

a linear change of variables $x := ax' - b$ and $y := cy' - d$ with $a, b, c, d \in k$ gives a k-isomorphism $C \xrightarrow{\sim} C'$, where

$$C' : f(x', y') = 0.$$

Here are some more invariants for a curve in Weierstrass form.

Definition 3.1.2. For a curve in Weierstrass form,

$$C : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6,$$

the **discriminant** of C is

$$\Delta_C := -b_2^2b_8 - 8b_4^3 - 27b_6^2 + 9b_2b_4b_6$$

where $b_8 := a_1^2a_6 + 4a_2a_6 - a_1a_3a_4 + a_2a_3^2 - a_4^2$. One has that C is nonsingular if and only if $\Delta_C \neq 0$, iff C is an elliptic curve.

If $E := C$ above is an elliptic curve, then its j**-invariant** is

$$j(E) := \frac{c_4^3}{\Delta_E},$$

and its **invariant differential** is

$$\omega := \frac{dx}{2y + a_1x + a_3} = \frac{dy}{3x^2 + 2a_2x + a_4 - a_1y}.$$

One has $4b_8 = b_2b_6 - b_4^2$ and $1728\Delta_E = c_4^3 - c_6^2$.

Both the j-invariant and invariant differential of an elliptic curve are very important. The j-invariant will parametrize elliptic curves up to isomorphism, and the invariant differential will "linearize" the group law on an elliptic curve, allowing us to analyze morphisms of elliptic curves more easily.

As you can see, the formulas for invariants of a curve in general Weierstrass form are notationally dense. However, much of it simplifies for curves in short Weierstrass form:

Notes Exercise 3.1.2. Assume that $\mathrm{char}(k) \neq 2$, and let $E \subseteq \mathbb{P}^2$ be an elliptic curve given by

$$E : y^2 = x^3 + Ax + B.$$

Show that $\Delta_E = -16(4A^3 + 27B^2)$ and $j(E) = 1728 \cdot \frac{(4A)^3}{\Delta_E}$.

It may be interesting to ask what type of linear change of variables will take Weierstrass equations to Weierstrass equations, fixing the point at infinity. As it turns out, such a change of variables must have the form

$$x := u^2x' + r, y := u^3y' + u^2sx' + t,$$

where $r, s, t, u \in \overline{k}$ and $u \neq 0$. If we further restrict our attention to a change of variables which preserves *short* Weierstrass form, we end up with

$$x := u^2 x', y := u^3 y'$$

for some $u \in \overline{k}^\times$.

The table shows how the invariants of a curve in Weierstrass form will change under a linear change of variables as above:

$ua_1' = a_1 + 2s$
$u^2 a_2' = a_2 - sa_1 + 3r - s^2$
$u^3 a_3' = a_3 + ra_1 + 2t$
$u^4 a_4' = a_4 - sa_3 + 2ra_2 - (t + rs)a_1 + 3r^2 - 2st$
$u^6 a_6' = a_6 + ra_4 + r^2 a_2 + r^3 - ta_3 - t^2 - rta_1$
$u^2 b_2' = b_2 + 12r$
$u^4 b_4' = b_4 + rb_2 + 6r^2$
$u^6 b_6' = b_6 + 2rb_4 + r^2 b_2 + 4r^3$
$u^8 b_8' = b_8 + 3rb_6 + 3r^2 b_4 + r^3 b_2 + 3r^4$
$u^4 c_4' = c_4$
$u^6 c_6' = c_6$
$u^{12}\Delta' = \Delta$
$j' = j$
$u^{-1}\omega' = \omega$

FIGURE 3.1.1. Change of variable formulas for Weierstrass equations [Sil09].

Observe from this table that the j-invariant does not change under a linear change of variables which preserves Weierstrass form. The j-invariant of an elliptic curve is quite useful: it parametrizes the elliptic curve up to isomorphism.

Proposition 3.1.1. [Sil09, Proposition III.1.4]

a. Two elliptic curves are $\overline{k}$-isomorphic if and only if they have the same j-invariant.
b. For any $j_0 \in \overline{k}$, there exists an elliptic curve whose j-invariant is j_0.

We have shown previously that when $\mathrm{char}(k) \neq 2$, an elliptic curve of the form

$$E : y^2 = (x - e_1)(x - e_2)(x - e_3)$$

has a differential $\omega := \frac{dx}{y}$ which is both holomorphic and nonvanishing, i.e., $\mathrm{div}\left(\frac{dx}{y}\right) = 0$ (see Example 2.4.3). As it turns out, for an elliptic curve in general Weierstrass form, the invariant differential $\omega := \frac{dx}{2y + a_1 x + a_3}$ also has this property:

Proposition 3.1.2. [Sil09, Proposition III.1.5] *For an elliptic curve E in Weierstrass form, the invariant differential ω is holomorphic and nonvanishing, i.e.,* $\mathrm{div}(\omega) = 0$.

We will opt to talk about singular curves at a later date. However, there is one result we need for §3.3 which concerns singular Weierstrass equations.

Proposition 3.1.3. [Sil09, Proposition III.1.6] *If a curve $C \subseteq \mathbb{P}^2$ given by a Weierstrass equation is singular, then there exists a rational map $C \dashrightarrow \mathbb{P}^1$ of degree 1, i.e., the curve C is* birational *to $\mathbb{P}^1$.*[6]

Remark 3.1.1. In the above proposition, since C is singular, we cannot use Corollary 2.2.4 to conclude that C and $\mathbb{P}^1$ are isomorphic. See also Exercise 1.3.

3.2. **The group law.** In this section of [Sil09], Silverman describes the group law on a planar elliptic curve, which we have already done in Chapter 0. In §3.1 and 3.2, Silverman also describes the group law on a *singular* cubic curve given by a Weierstrass equation. We will push our coverage of singular Weierstrass equations to Chapter 7, in the interest of completing the rest of Chapter 3 before Spring break.

Exercise 3.2.1. [Sil09, Exercise 3.3] Assume that $\mathrm{char}(k) \neq 3$, and let $A \in k^\times$. Then Exercise 2.5.4 ([Sil09, Exercise 2.7]) shows that the curve

$$E : X^3 + Y^3 = AZ^3$$

is a curve of genus one, so together with the point $O = [1 : -1 : 0]$, it is an elliptic curve. (See also Exercise 0.7.4.)

a. Prove that three points on E add to O if and only if they are collinear.
b. Let $P := [X : Y : Z]$. Prove the formulas

$$-P = [Y : X : Z]$$

and

$$[2]P = [-Y(X^3 + AZ^3) : X(Y^3 + AZ^3) : X^3Z - Y^3Z].$$

c. Develop an analogous formula for the sum of two distinct points.
d. Prove that E has j-invariant 0.

3.3. **Elliptic curves.** Recall our two definitions of elliptic curve thus far:

1. A smooth cubic curve $E \subseteq \mathbb{P}^2$ with a fixed point (coordinate-full);
2. A smooth curve of genus one with a fixed point (abstract, coordinate-free).

The main goal of this section is to prove that these two definitions are equivalent. In particular, we will show that for an abstract elliptic curve (E, O) defined over k, there exist functions $x, y \in k(E)$ which can be used as coordinate functions to map E isomorphically onto a planar curve in $\mathbb{P}^2$ given by a Weierstrass equation, and under this map $O \mapsto [0 : 1 : 0]$.

Proposition 3.3.1. [Sil09, Proposition III.3.1] *Let (E, O) be an abstract elliptic curve defined over k.*

a. There exist functions $x, y \in k(E)$ such that the map

$$\phi \colon E \to \mathbb{P}^2$$

via

$$\phi = [x : y : 1]$$

[6] A *birational* map is a rational map $\phi \colon V_1 \dashrightarrow V_2$, for which there exists a rational map $\psi \colon V_2 \dashrightarrow V_1$ such that ϕ and ψ are inverses to one another where they are defined.

is a k-isomorphism onto an elliptic curve

$$E' : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6,$$

where each $a_i \in k$, and we also have $\phi(O) = [0 : 1 : 0]$. (The functions x and y are called Weierstrass coordinates *for E.*

b. *Any two Weierstrass equations for E in part a. are related by a linear change of variables of the form*

$$x = u^2x' + r, y = u^3y' + su^2x' + t,$$

where $r, s, t, u \in k$ and $u \neq 0$.

c. *Conversely, every elliptic curve over k in Weierstrass form is an abstract elliptic curve over k, i.e., has genus 1.*

Proof. As noted in Example 2.5.4, since $g(E) = 1$, Riemann-Roch implies for each $n \in \mathbb{Z}^+$ that

$$\ell(n(O)) = n.$$

Thus, $\ell(2(O)) = 2$, and so there exists a nonconstant function $x \in \overline{k}(E)$ such that $\{1, x\}$ is a $\overline{k}$-basis for $\mathcal{L}(2(O))$; furthermore, as E and (O) are defined over k, by Proposition 2.5.4 we can assume that $x \in k(E)$. Similarly, there exists $y \in k(E)$ such that $\{1, x, y\}$ is a $\overline{k}$-basis for $\mathcal{L}(3(O))$.

We claim that x has a pole of exact order 2 at O. By an observation in Example 2.5.4, no rational function on E has a single pole, and which has order 1; however, from $x \in \mathcal{L}(2(O))$, we know that x is regular away from O, which forces $v_O(x) = -2$ (otherwise it is constant, contradicting that $\{1, x\}$ is a $\overline{k}$-basis for $\mathcal{L}(2(O))$). Similarly, y has a pole of exact order 3 at O, noting that the set $\{1, x, y\}$ is $\overline{k}$-linearly independent.

Next, we observe that there are 7 linearly dependent functions in $\mathcal{L}(6(O))$: they are $1, x, y, x^2, xy, y^2, x^3$. Since $\ell(6(O)) = 6$, this forces a nontrivial $\overline{k}$-linear dependence between these functions. In fact, since the k-span of these elements generate a k-vector space of dimension at most 6, there exists a nontrivial k-linear dependence between them: i.e., there exists $A_1, A_2, \ldots, A_7 \in k$ with

$$A_1 + A_2x + A_3y + A_4x^2 + A_5xy + A_6y^2 + A_7x^3 = 0.$$

We claim that $A_6 \neq 0$ and $A_7 \neq 0$: if e.g. $A_7 = 0$, then from

$$A_1 + A_2x + A_3y + A_4x^2 + A_5xy + A_6y^2 = 0,$$

each function in the sum has a different valuation at O. This forces each $A_i = 0$: for example, if $t \in \overline{k}(E)$ is a uniformizer at O, then multiplying the equation by t^6 and then evaluating at O shows that $A_6 = O$. Then multiplying by t^5 and then evaluating at O shows that $A_5 = 0$, and so on, which contradicts not all A_i being zero. We deduce that $A_6 \neq 0$ and $A_7 \neq 0$.

We can replace x by $-A_6A_7x$ and y by $A_6A_7^2y$, and then divide by $A_6^3A_7^4$, to get a nontrivial k-linear dependence

$$a_6 + a_4x + a_3y + a_2x^2 + a_1xy + y^2 + x^3 = 0$$

where each $a_i \in k$; this time, the indices are connected to the valuation of the rational function it is multiplied with. This equation defines a curve $C \subseteq \mathbb{P}^2$ in (by abuse of

notation) coordinates $x := \frac{X}{Z}$ and $y := \frac{Y}{Z}$, and by its construction, we have a surjective rational map

$$\phi\colon E \dashrightarrow C$$

defined over k, via

$$\phi = [x : y : 1].$$

Since E is a smooth curve, this is a k-morphism by Proposition 2.2.1 ([Sil09, Proposition II.2.1]), and since it is nonconstant, it is surjective by Theorem 2.2.2 ([Sil09, Theorem II.2.3]). Furthermore, we have $\phi(O) = [0 : 1 : 0]$ since $v_O(y) < v_O(x) < 0$ (see the proof of Proposition 2.2.1).

Finally, we must show that ϕ is an isomorphism; by Corollary 2.2.4 ([Sil09, Corollary 2.4.1]), it suffices to show that C is smooth and $\deg \phi = 1$. Suppose that $\deg \phi = 1$: we will argue that C is smooth. If C is *not* smooth, then by Proposition 3.1.3 ([Sil09, Proposition III.1.6]) there exists a degree 1 map $\psi\colon C \dashrightarrow \mathbb{P}^1$. Then $\psi \circ \phi\colon E \to \mathbb{P}^1$ is a degree 1 map between smooth curves, which by Corollary 2.2.4 ([Sil09, Corollary II.2.4.1]) forces E and $\mathbb{P}^1$ to be isomorphic. However, this is an impossibility, since $g(E) = 1$ and $g(\mathbb{P}^1) = 0$. We deduce that C is smooth if $\deg \phi = 1$.

Next, we will show that $\deg \phi = 1$: we must show that $[k(E) : k(\phi^*(C))] = 1$, i.e., $[k(E) : k(x, y)] = 1$. Observe that if $[k(E) : k(x)] = 2$ and $[k(E) : k(y)] = 3$, then we must have $[k(E) : k(x, y)] = 1$, and we would be done. To this end, first consider the "projection" map

$$\pi_x\colon E \to \mathbb{P}^1$$

via

$$\pi_x = [x : 1];$$

i.e., for each $P \in E$ we set $\pi_x(P) := [x(P) : 1]$. Observe that $\pi_x(O) = [x(O) : 1] = [1 : 0] =: \infty$, since O is a pole of x. By part a. of Proposition 2.2.5 ([Sil09, Proposition II.2.6]), we have

$$\sum_{P \in \pi_x^{-1}(\infty)} e_{\pi_x}(P) = \deg \pi_x.$$

We claim that $\pi_x^{-1}(\infty) = \{O\}$, and that $e_{\pi_x}(O) = 2$; this would imply that $\deg \pi_x = 2$.

First, if $P \in \pi_x^{-1}(\infty) = \{O\}$, then $[x(P) : 1] = [1 : 0]$, and so x has a pole at P; however, x only has a pole at O, which forces $P = O$. Next, giving $\mathbb{P}^1$ the coordinates X, Y, we can check that a uniformizer at ∞ is $\frac{Y}{X}$, and so $\pi_x^{-1}\left(\frac{Y}{X}\right) = \frac{1}{x}$, which implies that $e_{\pi_x}(O) := v_O\left(\frac{1}{x}\right) = 2$. We deduce that $[k(E) : k(x)] = 2$; similarly, one can show that $[k(E) : k(x, y)] = 3$. This concludes our proof of part a.

For part b., observe that if x, y and x', y' are two pairs of Weierstrass coordinates for E, then from $x, x' \in \mathcal{L}(2(O))$ and $y, y' \in \mathcal{L}(3(O))$, which have bases $\{1, x'\}$ and $\{1, x', y'\}$ respectively, there exist $u_1, u_2 \in k^\times$ and $r, s_2, t \in k$ with

$$x = u_1 x' + r, y = u_2 y' + s_2 x' + t.$$

Since both sets of coordinates satisfy equations where the terms for x^3 (resp. x'^3) and y^2 (resp. y'^2) have coefficient 1, this forces $u_1^3 = 1 = u_2^2$. Setting $u := \frac{u_2}{u_1}$ and $s := \frac{s_2}{u^2}$ gives the desired change of variables.

For part c., we must show that for an elliptic curve

$$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6,$$

we have $g(E) = 1$. We have shown this for an elliptic curve in short Weierstrass form in Example 2.5.4, noting that there exists a trivial canonical divisor, namely $\operatorname{div}\left(\frac{dx}{y}\right) = 0$.

We will do the same for the general Weierstrass form: consider the canonical divisor

$$\omega := \frac{dx}{2y + a_1x + a_3} \in \Omega_E.$$

Then we have seen that $\operatorname{div}(\omega) = 0$ in Proposition 3.1.2. (One can also use Exercise 2.5.4 on the genus formula for a smooth curve in $\mathbb{P}^2$.) □

Corollary 3.3.2. [Sil09, Corollary III.3.1.1] *Let $E_{/k}$ be an elliptic curve with Weierstrass coordinates x, y. Then $k(E) = k(x, y)$ and $[k(E) : k(x)] = 2$.*

In the second half of this section, we will describe the group law of an elliptic curve given by the chord and tangent method, in terms of divisors.

Lemma 3.3.3. [Sil09, Lemma III.3.3] *Let C be a curve of genus one and let $P, Q \in C$. Then*

$$(P) \sim (Q)$$

if and only if $P = Q$.

Proof. First suppose that $(P) = (Q) + \operatorname{div}(f)$ for some $f \in \overline{k}(E)$. Then we can write

$$\operatorname{div}(f) = (P) - (Q).$$

We thus have $\operatorname{div}(f) \geq -(Q)$, and so $f \in \mathcal{L}((Q))$. However, by Riemann-Roch we have $\ell((Q)) = 1$, and so f is constant. Therefore, $\operatorname{div}(f) = 0$, and we have $(P) = (Q)$, i.e., $P = Q$. The converse is clear. □

Here is the proposition which tells us the group law on an elliptic curve (E, O) (abstract or otherwise) is the same as a certain group law on $\operatorname{Pic}^0(E)$.

Proposition 3.3.4. [Sil09, Proposition III.3.4] *Let (E, O) be an elliptic curve.*

a. For any $D \in \operatorname{Div}^0(E)$, there exists a unique point $P \in E$ with

$$D \sim (P) - (O).$$

Call this map $\sigma\colon \operatorname{Div}^0(E) \to E$, i.e., $\sigma(D) = P$.

b. σ is surjective.

c. For $D_1, D_2 \in \operatorname{Div}^0(E)$, one has

$$\sigma(D_1) = \sigma(D_2)$$

if and only if

$$D_1 \sim D_2.$$

Thus, the induced map $\sigma\colon \operatorname{Pic}^0(E) \to E$ is a bijection.

d. The inverse of σ is

$$\kappa\colon E \to \mathrm{Pic}^0(E)$$

via

$$\kappa(P) := [(P) - (O)].$$

e. If E is given by a Weierstrass equation, then (E, O) is a group via the chord and tangent method, and σ and κ are group isomorphisms.

Proof. For part a., observe that by Riemann-Roch, $\ell(D+(O)) = 1$. Thus, we can choose a nonzero element $f \in \mathcal{L}(D+(O))$. Since $\mathrm{div}(f) \geq -D-(O) \Leftrightarrow \mathrm{div}(f)+D+(O) \geq 0$, and since $\deg(\mathrm{div}(f)) = 0$, we claim that this implies

$$\mathrm{div}(f) = -D - (O) + (P) \tag{5}$$

for some point $P \in E$. To see this, write $\mathrm{div}(f) + D + (O) = D'$ for some $D' \in \mathrm{Div}(E)$; since $\deg(D + (O)) = 1$, we have $\deg(D') = 1$. Writing $D' = \sum_{P \in E} n_P \cdot (P)$, we know that $D' = \mathrm{div}(f) + D + (O) \geq 0$, i.e., D' is effective; thus, each $n_P \geq 0$. From $\deg(D') = 1$, this forces $n_P = 0$ for all but one point $P \in E$, which must also have $n_P = 1$. We deduce that $D' = (P)$ for some $P \in E$, whence we conclude that (5) holds.

It follows that $D \sim (P) - (O)$. We also claim this P is unique: if we have $D \sim (P') - (O)$, then $(P) - (O) \sim (P') - (O)$, and thus $(P) \sim (P')$, which by the previous lemma ([Sil09, Lemma III.3.3]) implies that $P = P'$.

For part b., simply observe that for $P \in E$, one has for $D := (P) - (O) \in \mathrm{Div}^0(E)$ that $D \sim (P) - (O)$, and thus $\sigma(D) = P$.

For part c., writing each $\sigma(D_i) := P_i \in E$, one has $D_i \sim (P_i) - (O)$, and thus $D_1 \sim D_2$ if and only if $(P_1) - (O) \sim (P_2) - (O)$, iff $(P_1) \sim (P_2)$, iff (by lemma) $P_1 = P_2$.

Part d. is clear (from our surjectivity check). For part e., it suffices to show that for $P, Q \in E$, one has

$$\kappa(P \oplus Q) = \kappa(P) + \kappa(Q),$$

where $P \oplus Q$ is the group law on (E, O) via the chord and tangent method, and $\kappa(P) + \kappa(Q)$ is addition in $\mathrm{Pic}^0(E)$. This is equivalent to i.e.,

$$[(P \oplus Q) - (O)] = [(P) - (O)] + [(Q) - (O)],$$

i.e.,

$$(P \oplus Q) - (O) \sim (P) + (Q) - 2(O),$$

i.e.,

$$(P \oplus Q) + (O) \sim (P) + (Q).$$

To do this, we will trace through the chord and tangent method and produce rational functions from it. To compute $P \oplus Q$, we first consider the (projective) line $L_{P,Q}$ defined by

$$F(X, Y, Z) : aX + bY + cZ = 0.$$

This line intersects E at a third point $P * Q$. Then we consider the line $L_{P*Q,O}$ defined by

$$G(X, Y, Z) : a'X + b'Y + c'Z = 0.$$

This line intersects E at the third point $P * Q$.

Both lines only intersect E at their 3 respective points; additionally, since the line $Z = 0$ intersects E at O exactly 3 times ($O = [0 : 1 : 0]$ is flex for a Weierstrass equation), we see that

$$\operatorname{div}\left(\frac{F}{Z}\right) = (P) + (Q) + (P * Q) - 3(O)$$

and

$$\operatorname{div}\left(\frac{G}{Z}\right) = (P * Q) + (P \oplus Q) - 2(O).$$

Thus, we find that

$$\operatorname{div}\left(\frac{G}{F}\right) = (P \oplus Q) + (O) - (P) - (Q).$$

We deduce that

$$(P \oplus Q) + (O) \sim (P) + (Q).$$

We conclude that $\kappa\colon E \to \operatorname{Pic}^0(E)$ is a homomorphism, and thus an isomorphism. □

Corollary 3.3.5. [Sil09, Corollary III.3.5] *Let E be an elliptic curve and let $D := \sum_{P\in E} n_P(P) \in \operatorname{Div}(E)$. Then $D \in \operatorname{Prin}(E)$ if and only if*

$$\deg D := \sum_{P\in E} n_P = 0$$

and

$$\sum_{P\in E} n_P P = O,$$

where the second sum is addition in E.

Proof. Before we prove this, let us make an observation. Suppose that we have a divisor $D \in \operatorname{Div}^0(E)$. Then we can write

$$D = \sum_{P\in E} n_P \cdot (P),$$

where

$$\sum_{P\in E} n_P = 0.$$

We check that

$$\begin{aligned} D &= \sum_{P\in E} n_P \cdot ((P) - (O)) + \sum_{P\in E} n_P \cdot (O) \\ &= \sum_{P\in E} n_P \cdot ((P) - (O)) + \left(\sum_{P\in E} n_P\right) \cdot (O) \\ &= \sum_{P\in E} n_P \cdot ((P) - (O)) \qquad\qquad (\text{since } \deg(D) = 0). \end{aligned}$$

By Proposition 3.3.4 ([Sil09, Proposition III.3.4]), we have isomorphisms

$$\sigma\colon \operatorname{Pic}^0(E) \xrightarrow{\sim} E,\ \sigma([D]) := P_D \in E \text{ such that } D \sim (P_D) - (O)$$

and

$$\tau\colon E \xrightarrow{\sim} \mathrm{Pic}^0(E),\ \tau(P) := [(P) - (O)],$$

which are inverse to each other. It follows that

$$\begin{aligned}\sigma([D]) &= \sigma\left(\sum_{P\in E} n_P \cdot [(P) - (O)]\right)\\ &= \sum_{P\in E} n_P \cdot \sigma([(P) - (O)])\\ &= \sum_{P\in E} n_P \cdot \sigma(\tau(P))\\ &= \sum_{P\in E} n_P \cdot P.\end{aligned}$$

We conclude that for any degree 0 divisor $D = \sum_{P\in E} n_P \cdot (P) \in \mathrm{Div}^0(E)$, one has

$$\sigma([D]) = \sum_{P\in E} n_P \cdot P. \tag{6}$$

We now prove the result. For a divisor

$$D := \sum_{P\in E} n_P \cdot (P) \in \mathrm{Div}(E),$$

if $D \in \mathrm{Prin}(E)$ then $\sigma([D]) = \sigma([0]) = O$, which by (6) implies that

$$\sum_{P\in E} n_P \cdot P = O;$$

we also know that $\deg(D) = \sum_{P\in P} n_P = 0$ by Proposition 2.3.1 ([Sil09, Proposition II.3.1]). Conversely, suppose that $D \in \mathrm{Div}(E)$ satisfies both $\sum_{P\in E} n_P = 0$ and

$$\sum_{P\in E} n_P \cdot P = 0.$$

Then the first condition implies that $D \in \mathrm{Div}^0(E)$, which by (6) means that

$$\sigma([D]) = \sum_{P\in E} n_P \cdot P.$$

However, the second condition then implies that $\sigma([D]) = O$, which forces $[D] = [0]$, i.e., $D \in \mathrm{Prin}(E)$. □

We can combine Proposition 3.3.4 with Notes Exercise 2.3.6 and conclude there exists an exact sequence

$$1 \to \overline{k}^\times \to \overline{k}(E)^\times \xrightarrow{\mathrm{div}} \mathrm{Div}^0(E) \xrightarrow{\sigma} E \to 0$$

Furthermore, Exercise 2.5.6 shows that this is also true over k,

$$1 \to k^\times \to k(E)^\times \xrightarrow{\mathrm{div}} \mathrm{Div}^0_k(E) \xrightarrow{\sigma} E(k) \to 0.$$

To wrap this section up, we will prove that the addition law on an elliptic curve over k is a *k-morphism* of elliptic curves.

Theorem 3.3.6. [Sil09, Theorem III.3.6] *Let $E_{/k}$ be an elliptic curve in Weierstrass form. Then the group law*

$$\oplus\colon E \times E \to E$$

is a k-morphism. Additionally, the inverse map

$$\ominus\colon E \to E$$

is a k-morphism.

Proof. If we write our equation as

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6,$$

then the inverse map on points $P = (x, y) \in E$ is

$$\ominus P = (x, -y - a_1x - a_3),$$

see Exercise 0.7.1 (formulas for addition on an elliptic curve in general Weierstrass form). This is clearly a rational map defined over k, and it extends to a k-morphism via Proposition 2.2.1.

Next, fix a point $Q \neq O \in E$, and define the translation-by-Q map $\tau_Q\colon E \to E$ via

$$\tau_Q(P) := P \oplus Q.$$

This is a rational map over k by Exercise 0.7.1. In fact, this is a k-isomorphism, with inverse $R \mapsto R \ominus Q$.

Consider the map

$$\oplus\colon E \times E \to E$$

given by addition. It is a rational map of varieties defined over k, and defined everywhere except possibly at pairs $(P, P), (P, -P), (P, O), (O, P)$.

To tackle this issue, for points $Q_1, Q_2 \in E$, let $\tau_i\colon E \to E$ be translation-by-Q_i for each Q_i. Then we have the composition

$$\phi\colon E \times E \xrightarrow{\tau_1\times\tau_2} E \times E \xrightarrow{\oplus} E \xrightarrow{\tau_1^{-1}} E \xrightarrow{\tau_2^{-1}} E.$$

Under this map ϕ, we have

$$\begin{aligned}(P_1, P_2) &\xrightarrow{\tau_1\times\tau_2} (P_1 + Q_1, P_2 + Q_2)\\ &\xrightarrow{\oplus} P_1 + Q_1 + P_2 + Q_2\\ &\xrightarrow{\tau_1^{-1}} P_1 + P_2 + Q_2\\ &\xrightarrow{\tau_2^{-1}} P_1 + P_2.\end{aligned}$$

Thus, $\phi = \oplus$ wherever they are both defined. Furthermore, as τ_1 and τ_2 are (iso)morphisms, we find that ϕ is defined at all points on $E \times E$, except possibly those of the form $(P - Q_1, P - Q_2), (P - Q_1, -P - Q_2), (P - Q_1, -Q_2), (-Q_1, P - Q_2)$. However, since Q_1, Q_2 were arbitrary and the definition of ϕ is independent of Q_1 and Q_2, we can find a sequence of rational maps

$$\phi_1, \phi_2, \ldots, \phi_n\colon E \times E \to E$$

such that:

1. $\phi_1 = \oplus$ is the addition map in Exercise 0.7.1;
2. For each point $(P_1, P_2) \in E \times E$, some ϕ_i is defined at (P_1, P_2);
3. If both ϕ_i and ϕ_j are defined at (P_1, P_2), then $\phi_i(P_1, P_2) = \phi_j(P_1, P_2)$.

It follows that $\oplus$ is defined everywhere on $E \times E$ – simply choose the right ϕ_i above defined at that point (P_1, P_2), as the preceding discussion shows that $\phi_i(P_1, P_2) = P_1 \oplus P_2$. We conclude that $\oplus$ is a k-morphism. □

From here on out, we will write $+$ instead of $\oplus$ to ease notation.

Exercise 3.3.1. [Sil09, Exercise 3.6] Let C be a smooth curve of genus g, let $P_0 \in C$, and let $n \geq 2g + 1$ be an integer. Choose a basis $\{f_0, \ldots, f_m\}$ for $\mathcal{L}(n(P_0))$, and define a map

$$\phi \colon C \to \mathbb{P}^m$$

via

$$\phi := [f_0 : \ldots : f_m].$$

a. Prove that the image $C' := \phi(C)$ is a curve in $\mathbb{P}^m$.
b. Prove that the map $\phi \colon C \to C'$ has degree one.
c. *Prove that C' is smooth and that $\phi \colon C \to C'$ is an isomorphism.

3.4. **Isogenies.** In this section, we will define an *isogeny* of elliptic curves: these will be the morphisms of curves which are also group homomorphisms. We will give several examples of isogenies, and show that the algebro-geometric definition of an isogeny implies they are group homomorphisms. We will then show that isogenies, being particularly rigid when compared to a general morphism of curves, also satisfy nice general properties.

Definition 3.4.1. Given two elliptic curves (E, O) and (E', O'), an **isogeny** between E and E' is a nonconstant (i.e., surjective) morphism $\phi \colon E \to E'$ satisfying $\phi(O) = O'$. In this case, we say that E and E' are *isogenous.*

Remark 3.4.1. We will call the constant zero map $[0] \colon E \to E'$ via $P \mapsto O'$ the *zero isogeny.* We want to include this since we will put a group structure on the set of isogenies.

For two elliptic curves E and E', let us define

$$\mathrm{Hom}(E, E') := \{\text{isogenies } \phi \colon E \to E'\} \cup \{[0]\}.$$

Given two isogenies $\phi, \psi \in \mathrm{Hom}(E, E')$, the function

$$\phi + \psi \colon E \to E'$$

defined by their pointwise sum is also a morphism: this is because addition on E' is a morphism by Theorem 3.3.6 ([Sil09, Theorem III.3.6]), and $\phi + \psi$ is post-composition of the morphism $\phi \times \psi \colon E \times E \to E' \times E'$ with addition on E'. Therefore, $\mathrm{Hom}(E, E')$ is a group under addition.

In the case where $E = E'$, let us set

$$\mathrm{End}(E) := \mathrm{Hom}(E, E);$$

this is called the **endomorphism ring of E.** When there is no confusion, we will call its elements *endomorphisms.*

We can put a ring structure on $\mathrm{End}(E)$ by defining multiplication of isogenies as composition: i.e., given $\phi, \psi \in \mathrm{End}(E)$, we define $\phi \cdot \psi \colon E \to E$ via

$$(\phi \cdot \psi)(P) := \phi(\psi(P)).$$

The unit group of $\mathrm{End}(E)$ is called the **automorphism group of E,** denoted $\mathrm{Aut}(E)$. This is the group of isomorphisms $\phi \colon E \to E$ with $\phi(O) = O$. When there is no confusion, we will simply call these automorphisms.

For two elliptic curves E and E' defined over k, we let $\mathrm{Hom}_k(E, E')$ be the group of k-rational isogenies from E to E', $\mathrm{End}_k(E)$ the ring of k-rational endomorphisms of E, and $\mathrm{Aut}_k(E)$ the k-rational automorphisms on E.

Example 3.4.1. For the elliptic curve

$$E_{/\mathbb{Q}} : y^2 = x^3 - x,$$

one has the isogeny

$$\phi \colon E \to E$$

via $\phi(x, y) := (-x, iy)$. Thus, $\phi \in \mathrm{End}(E) \smallsetminus \mathrm{End}_{\mathbb{Q}}(E)$.

Notes Exercise 3.4.1. Check in the above example that $\phi^2 = [-1]$. Use this to deduce that ϕ is an automorphism of E.

Example 3.4.2. Here is the important class of endomorphisms. For an elliptic curve E, for each integer $n \in \mathbb{Z}^+$ we have the **multiplication-by-n map**

$$[n] \colon E \to E$$

defined by $[n](P) := nP$. For $n < 0$, we set $[n](P) := n(-P)$. This is a morphism by induction on Theorem 3.3.6 ([Sil09, Theorem III.3.6]); since $[n](O) = O$, it is also an isogeny. Furthermore, if E is defined over k, then so is $[n]$.

Here are some properties of endomorphisms on an elliptic curve.

Proposition 3.4.1. [Sil09, Proposition III.4.2]

a. *Let E be an elliptic curve, and let $n \in \mathbb{Z}$ with $n \neq 0$ in k. Then $[n] \colon E \to E$ is nonconstant, hence surjective.*
b. *For elliptic curves E and E', the group of isogenies $\mathrm{Hom}(E, E')$ is a torsionfree $\mathbb{Z}$-module.*
c. *Let E be an elliptic curve. Then $\mathrm{End}(E)$ is a (not necessarily commutative) ring of characteristic 0 with no zero-divisors.*

Proof. Part a. can be proven using the invariant differential, so we will defer this to the next section. Let us prove parts b. and c. using a.

For part b., let $\phi \in \mathrm{Hom}(E, E')$ be an isogeny. Suppose that for some nonzero $n \in \mathbb{Z}$ we have $n\phi = [0]$. The morphism $n\phi \colon E \to E'$ is equivalent to the composition $E \xrightarrow{\phi} E' \xrightarrow{[n]} E'$; thus, its degree equals

$$\deg([n]) \cdot \deg(\phi) = 0.$$

By part a., since $n \neq 0$ we know that $[n]$ is nonconstant, and thus $\deg([n]) \neq 0$, which forces $\phi = 0$. We deduce that $\mathrm{Hom}(E, E')$ is a torsionfree abelian group.

For part c., part b. shows that $\mathrm{End}(E)$ has characteristic zero, i.e., the map $[\cdot]\colon \mathbb{Z} \to \mathrm{End}(E)$ is injective. If $\phi, \psi \in \mathrm{End}(E)$ satisfy

$$\phi \cdot \psi = [0],$$

then taking degrees implies that

$$\deg(\phi) \cdot \deg(\psi) = 0,$$

which forces $\phi = [0]$ or $\psi = [0]$. We conclude that $\mathrm{End}(E)$ has no nonzero zero-divisors. (Thus, if $\mathrm{End}(E)$ is a commutative ring, then it is an integral domain.) □

Given an elliptic curve E, observe that for integers $n \in \mathbb{Z}^+$, the kernel of the multiplication-by-n map $[n]\colon E \to E$ is precisely the points of order dividing n. This motivates the following definition.

Definition 3.4.2. For an elliptic curve E and integer $n \in \mathbb{Z}^+$, the **n-torsion subgroup of** E is the subset of E of points with order dividing n:

$$E[n] := \{P \in E : [n]P = O\}.$$

The **full torsion group of** E is

$$E[\mathrm{tors}] := \bigcup_{n \geq 1} E[n].$$

If E is defined over k, then $E(k)[n]$ and $E(k)[\mathrm{tors}]$ are the k-rational subgroups of $E[n]$ and $E[\mathrm{tors}]$, respectively.

Example 3.4.3. The torsion points on an elliptic curve are very interesting to study. Over an algebraically closed field, there are infinitely many torsion points. However, over non-algebraically closed fields, this isn't necessarily the case. For example, a classic theorem of Mazur [Maz77] proved that for any elliptic curve $E_{/\mathbb{Q}}$, the group $E(\mathbb{Q})[\mathrm{tors}]$ is isomorphic to one of the following 15 groups:

$$E(\mathbb{Q})[\mathrm{tors}] \cong \begin{cases} \mathbb{Z}/N\mathbb{Z} & N = 1, 2, \ldots, 10, 12, \\ \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/N\mathbb{Z} & N = 1, 2, 3, 4. \end{cases}$$

Remark 3.4.2. We will show in this section that all fibers of a separable isogeny $\phi\colon E \to E'$ have size equal to $\deg(\phi)$; in general, all but finitely fibers of a morphism have this size, see Proposition 2.2.5. In §3.6, we will see that $\deg([n]) = n^2$. Therefore, we will eventually conclude that $\#E[n] = n^2$ when $[n]$ is separable, which is true when $\mathrm{char}(k) = 0$ or $\mathrm{char}(k)$ is coprime to n; we will prove this in §3.5. Thus, in this situation, we can conclude that E has exactly n^2 points of order dividing n over $\overline{k}$. There are other more computational ways to prove this fact, too – see [Sil09, Exercises 3.7, 3.8, 3.9].

Remark 3.4.3. By Proposition 3.4.1, we have an injection $[\cdot]\colon \mathbb{Z} \to \mathrm{End}(E)$. For "most" elliptic curves E, this is an isomorphism, i.e., $\mathrm{End}(E) = \{[n] : n \in \mathbb{Z}\}$. However, it can happen that $\mathrm{End}(E) \supsetneq \mathbb{Z}$, in which case we say that E has **complex multiplication.**

Example 3.4.4. A previous example in this section showed that $E_{/\mathbb{Q}} : y^2 = x^3 - x$ has an endomorphism $\phi(x, y) := (-x, iy) \notin \mathrm{End}_{\mathbb{Q}}(E)$. Writing $[i] := \phi$, we have a map

$$[\cdot] \colon \mathbb{Z}[i] \to \mathrm{End}(E)$$

via $[a + bi] := [a] + [b] \cdot [i]$. As it turns out, this is a ring isomorphism, and so $\mathbb{Z}[i] \cong \mathrm{End}(E)$. Furthermore, we have $\{\pm 1, \pm i\} \cong \mathrm{Aut}(E)$ under this isomorphism. This is an example of a CM elliptic curve, with "CM field" $\mathbb{Q}(i)$.

Example 3.4.5. Here is an example of an isogeny and its *dual* (which we will discuss in detail in §3.6). Let $\mathrm{char}(k) \neq 2$, and fix $a, b \in k$ where $b \neq 0$ and $r := a^2 - 4b \neq 0$. Consider the elliptic curves

$$E_1 : y^2 = x^3 + ax^2 + bx$$

and

$$E_2 : y^2 = x^3 - 2ax^2 + rx;$$

since $b \neq 0$ and $\mathrm{char}(k) \neq 2$, one can double-check that both curves are nonsingular by checking whether the polynomials in x have repeated roots, see Exercise 0.4.1. One has isogenies $\phi \colon E_1 \to E_2$ and $\widehat{\phi} \colon E_2 \to E_1$ given by

$$\phi(x, y) := \left(\frac{y^2}{x^2}, \frac{y(b - x^2)}{x^2} \right)$$

and

$$\widehat{\phi}(x, y) := \left(\frac{y^2}{4x^2}, \frac{y(r - x^2)}{8x^2} \right).$$

Both have degree 2, and in fact $\widehat{\phi} \circ \phi = \phi \circ \widehat{\phi} = [2]$. These isogenies ϕ and $\widehat{\phi}$ are *dual* to each other.

Example 3.4.6. in §2.2, we described the *Frobenius map.* Given a field k of positive characteristic p, for a power $q := p^r$ and a curve $C_{/k}$ defined by $I \subseteq k[X_0, X_1, \ldots, X_n]$, we had a new curve $C^{(q)}$ defined by the ideal $I^{(q)} := \langle F^{(q)} : f \in I \rangle$, where $F^{(q)}$ was the polynomial obtained from raising the coefficients of F to the q'th power. We then had a map $C \to C^{(q)}$ called the *q-power Frobenius morphism,* which was explicitly

$$F_q : [x_0 : \ldots : x_n] \mapsto [x_0^q : \ldots : x_n^q].$$

When $k = \mathbb{F}_q$, the q'th power map on k is the identity; it follows that $C^{(q)} = C$, and so $F_q \in \mathrm{End}_k(C)$. One can check that the set of points in $C(\overline{\mathbb{F}_q})$ fixed by F_q is precisely $C(\mathbb{F}_q)$. As it turns out, this can be used to give a formula for $\#C(\mathbb{F}_q)$, which we will see in the case where $C = E$ is an elliptic curve (§5.1): in particular, the *Hasse-Weil bound* says that $|\#E(\mathbb{F}_q) - q + 1| \leq 2\sqrt{q}$.

Example 3.4.7. Let us make an observation regarding morphisms of elliptic curves. Given an elliptic curve E and a point $Q \in E$, we have a *translation-by-Q* map $\tau_Q \colon E \to E$ by

$$\tau_Q(P) := P + Q.$$

This is an isomorphism, with inverse τ_{-Q}. However, this is not an isogeny unless O.

Given a morphism $\psi\colon E \to E'$, we consider the composition

$$\phi_0\colon E \xrightarrow{\phi} E' \xrightarrow{\tau_{-\phi(O)}} E'.$$

Then ϕ_0 is a morphism, with $\phi_0(O) := \tau_{-\phi(O)}(\phi(O)) = O'$. In particular, $\phi = \tau_{\phi(O)} \circ \phi_0$. We deduce that any morphism of elliptic curves is an isogeny followed by a translation.

Let us now show that any isogeny is also a group homomorphism.

Theorem 3.4.2. [Sil09, Theorem III.4.8] *Let*

$$\phi\colon E \to E'$$

be an isogeny. Then ϕ is a group homomorphism: for all $P, Q \in E$, one has

$$\phi(P+Q) = \phi(P) + \phi(Q).$$

Proof. Assume that ϕ is nonconstant. Then Remark 2.3.2 at the end of §2.3 noted that there exists an induced "norm" map $\phi_*\colon \mathrm{Pic}^0(E) \to \mathrm{Pic}^0(E')$, which was defined for $P \in E$ by

$$\phi_*((P)) := (\phi(P)),$$

and then extended linearly. On the other hand, by Proposition 3.3.4 ([Sil09, Proposition III.3.4]), we have group isomorphisms $\kappa\colon E \to \mathrm{Pic}^0(E)$ and $\kappa'\colon E' \to \mathrm{Pic}^0(E')$, given by e.g.

$$\kappa(P) := [(P) - (O)].$$

Since $\phi(O) = O'$, we have a commutative diagram

$$\begin{array}{ccc} E & \xrightarrow[\kappa]{\cong} & \mathrm{Pic}^0(E) \\ \phi\downarrow & & \downarrow\phi_* \\ E' & \xrightarrow[\kappa']{\cong} & \mathrm{Pic}^0(E') \end{array}$$

Since κ, κ' and ϕ_* are homomorphisms with κ' injective, we conclude that ϕ is a homomorphism (check it!). □

Corollary 3.4.3. [Sil09, Corollary III.4.9] *For an isogeny $\phi\colon E \to E'$, the kernel $\ker\phi = \phi^{-1}(O')$ is a finite subgroup of E.*

Proof. since ϕ is a homomorphism, $\ker\phi$ is a subgroup of E. The size of $\ker\phi$ is at most $\deg\phi$ by Proposition 2.2.5 ([Sil09, Proposition II.2.6]). □

The next result is a collection of implications from the fact that an isogeny is a group homomorphism.

Theorem 3.4.4. [Sil09, Theorem III.4.10] *Let $\phi\colon E \to E'$ be an isogeny.*

a. For every $Q \in E'$,

$$\#\phi^{-1}(Q) = \deg_s(\phi).$$

Furthermore, for every $P \in E$,

$$e_\phi(P) = \deg_i(\phi).$$

b. We have an isomorphism

$$\ker \phi \xrightarrow{\sim} \mathrm{Aut}(\overline{k}(E)/\phi^*(\overline{k}(E')))$$

via

$$R \mapsto \tau_R^*.$$

(Here, $\tau_R\colon E \to E$ is translation by R, and τ_R^* is the automorphism on $\overline{k}(E)$ induced by τ_R.)

c. ϕ is separable if and only if ϕ is unramified. In such a case, one has

$$\#\ker \phi = \deg(\phi),$$

and $\overline{k}(E)/\phi^*(\overline{k}(E'))$ is Galois.

Proof. We will only prove part a.; the other parts are also proven in [Sil09]. By Proposition 2.2.5 ([Sil09, Proposition II.2.6]), we know that $\#\phi^{-1}(Q) = \deg_s(\phi)$ for all but finitely many points $Q \in E'$. We claim that all of the sets $\phi^{-1}(Q)$, for $Q \in E'$, are in bijection. To see this, fix $Q, Q' \in E$; since $\phi\colon E \to E'$ is surjective, there exists $R \in E$ with $\phi(R) = Q' - Q$. It follows that for all $P \in \phi^{-1}(Q)$, we have

$$\phi(P+R) = \phi(P) + \phi(R) = Q + (Q' - Q) = Q',$$

since ϕ is a homomorphism. In particular, translation-by-R induces a map

$$\tau_R\colon \phi^{-1}(Q) \to \phi^{-1}(Q').$$

Since we also have the inverse map $\tau_{-R}\colon \phi^{-1}(Q') \to \phi^{-1}(Q)$, we deduce that $\#\phi^{-1}(Q) = \#\phi^{-1}(Q')$.

For the second part of a., fix any point $Q \in E'$, and let $P, P' \in \phi^{-1}(Q)$. Let us set $R := P' - P$. Then $\phi(R) = O$, and thus $\phi \circ \tau_R = \phi$ (this just shows that for any element $R \in \ker \phi$, one has $\phi \circ \tau_R = \phi$). Then by Proposition 2.2.5 ([Sil09, Proposition II.2.6]), we have

$$\begin{aligned} e_\phi(P) &= e_{\phi\circ\tau_R}(P) \\ &= e_{\tau_R}(P) \cdot e_\phi(\tau_R(P)) \\ &= e_\phi(\tau_R(P)) \qquad\qquad (\text{since } \deg(\tau_R) = 1) \\ &= e_\phi(P+R) \\ &= e_\phi(P'). \end{aligned}$$

We deduce that the ramification index in any fiber $\phi^{-1}(Q)$ is constant. Thus, by Proposition2.2.5, the formula

$$\sum_{P \in \phi^{-1}(Q)} e_\phi(P) = \deg(\phi)$$

becomes

$$(\#\phi^{-1}(Q)) \cdot e_\phi(P) = \deg(\phi).$$

By part a., this simplifies to

$$\deg_s(\phi) \cdot e_\phi(P) = \deg(\phi).$$

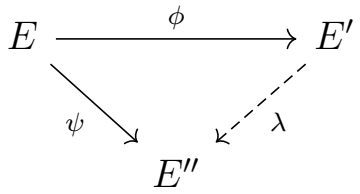
However, since $\deg(\phi) = \deg_s(\phi) \cdot \deg_i(\phi)$, we deduce that

$$e_\phi(P) = \deg_i(\phi).$$

Since $Q \in E'$ was arbitrary, this concludes part a. □

There are a number of interesting consequences from the fact that a separable isogeny $\phi\colon E \to E'$ induces a Galois extension $\overline{k}(E)/\phi^*(\overline{k}(E'))$. One of these is the following:

Corollary 3.4.5. [Sil09, Corollary III.4.11] *Let $\phi\colon E \to E'$ and $\psi\colon E \to E''$ be isogenies, and assume that ϕ is separable. If $\ker\phi \subseteq \ker\psi$, then there exists a unique isogeny $\lambda\colon E' \to E''$ such that the following diagram commutes:*



Here is a "converse" result, which shows that given a finite subgroup of E, there exists a separable isogeny from E whose kernel is this subgroup:

Proposition 3.4.6. [Sil09, Proposition III.4.12] *Let E be an elliptic curve and $C \subseteq E$ a finite subgroup. Then there exists an elliptic curve E' unique up to isomorphism, and a separable isogeny $\phi\colon E \to E'$, such that*

$$\ker\phi = C.$$

(We sometimes write $E/C := E'$.)

Remark 3.4.4. One can show a bit more in the proposition above. For an elliptic curve $E_{/k}$, say that a subgroup $C \subseteq E$ is *k-rational* if it is stable under the action of G_k, i.e., if for all $R \in C$ and for all $\sigma \in G_k$, one has $\sigma(R) \in C$. Then the curve E' in the proposition above can be defined over k, and so can the isogeny ϕ. See [Sil09, Exercise 3.13].

3.5. **The invariant differential.** In this section, we will discuss some properties of the invariant differential of an elliptic curve, and some of their consequences. As mentioned in §2.4, differentials provide a nice way of determining whether morphisms of smooth curves are separable. We will use them to determine when a multiplication-by-n map is separable, as well as when an auxiliary map of q-power Frobenius is separable (which will be useful for proving the Hasse-Weil bound in Chapter 5).

Recall from §3.1 that for an elliptic curve

$$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6,$$

its *invariant differential* is

$$\omega := \frac{dx}{2y + a_1x + a_3} \in \Omega_E.$$

We've cited that it has no zeroes or poles in Proposition 3.1.2 ([Sil09, Proposition III.1.5]), i.e., $\operatorname{div}(\omega) = 0$. Next, we will see that it is invariant under the pullback of

translation maps. Recall that for a morphism $\phi\colon C_1 \to C_2$ of smooth curves, we have a pullback map $\phi^*\colon \Omega_{C_2} \to \Omega_{C_1}$ on differentials via

$$\phi^*\left(\sum f_i dx_i\right) := \sum \phi^*(f_i) d(\phi^*(x_i)).$$

Proposition 3.5.1. [Sil09, Proposition III.5.1] *Let E and ω be as above, and for a point $Q \in E$, let $\tau_Q\colon E \to E$ be the translation-by-Q map. Then for all $Q \in E$, we have*

$$\tau_Q^*(\omega) = \omega.$$

This proposition can be used to prove the following result.

Theorem 3.5.2. [Sil09, Theorem III.5.2] *Let E and E' be elliptic curves, let ω be an invariant differential on E,*[7] *and let*

$$\phi, \psi\colon E \to E'$$

be isogenies. Then

$$(\phi + \psi)^*(\omega) = \phi^*(\omega) + \psi^*(\omega).$$

This proof is also in [Sil09]; however, despite being an important theorem, it is a bit tedious to prove, so we forgo a proof of it here. Let us observe some important consequences of this theorem instead.

Corollary 3.5.3. [Sil09, Corollary III.5.3] *Let ω be an invariant differential on an elliptic curve E, and let $n \in \mathbb{Z}$. Then*

$$[n]^*(\omega) = n\omega.$$

Proof. When $n > 1$, we observe that

$$\begin{aligned}
[n]^*(\omega) &= [(n-1)+1]^*(\omega) \\
&= [n-1]^*(\omega) + \omega && \text{(by Theorem 3.5.2)} \\
&= (n-1)\omega + \omega && \text{(by induction)} \\
&= n\omega.
\end{aligned}$$

Clearly $[0]^*(\omega) = 0$. If $n < 0$, then we can apply induction in the opposite direction and conclude our proof *if* we show that $[-1]^*(\omega) = -\omega$. We show this by using the formula for inversion of a point on an elliptic curve in general Weierstrass form (see Exercise

[7] Note that if E is in Weierstrass form, then we have a canonical choice of ω. Otherwise, ω is canonical up to scalar, see Figure 3.1.1.

0.7.1):

$$\begin{aligned}
[-1]^*(\omega) :&= [-1]^* \left(\frac{dx}{2y + a_1x + a_3} \right) \\
&= \frac{d[-1]^*(x)}{2[-1]^*(y) + a_1[-1]^*(x) + a_3} \\
&= \frac{dx}{2(-y - a_1x - a_3) + a_1x + a_3} \quad (\text{since } -(x, y) = (x, -y - a_1x - a_3)) \\
&= \frac{dx}{-2y - a_1x - a_3} \\
&= -\omega.
\end{aligned}$$

This concludes our proof. □

The following corollary is a proof of part. a. in Proposition 3.4.1 ([Sil09, Proposition III.4.2]), in the case where $\text{char}(k) \nmid n$. In fact, it shows more.

Corollary 3.5.4. [Sil09, Corollary III.5.4] *Let E be an elliptic curve and let $n \in \mathbb{Z}$ be where $\text{char}(k) \nmid n$. Then $[n]$ is nonconstant, hence surjective, and is a separable map.*

Proof. By the corollary above, we have $[n]^*(\omega) = n\omega \neq 0$, whence it follows that $[n]$ is nonzero. Since $[n](O) = O$, this then implies that $[n]$ is nonconstant, hence surjective.

For the second part, recall Proposition 2.4.1 ([Sil09, Proposition II.4.2]), which showed that a morphism $\phi\colon C_1 \to C_2$ of smooth curves is separable if and only if $\phi^*\colon \Omega_{C_2} \to \Omega_{C_1}$ is injective, i.e., nonzero. From this, it suffices to show that $[n]^*(\omega) \neq 0$. However, this follows from what we showed in the last paragraph: $[n]^*(\omega) = n\omega \neq 0$. □

Here is another corollary, which will be useful in Chapter 5 when we study $\#E(k)$ when k is a finite field.

Corollary 3.5.5. [Sil09, Corollary III.5.5] *Let $k := \mathbb{F}_q$ be a finite field of characteristic p, and let $E_{/\mathbb{F}_q}$ be an elliptic curve. Then letting $F_q\colon E \to E$ denote q-power Frobenius, we have that the endomorphism*

$$m + nF_q\colon E \to E$$

via $m + nF_q := [m] + [n] \cdot F_q$ is separable if and only if $p \nmid m$. In particular, the map $1 - F_q$ is separable.

Proof. Again by 2.4.1 ([Sil09, Proposition II.4.2]), we know that an endomorphism $\psi \in \text{End}(E)$ is **in**separable if and only if $\psi^*(\omega) = 0$. Since $F_q\colon E \to E$ is (purely) inseparable, we thus have $F_q^*(\omega) = 0$ (it is also easy to check this directly with the

formula for ω). We use this to check that

$$\begin{aligned}(m+nF_q)^*(\omega) &= [m]^*(\omega) + ([n]\circ F_q)^*(\omega)\\ &= m\omega + F_q^*([n]^*(\omega))\\ &= m\omega + F_q^*(n\omega)\\ &= m\omega + nF_q^*(\omega)\\ &= m\omega + n\cdot 0\\ &= m\omega.\end{aligned}$$

Using the previous corollary, we conclude that $m + nF_q$ is separable if and only if $m\omega \neq 0$, iff $p \nmid m$. □

The final corollary for this section will show tell us more about the structure of $\mathrm{End}(E)$.

Corollary 3.5.6. [Sil09, Corollary III.5.6] *Let $E_{/k}$ be an elliptic curve and ω an invariant differential on E. Define a map*

$$\mathrm{End}(E) \to \overline{k}$$

via

$$\phi \mapsto a_\phi \text{ such that } \phi^*\omega = a_\phi\omega.$$

a. *The map $\phi \mapsto a_\phi$ is a ring homomorphism.*
b. *The kernel of $\phi \mapsto a_\phi$ is the set of inseparable endomorphisms of E.*
c. *If $\mathrm{char}(k) = 0$, then $\mathrm{End}(E)$ is a commutative ring.*

The proof of this corollary is in [Sil09], and also explains why each $a - \phi$ is a constant function. Let us also remark that if $\mathrm{char}(k) = 0$, then every morphism over $\overline{k}$ is separable, and thus the kernel of this map is 0. This implies that we have an embedding $\mathrm{End}(E) \hookrightarrow \overline{k}$, whence $\mathrm{End}(E)$ is commutative, which proves part c. using part b.

3.6. **The dual isogeny.** In this section, we show that any isogeny of elliptic curves has a *dual* isogeny in the other direction. Understanding the dual isogeny is important for several reasons: one example is that it allows us to describe the structure of the n-torsion subgroup of an elliptic curve.

Recall that for two elliptic curves E and E' and an isogeny $\phi\colon E \to E'$, there is an induced map

$$\phi^*\colon \mathrm{Pic}^0(E') \to \mathrm{Pic}^0(E)$$

via

$$\phi^*([(Q)]) := \sum_{P\in\phi^{-1}(Q)} e_\phi(P)\cdot[(P)],$$

and then extending linearly (see Remark 2.3.2). On the other hand, we also have group isomorphisms $\kappa\colon E \to \mathrm{Pic}^0(E)$ and $\kappa'\colon E' \to \mathrm{Pic}^0(E')$, where

$$\kappa'(Q) = [(Q) - (O')],$$

and

$$\kappa^{-1}([P]) = P.$$

Then we have a composition map

$$\kappa^{-1} \circ \phi^* \circ \kappa' : E' \to E$$

which fits into the commutative diagram

$$\begin{array}{ccc} \mathrm{Pic}^0(E') & \xrightarrow{\phi^*} & \mathrm{Pic}^0(E) \\ {\scriptstyle \kappa'}\uparrow{\scriptstyle \cong} & & {\scriptstyle \cong}\downarrow{\scriptstyle \kappa^{-1}} \\ E' & \dashrightarrow & E \end{array}$$

As it turns out (and is not at all obvious), this map is an isogeny, and is called the **dual isogeny of ϕ.** It is written as $\widehat{\phi}$.

Let us prove that this is an isogeny.

Theorem 3.6.1. [Sil09, Theorem III.6.1] *Let $\phi\colon E \to E'$ be an isogeny of degree d.*

a. There exists a unique isogeny $\widehat{\phi}\colon E' \to E$ such that

$$\widehat{\phi} \circ \phi = [d].$$

b. As a group homomorphism, $\widehat{\phi} = \kappa^{-1} \circ \phi^* \circ \kappa'$.

Proof. First we prove uniqueness in part a.: suppose $\widehat{\phi}, \widehat{\phi}'\colon E' \to E$ are two isogenies with

$$\widehat{\phi}' \circ \phi = \widehat{\phi} \circ \phi = [d].$$

Then we have

$$(\widehat{\phi}' - \widehat{\phi}) \circ \phi = [0].$$

However, since ϕ is surjective, this implies that $\widehat{\phi}' - \widehat{\phi} = [0]$, and thus $\widehat{\phi}' = \widehat{\phi}$. We deduce that $\widehat{\phi}$ is unique.

Next, we prove that $\widehat{\phi}$ exists. We claim that the "dual operation" is distributive over compositions: i.e., if $\psi\colon E' \to E''$ is another isogeny (say of degree e), and the duals of ϕ and ψ exist, then the dual of $\psi \circ \phi$ exists, and

$$\widehat{\psi \circ \phi} = \widehat{\phi} \circ \widehat{\psi}.$$

This will help us construct the dual of an isogeny in the case where ϕ is inseparable.

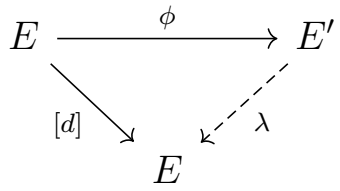
Towards the claim: we check that $\widehat{\phi} \circ \widehat{\psi}$ satisfies

$$\begin{aligned} (\widehat{\phi} \circ \widehat{\psi}) \circ (\psi \circ \phi) &= \widehat{\phi} \circ \widehat{\psi} \circ \widehat{\psi} \circ \widehat{\phi} \\ &= \widehat{\phi} \circ [e] \circ \phi \\ &= [e] \circ \widehat{\phi} \circ \phi \\ &= [de]. \end{aligned}$$

Since $\deg(\psi \circ \phi) = \deg(\psi) \cdot \deg(\phi) = de$, this shows that $\widehat{\psi \circ \phi} = \widehat{\phi} \circ \widehat{\psi}$ by uniqueness. Thus the claim is proven.

Now we construct the dual isogeny in two cases.

i. ϕ is separable. Thus, by Theorem 3.4.4 ([Sil09, Theorem III.4.10]), we know that $\#\ker\phi = \deg(\phi) = d$. Thus, $\ker\phi \subseteq \ker[d]$, so by Corollary 3.4.5 ([Sil09, Corollary III.4.11]) we have an isogeny $\lambda\colon E' \to E$ such that the following diagram commutes:



This says that $\lambda \circ \phi = [d]$. Thus, λ is the dual isogeny of E.

ii. ϕ is inseparable. This forces the characteristic of k to be $p > 0$. By Corollary 2.2.8 ([Sil09, Corollary II.2.12]), we can write

$$\phi = \psi \circ F_q$$

where $F_q\colon E \to E^{(q)}$ is q-power Frobenius for some power $q := p^r$ of p, and $\psi\colon E^{(q)} \to E'$ is a separable morphism. By the separable case above, we know that $\widehat{\psi}\colon E' \to E^{(q)}$ exists. Therefore, by our previous claim on distributivity of the dual operation, if the dual of F_q exists, then the dual of $\psi \circ F_q = \phi$ exists, and we're done. In fact, observe that $F_q = F_p^r$; therefore, it suffices to show that F_p has a dual.

We will show that $\widehat{F_p}$ exists by showing that $[p]\colon E \to E$ is inseparable, and then decomposing it. We know by Corollary 3.5.3 ([Sil09, Corollary III.5.3]) that for an invariant differential ω of E, we have

$$[p]^*(\omega) = p\omega = 0,$$

since the characteristic of k is p. Thus, by Proposition 2.4.1 ([Sil09, Proposition II.4.2]), this implies that $[p]$ is inseparable. Therefore, another application of Corollary 2.2.8 ([Sil09, Corollary II.2.12]) shows that

$$[p] = \lambda \circ F_{p^s}$$

for some q-power Frobenius $F_q\colon E \to E^{(q)}$ and some separable morphism $\lambda\colon E^{(q)} \to E$. Writing $q = p^s$, we know that $s \geq 1$; thus, from $[p] = (\lambda \circ F_{p^{s-1}}) \circ F_p$, we deduce that F_p has a dual, which is $\widehat{F_p} = \lambda \circ F_{p^{s-1}}$.

We thus conclude that the dual exists.

For part b., we must show that for all $Q \in E'$ one has

$$\widehat{\phi}(Q) = (\kappa^{-1} \circ \phi^* \circ \kappa')(Q).$$

Since $\phi\colon E \to E'$ is surjective, let us fix $P_0 \in \phi^{-1}(Q)$. On the one hand, we have

$$\widehat{\phi}(Q) = \widehat{\phi}(\phi(P_0)) = dP_0,$$

where $d := \deg \phi$. Thus, we will check that $(\kappa^{-1} \circ \phi^* \circ \kappa')(Q) = dP_0$:

$$\begin{aligned}
&(\kappa^{-1} \circ \phi^* \circ \kappa')(Q) \\
&= (\kappa^{-1} \circ \phi^*)([(Q)] - [(O')]) \\
&= \kappa^{-1} \left(\sum_{P \in \phi^{-1}(Q)} e_\phi(P) \cdot [(P)] - \sum_{T \in \phi^{-1}(O')} e_\phi(T) \cdot [(T)] \right) \\
&= \sum_{P \in \phi^{-1}(Q)} e_\phi(P) \cdot P - \sum_{T \in \phi^{-1}(O')} e_\phi(T) \cdot T && \text{(since } \kappa^{-1} = \sigma : [(P)] \mapsto P\text{)} \\
&= \sum_{P \in \phi^{-1}(Q)} \deg_i(\phi) \cdot P - \sum_{T \in \phi^{-1}(O')} \deg_i(\phi) \cdot T && \text{(by Thm. 3.4.4 ([Sil09, Theorem III.4.10]))} \\
&= \deg_i(\phi) \cdot \left(\sum_{P \in \phi^{-1}(Q)} P - \sum_{T \in \phi^{-1}(O')} T \right).
\end{aligned}$$

To simplify this, observe that for each $P \in \phi^{-1}(Q)$, we have $P_0 - P \in \ker \phi = \phi^{-1}(O')$. Thus, we can express $T \in \phi^{-1}(O')$ as $P_0 - P$ for some unique $P \in \phi^{-1}(Q)$. We can use this to check that

$$\begin{aligned}
&\deg_i(\phi) \cdot \left(\sum_{P \in \phi^{-1}(Q)} P - \sum_{T \in \phi^{-1}(O')} T \right) \\
&= \deg_i(\phi) \cdot \left(\sum_{P \in \phi^{-1}(Q)} P - \sum_{P \in \phi^{-1}(Q)} (P_0 - P) \right) \\
&= \deg_i(\phi) \cdot \left(\sum_{P \in \phi^{-1}(Q)} P_0 \right) \\
&= \deg_i(\phi) \cdot \#\phi^{-1}(Q) \cdot P_0 \\
&= \deg_i(\phi) \cdot \deg_s(\phi) \cdot P_0 && \text{(by Theorem 3.4.4 ([Sil09, Theorem III.4.10]))} \\
&= \deg(\phi) \cdot P_0 \\
&= dP_0.
\end{aligned}$$

We have thus shown that $\widehat{\phi}(Q) = (\kappa^{-1} \circ \phi^* \circ \kappa')(Q)$. Since $Q \in E'$ was arbitrary, we conclude that $\widehat{\phi} = \kappa^{-1} \circ \phi^* \circ \kappa'$. □

Thus, we now have a definition of the **dual isogeny** to an isogeny $\phi \colon E \to E'$, given by the above theorem: it can be described as the unique isogeny $\widehat{\phi} \colon E' \to E$ for which $\widehat{\phi} \circ \phi = [\deg(\phi)]$. Let us also define $\widehat{[0]} := [0]$.

Here are several important properties of the dual isogeny.

Theorem 3.6.2. [Sil09, Theorem III.6.2] *Let $\phi \colon E \to E'$ be an isogeny.*

a. Let $d := \deg \phi$. *Then*

$$\widehat{\phi} \circ \phi = [d] \text{ on } E \text{ and } \phi \circ \widehat{\phi} = [d] \text{ on } E'.$$

b. Let $\lambda \colon E' \to E''$ *be another isogeny. Then*

$$\widehat{\lambda \circ \phi} = \widehat{\phi} \circ \widehat{\lambda}.$$

c. If $\psi \colon E \to E'$ *is another isogeny, then*

$$\widehat{\phi + \psi} = \widehat{\phi} + \widehat{\psi}.$$

d. For all $n \in \mathbb{Z}$,

$$\widehat{[n]} = [n] \text{ and } \deg([n]) = n^2.$$

e. One has $\deg(\widehat{\phi}) = \deg(\phi)$.

f. One has $\widehat{\widehat{\phi}} = \phi$.

The proof of this theorem is only somewhat complicated for part c.; the rest follow rather quickly.

Here is an important corollary describing the structure of the n-torsion subgroup of an elliptic curve.

Corollary 3.6.3. [Sil09, Corollary III.6.4] *Let* E *be an elliptic curve, and let* $n \neq 0 \in \mathbb{Z}$.

a. $\deg[n] = n^2$.

b. If $n \neq 0$ *in* k, *i.e., if* $\operatorname{char}(k) = 0$ *or* $p = \operatorname{char}(k) > 0$ *and* $p \nmid n$, *then*

$$E[n] \cong \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}.$$

c. If $\operatorname{char}(k) = p > 0$, *then one of the following is true:*

i. $E[p^e] = \{O\}$ *for all* $e = 1, 2, 3, \ldots$ *(supersingular case);*

ii. $E[p^e] \cong \mathbb{Z}/p^e\mathbb{Z}$ *for all* $e = 1, 2, 3, \ldots$ *(ordinary case).*

Proof. Part a. was proven in Theorem 3.6.2 ([Sil09, Theorem III.6.2]). To prove part b., note that by Corollary 3.5.4 ([Sil09, Corollary III.5.4]), we know that $[n]$ is separable in this case, and thus by Theorem 3.4.4 ([Sil09, Theorem III.4.10]) we have

$$\#E[n] = \deg_s([n]) = \deg([n]) = n^2$$

(where $\deg([n]) = n^2$ by Theorem 3.6.2 ([Sil09, Theorem III.6.2])). By the same argument, for each $d \mid n$, we also have $\#E[d] = d^2$. Since $E[n]$ is a finite abelian group, a group theory argument shows that

$$E[n] \cong \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z},$$

see Exercise 3.6.1 ([Sil09, Exercise 3.30]).

For part c., let $F_p\colon E \to E^{(p)}$ be p-power Frobenius. Then

$$\begin{aligned}
\#E[p^e] &= \deg_s([p^e]) && \text{(by Theorem 3.4.4 ([Sil09, Theorem III.4.10]))}\\
&= \deg_s([p])^e\\
&= \deg_s(\widehat{F_p} \circ F_p)^e && \text{(since } \deg(F_p) = p)\\
&= \deg_s(\widehat{F_p})^e \cdot \deg_s(F_p)^e\\
&= \deg_s(\widehat{F_p})^e && \text{(since } F_p \text{ is purely inseparable).}
\end{aligned}$$

Since $\deg(\widehat{F_p}) = \deg(F_p) = p$, we find from $\deg(\widehat{F_p}) = \deg_s(\widehat{F_p}) \cdot \deg_i(F_p)$ that there are two cases:

i. If $\deg_s(\widehat{F_p}) = 1$, then $\widehat{F_p}$ is purely inseparable, and by the calculations above we have $\#E[p^e] = 1$ for all e.
ii. If $\deg_s(\widehat{F_p}) = p$, then $\widehat{F_p}$ is separable, and thus the calculations above show that $\#E[p^e] = p^e$ for all e. Again by Exercise 3.6.1 ([Sil09, Exercise 3.30]), this implies that
$$E[p^e] \cong \mathbb{Z}/p^e\mathbb{Z}.$$ □

To wrap this section up, we will prove that the degree map $\deg\colon \mathrm{Hom}(E, E') \to \mathbb{Z}_{\geq 0}$, which takes an isogeny to its degree, is a *positive definite quadratic form.* This will also have an application later when we prove the Hasse-Weil bound, as well as when we talk about heights on elliptic curves. (It can also help in the description of $\mathrm{End}(E)$.)

Definition 3.6.1. Let G be an abelian group. A function
$$d\colon G \to \mathbb{R}$$
is a **quadratic form** if it has the following two properties:

i. For all $g \in G$, we have $d(-g) = d(g)$.
ii. The pairing
$$p\colon G \times G \to \mathbb{R} \text{ by } p(g, h) := d(g + h) - d(g) - d(h)$$
is bilinear.

A quadratic form is **positive definite** if it also satisfies the following:

iii. For all $g \in G$, we have $d(g) \geq 0$;
iv. $d(g) = 0$ if and only if $g = 0$.

Notes Exercise 3.6.1. Show that for a quadratic form $d\colon G \to \mathbb{R}$, one has for all $g \in G$ and $n \in \mathbb{Z}$ that $d(ng) = n^2 d(g)$.

Corollary 3.6.4. [Sil09, Corollary III.6.3] *For elliptic curves E and E', the degree map*
$$\deg\colon \mathrm{Hom}(E, E') \to \mathbb{Z}_{\geq 0}$$
is a positive definite quadratic form.

Proof. The only nontrivial thing to check is that the pairing
$$p(\phi, \psi) := \deg(\phi + \psi) - \deg(\phi) - \deg(\psi)$$

is bilinear. We can check this by checking it under the map $[\cdot]\colon \mathbb{Z} \to \mathrm{End}(E)$:

$$\begin{aligned}
[p(\phi,\psi)] &= [\deg(\phi+\psi) - \deg(\phi) - \deg(\psi)] \\
&= [\deg(\phi+\psi)] - [\deg(\phi)] - [\deg(\psi)] \\
&= \widehat{\phi+\psi} \circ (\phi+\psi) - \widehat{\phi}\circ\phi - \widehat{\psi}\circ\psi \\
&= (\widehat{\phi}+\widehat{\psi})\circ(\phi+\psi) - \widehat{\phi}\circ\phi - \widehat{\psi}\circ\psi && \text{(by Thm. 3.6.2 ([Sil09, Theorem III.6.2]))} \\
&= \widehat{\phi}\circ\phi + \widehat{\phi}\circ\psi + \widehat{\psi}\circ\phi + \widehat{\psi}\circ\psi - \widehat{\phi}\circ\phi - \widehat{\psi}\circ\psi && \text{(since isogenies are homomorphisms)} \\
&= \widehat{\phi}\circ\psi + \widehat{\psi}\circ\phi.
\end{aligned}$$

It follows that $p(\cdot,\cdot)$ is bilinear: for example, we check for $\phi,\phi',\psi \in \mathrm{Hom}(E,E')$ that

$$\begin{aligned}
[p(\phi+\phi',\psi)] &= \widehat{\phi+\phi'}\circ\psi + \widehat{\psi}\circ(\phi+\phi') && \text{(by above calculations)} \\
&= (\widehat{\phi}+\widehat{\phi'})\circ\psi + \widehat{\psi}\circ(\phi+\phi') && \text{(by Thm. 3.6.2 ([Sil09, Theorem III.6.2]))} \\
&= \widehat{\phi}\circ\psi + \widehat{\phi'}\circ\psi + \widehat{\psi}\circ\phi + \widehat{\psi}\circ\phi' \\
&= (\widehat{\phi}\circ\psi + \widehat{\psi}\circ\phi) + (\widehat{\phi'}\circ\psi + \widehat{\psi}\circ\phi') \\
&= [p(\phi,\psi)] + [p(\phi',\psi)] \\
&= [p(\phi,\psi) + p(\phi',\psi)].
\end{aligned}$$

However, $[\cdot]$ is an injection by Proposition 3.4.1 ([Sil09, Proposition III.4.2]), which forces $p(\phi+\phi',\psi) = p(\phi,\psi) + p(\phi',\psi)$. We deduce that the first coordinate is linear, and a similar argument shows that the second coordinate is linear. □

Exercise 3.6.1. [Sil09, Exercise 3.30] Let G be a finite abelian group of order n^r. Suppose that for each $d \mid n$ we have $\#G[d] = d^r$, where $G[d]$ is the subgroup of G of elements whose orders divide d. Prove that

$$G \cong (\mathbb{Z}/n\mathbb{Z})^r.$$

Exercise 3.6.2. In this exercise, we assume that $\mathrm{char}(k) = 0$.

a. Suppose that C_1 and C_2 are curves defined over k, and that $\phi\colon C_1 \to C_2$ is a morphism. Let us write
$$\phi = [f_0 : f_1 : \ldots : f_n]$$
where each $f_i \in \overline{k}(C_1)$. Prove that for each $\sigma \in G_k$, the map $\phi^\sigma\colon C_1 \to C_2$ defined by
$$\phi^\sigma := [f_0^\sigma : f_1^\sigma : \ldots : f_n^\sigma]$$
is a morphism to C_2 with $\deg(\phi^\sigma) = \deg(\phi)$. (*Hint:* show that $\phi^*(\overline{k}(C_2)) \cong (\phi^\sigma)^*(\overline{k}(C_2))$.)

b. Let E_1/k and E_2/k be non-CM elliptic curves, and fix an isogeny $\phi\colon E_1 \to E_2$. Show that for each $\sigma \in G_k$, there exists $a_\sigma \in \{\pm 1\}$ with $\phi^\sigma = a_\sigma \cdot \phi$.

c. Continuing part b., show that the map $\chi\colon G_k \to \{\pm 1\}$ defined by $\sigma \mapsto a_\sigma$ is a homomorphism. Conclude that there exists $d \in \overline{k}^\times$ such that for all $\sigma \in G_k$, one has
$$\sigma(\sqrt{d}) = \chi(\sigma)\cdot\sqrt{d}.$$

This exercise can be used to show that there exists a *twist*[8] of E_2 by χ, denoted E_2^χ/k, and a k-**rational** isogeny $\psi\colon E_1 \to E_2^\chi$. Thus, in the non-CM case, we can assume an isogeny between k-rational elliptic curves is also k-rational (up to $\overline{k}$-isomorphism of the target elliptic curve). More on twists in Chapter 10.

Exercise 3.6.3. Let E and E' be elliptic curves, and let $\phi\colon E \to E'$ be an isogeny.

a. Show that if E, E' and ϕ are k-rational, then so is the dual $\widehat{\phi}$.
b. Show that if ϕ is *cyclic,*[9] then so is its dual $\widehat{\phi}$ if one of the following holds:
   i. $\mathrm{char}(k) = 0$.
   ii. $\mathrm{char}(k) > 0$ is coprime to $\deg(\phi)$.

3.7. **The Tate module (and Galois representations).** In this section, we will describe the Galois representations of an elliptic curve, as well as the associated p-adic Tate modules. These representations/modules are intimately connected to torsion subgroups.

Given an elliptic curve E and an integer $n \in \mathbb{Z}^+$, recall that $E[n]$ denotes the n-torsion subgroup of E. We have previously noted that when E is defined over k, we have an action of G_k on E (see Notes Exercises 1.1.2 and 1.2.4). Since $[n]$ is k-rational (see Example 3.4.2), we also have an induced action of G_k on $E[n]$: for each $P \in E[n]$ and $\sigma \in G_k$, we have

$$nP^\sigma = [n](P^\sigma) = [n]^\sigma(P^\sigma) = ([n]P)^\sigma = O^\sigma = O,$$

whence it follows that $P^\sigma \in E[n]$. Therefore, we have an associated group action homomorphism

$$\rho_{E,n}\colon G_k \to \mathrm{Aut}(E[n])$$

called the **mod-n Galois representation of E.**

We showed in §3.6 that when $p := \mathrm{char}(k)$ does not divide n, one has

$$E[n] \cong \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}.$$

In particular, $E[n]$ can be regarded as a free rank two $\mathbb{Z}/n\mathbb{Z}$-module. Thus, if we fix a $\mathbb{Z}/n\mathbb{Z}$-basis $\{P, Q\}$ for $E[n]$, then we have an isomorphism $\mathrm{Aut}(E[n]) \cong \mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$, where the latter group is the general linear group of 2×2 invertible matrices over $\mathbb{Z}/n\mathbb{Z}$. Therefore, our representation can be expressed as

$$\rho_{E,n,P,Q}\colon G_k \to \mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z}).$$

For example, for an automorphism $\sigma \in G_k$, the equation

$$\rho_{E,n,P,Q}(\sigma) = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$$

is equivalent to having that $P^\sigma = aP + cQ$ and $Q^\sigma = bP + dQ$.

Remark 3.7.1. We often write $\rho_{E,n}$ instead of $\rho_{E,n,P,Q}$, suppressing dependence on the basis. This conjugates the image $\rho_{E,n,P,Q}(G_k)$ – see the notes exercise below.

[8] A *twist* of an elliptic curve E is an elliptic curve E' which is isomorphic to E over $\overline{k}$.

[9] Say that an isogeny is *cyclic* if its kernel is cyclic.

Notes Exercise 3.7.1. Assume that $\mathrm{char}(k) \nmid n$, and fix a basis $\{P, Q\}$ of $E[n]$. Show that a change of basis conjugates the image $\rho_{E,n,P,Q}(G_F)$ in $\mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$.

Example 3.7.1. The matrix description of the mod-n Galois representation can be extremely useful in understanding torsion points. Fix an integer $n \in \mathbb{Z}^+$, and assume that $\mathrm{char}(k) \nmid n$. For an elliptic curve $E_{/k}$, for any basis $\{P, Q\}$ of $E[n]$ such that

$$\rho_{E,n,P,Q}(G_k) \subseteq \left\{ \begin{bmatrix} 1 & * \\ 0 & * \end{bmatrix} \right\},$$

one has that P is k-rational: this is because for all $\sigma \in G_k$, one has

$$P^\sigma = 1 \cdot P + 0 \cdot Q = P.$$

Alternatively, if

$$\rho_{E,n,P,Q}(G_k) \subseteq \left\{ \begin{bmatrix} * & * \\ 0 & * \end{bmatrix} \right\},$$

then $\langle P \rangle$ is k-rational, since for all $\sigma \in G_k$ one has

$$P^\sigma = a_\sigma \cdot P,$$

and thus $P^\sigma \in \langle P \rangle$. The converse directions also hold.

Next, we describe the Tate modules of an elliptic curve. Their construction is in analogy to the construction of the p-adic integers, by way of inverse limits.

Definition 3.7.1. Let E be an elliptic curve, and fix a prime $p \in \mathbb{Z}^+$. Then for each $k \geq 1$, there is a natural map $E[p^{k+1}] \to E[p^k]$. This forms an inverse system, and we define the **p-adic Tate module of** E as the inverse limit

$$T_p(E) := \varprojlim_{k \geq 1} E[p^k].$$

Since each $E[p^k]$ is a $\mathbb{Z}/p^k\mathbb{Z}$-module, it follows that $T_p(E)$ is a $\mathbb{Z}_p$-module, where

$$\mathbb{Z}_p := \varprojlim_{k \geq 1} \mathbb{Z}/p^k\mathbb{Z}$$

denotes the *ring of p-adic integers.* It also follows that $T_p(E)$ has a natural topology as the inverse limit of spaces with a discrete topology.

Since each subgroup $E[p^k]$ is a $\mathbb{Z}/p^k\mathbb{Z}$-module, it follows that $T_p(E)$ is a $\mathbb{Z}_p$-module, where

$$\mathbb{Z}_p := \varprojlim_{k \geq 1} \mathbb{Z}/p^k\mathbb{Z}$$

is the **ring of p-adic integers.**

As a consequence of knowing the structure of each $E[p^k]$, we have the following result.

Proposition 3.7.1. [Sil09, Proposition III.7.1] *For an elliptic curve E, one has the following:*

a. $T_p(E) \cong_{\mathbb{Z}_p} \mathbb{Z}_p \times \mathbb{Z}_p$ *if* $\mathrm{char}(k) \neq p$.
b. $T_p(E) = 0$ *if E is* supersingular.
c. $T_p(E) \cong_{\mathbb{Z}_p} \mathbb{Z}_p$ *if E is* ordinary.

For an elliptic curve $E_{/k}$ and a prime $p \in \mathbb{Z}^+$, since G_k acts on each $E[p^k]$, it also acts (continuously) on $T_p(E)$. This action is described by the **p-adic Galois representation of E,** which is written as

$$\rho_{E,p^\infty} \colon G_k \to \mathrm{Aut}(T_p(E)).$$

For the rest of this section, fix a prime $p \in \mathbb{Z}^+$ with $\mathrm{char}(k) \neq p$. We will use the p-adic Tate module to help describe the groups $\mathrm{Hom}(E_1, E_2)$ and $\mathrm{Hom}_k(E_1, E_2)$ for two isogenous elliptic curves E_1 and E_2 (this also includes the case where $E_1 = E_2$). Suppose we have an isogeny $\phi \colon E_1 \to E_2$. Then for each $n \in \mathbb{Z}^+$, we have a homomorphism

$$\phi \colon E_1[n] \to E_2[n].$$

In particular, for each $k \in \mathbb{Z}^+$ we have $\phi \colon E_1[p^k] \to E_2[p^k]$. This induces a homomorphism

$$\phi_p \colon T_p(E_1) \to T_p(E_2).$$

In particular, we have a natural group homomorphism

$$\mathrm{Hom}(E_1, E_2) \to \mathrm{Hom}(T_p(E_1), T_p(E_2)).$$

If $E := E_1 = E_2$, then this map

$$\mathrm{End}(E) \to \mathrm{End}(T_p(E))$$

is a ring homomorphism.

Theorem 3.7.2. [Sil09, Theorem III.7.4] *For elliptic curves E_1 and E_2, if $p \neq \mathrm{char}(k)$ is a prime, then the natural map*

$$\mathrm{Hom}(E_1, E_2) \otimes \mathbb{Z}_p \to \mathrm{Hom}(T_p(E_1), T_p(E_2))$$

via $\phi \mapsto \phi_p$ is injective.

As a consequence of this theorem, we can realize $\mathrm{Hom}(E_1, E_2)$ as a subgroup of $\mathrm{Hom}(T_p(E_1), T_p(E_2))$; similarly, $\mathrm{End}(E)$ is a subring of $\mathrm{End}(T_p(E))$. In particular, we can use this to describe $\mathrm{Hom}(E_1, E_2)$ and $\mathrm{End}(E)$, using that $T_p(E_1), T_p(E_2)$ and $T_p(E)$ are well-understood by Proposition 3.7.1 ([Sil09, Proposition III.7.1]).

Corollary 3.7.3. [Sil09, Corollary III.7.5] *Let E_1 and E_2 be elliptic curves. Then $\mathrm{Hom}(E_1, E_2)$ is a free $\mathbb{Z}$-module of rank ≤ 4.*

Note that the proof of this corollary in [Sil09] is false. However, there is a corrected proof on the following errata page: `https://www.math.brown.edu/~jhs/AEC/AECErrata.pdf`.

There is an analogous result to Theorem 3.7.2 above ([Sil09, Theorem III.7.4]) for k-rational isogenies, which is considerably more difficult to prove. Let us define $\mathrm{Hom}_k(T_p(E_1), T_p(E_2))$ as the group of $\mathbb{Z}_p$-module homomorphisms which are k-rational, i.e., which commute with the action of G_k. Then similar to before, we have a natural map

$$\mathrm{Hom}_k(E_1, E_2) \to \mathrm{Hom}_k(T_p(E_1), T_p(E_2))$$

via $\phi \mapsto \phi_p$. By Theorem 3.7.2), this map is injective. However, we can say more:

Theorem 3.7.4 (Isogeny Theorem)**.** [Sil09, Theorem III.7.7] *For elliptic curves E_1 and E_2, if $p \neq \mathrm{char}(k)$ is a prime, then the natural map*

$$\mathrm{Hom}_k(E_1, E_2) \otimes \mathbb{Z}_p \to \mathrm{Hom}_k(T_p(E_1), T_p(E_2))$$

via $\phi \mapsto \phi_p$ is an isomorphism if k is a finite field or a number field.

The proof of the above theorem is due to Tate in the finite field case [Tat66], and the number field case is due to Faltings.

We wrap this section up with an important result on the image of Galois of elliptic curves.

Theorem 3.7.5 (Serre's open image theorem)**.** *Let F be a number field and $E_{/F}$ a non-CM elliptic curve. Then for all but finitely many primes $p \in \mathbb{Z}^+$, the p-adic Galois representation*

$$\rho_{E,p^\infty} \colon G_F \to \mathrm{GL}(\mathbb{Z}_p)$$

is surjective.

Remark 3.7.2. In contrast to Serre's open image theorem, if $E_{/F}$ is an elliptic curve with CM, then the image $\rho_{E,p^\infty}(G_F)$ is always abelian in $\mathrm{GL}_2(\mathbb{Z}_p)$, which implies it can never be surjective; see Exercise 3.7.1 below.

Exercise 3.7.1. [Sil09, Exercise 3.24] Let $E_{/k}$ be an elliptic curve with complex multiplication over k, i.e., such that $\mathrm{End}_k(E) \neq \mathbb{Z}$. Prove that for all primes $p \neq \mathrm{char}(k)$, the action of G_k on $T_p(E)$ is abelian. (*Hint:* use the fact that all endomorphisms in $\mathrm{End}_k(E)$ commute with the action of G_k on $T_p(E)$.)

3.8. **The Weil Pairing.** In this section, we will define and describe a particularly useful perfect pairing associated to torsion subgroups of elliptic curves, called the *Weil pairing.*

Throughout this section, fix an integer $n \in \mathbb{Z}^+$ that is coprime to $\mathrm{char}(k)$. Let $E_{/k}$ be an elliptic curve; we have shown in §3.6 that we have

$$E[n] \cong \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}.$$

Thus, $E[n]$ is a free rank two $\mathbb{Z}/n\mathbb{Z}$-module. We will define a nondegenerate alternating bilinear map on $E[n] \times E[n]$ analogous to the determinant, but which is also Galois invariant, i.e., commutes with Galois in a predictable way. Unlike the determinant, which takes values in $(\mathbb{Z}/n\mathbb{Z})^\times$, our pairing will take values in $\mu_n := \mu_n(\overline{k})$, the group of n'th roots of unity in $\overline{k}$. Our definition will use rational functions on E, à la our consequences of Riemann-Roch.

We will denote this pairing by $e_n \colon E[n] \times E[n] \to \mu_n$. In our construction, we will use Corollary 3.3.5 ([Sil09, Corollary III.3.5]) several times: this states that a divisor $D = \sum_{P \in E} n_P \cdot (P) \in \mathrm{Div}(E)$ is principal if and only if $\deg(D) = 0$ and

$$\sum_{p \in E} n_P P = O.$$

Fix points $S, T \in E[n]$. We want to define $e_n(S, T)$. First, observe that $nT = O$, so that $nT - nO = O$. Thus, Corollary 3.3.5 implies that $n(T) - n(O) \in \mathrm{Prin}(E)$; let us

write

$$n(T) - n(O) = \operatorname{div}(f) \tag{7}$$

for some $f \in \overline{k}(E)$.

We claim that $[n]^*((T) - (O))$ is principal as well; we'll use the above corollary to prove this. First, we show that its degree is 0:

$$\begin{aligned}
&\deg([n]^*((T) - (O))) \\
&= \deg([n]) \cdot \deg((T) - (O)) \qquad \text{(Proposition 2.3.2 [Sil09, Proposition II.3.6])} \\
&= 0.
\end{aligned}$$

Next, we check that the sum in E associated to $[n]^*((T)-(O))$ is O. First, we explicitly compute its divisor:

$$\begin{aligned}
&[n]^*((T) - (O)) \\
&= \sum_{T' \in [n]^{-1}(T)} e_{[n]}(T') \cdot (T') - \sum_{Q \in E[n]} e_{[n]}(Q) \cdot (Q) \quad \text{(definition of pullback, extended linearly)} \\
&= \sum_{T' \in [n]^{-1}(T)} (T') - \sum_{Q \in E[n]} (Q) \qquad \text{([n] separable, Thm. 3.4.4 [Sil09, Theorem III.4.10]} \\
&\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad \text{and Cor. 3.5.4 [Sil09, Corollary III.5.4]).}
\end{aligned}$$

Similar to the ideas in Theorem 3.6.1 ([Sil09, Theorem III.6.1]), if we fix $T_0 \in [n]^{-1}(T)$, then each element $Q \in E[n]$ can be written as $T' - T_0$ for some unique $T' \in [n]^{-1}(T)$. It follows that our divisorial sum becomes

$$\begin{aligned}
&\sum_{T' \in [n]^{-1}(T)} (T') - \sum_{Q \in E[n]} (Q) \\
&= \sum_{T' \in [n]^{-1}(T)} (T') - \sum_{T' \in [n]^{-1}(T)} (T' - T_0).
\end{aligned}$$

Therefore, the corresponding sum in E is

$$\begin{aligned}
&\sum_{T' \in [n]^{-1}(T)} T' - \sum_{T' \in [n]^{-1}(T)} T' - T_0 \\
&= \#[n]^{-1}(T) \cdot T_0 \\
&= \deg([n]) \cdot T_0 \qquad \text{([n] is separable)} \\
&= n^2 \cdot T_0 \qquad \text{($\deg([n]) = n^2$, see Thm. 3.6.2 [Sil09, Theorem III.6.2]).}
\end{aligned}$$

Since $nT_0 = O$, we deduce from these calculations that the associated sum in E for the divisor $[n]^*((T) - (O))$ is O. It follows by the corollary that $[n]^*((T) - (O))$ is a principal divisor. Let us write this as

$$[n]^*((T) - (O)) = \operatorname{div}(g). \tag{8}$$

It is easy to check with (7) and (8) that $[n]^*(f)$ and g^n have the same divisor. thus, the rational function $\frac{[n]^*(f)}{g^n} \in \overline{k}(E)$ has a trivial divisor, which forces it to be constant;

without loss of generality, let us assume that $\frac{[n]^*(f)}{g^n} = 1$, i.e.,

$$[n]^*(f) = g^n. \tag{9}$$

Thus, for points $P \in E$, we have

$$f(nP) = g(P)^n.$$

In particular, for any point $X \in E$, we check that both

$$g(X+S)^n = f(nX+nS) = f(nX) = g(X)^n,$$

and so

$$\left(\frac{g(X+S)}{g(X)}\right)^n = 1. \tag{10}$$

Since $g(X+S) = (g \circ \tau_S)(X)$, where $\tau_S \colon E \to E$ is translation-by-S, this implies that for the rational function $\frac{g\circ\tau_S}{g} \in \overline{k}(E)$, the associated morphism

$$\phi \colon E \to \mathbb{P}^1$$

defined by

$$\phi = \left[\frac{g \circ \tau_S}{g} : 1\right]$$

is constant, since its values lie in μ_n, and thus cannot surject onto $\mathbb{P}^1(\overline{k})$; see also Theorem 2.2.2 ([Sil09, Theorem II.2.3]) and Example 2.2.1. Thus, we define the **n-Weil pairing** on S, T as this constant value:

$$e_n(S,T) := \frac{g(X+S)}{g(X)},$$

where $g(X+S)$ and $g(X)$ are both defined and nonzero. By (10), we know that $e_n(S,T)$ is an n'th root of unity.

Remark 3.8.1. In our definition of e_n, we assumed that $[n]^*(f) = g^n$, instead of up to a constant. Observe that this does not affect the actual value of e_n.

To summarize our construction of the Weil pairing $e_n \colon E[n] \times E[n] \to \mu_n$:

1. Fix $S, T \in E[n]$.
2. We can write $n(T) - n(O) = \operatorname{div}(f)$ and $[n]^*((T) - (O)) = \operatorname{div}(g)$ for some $f, g \in \overline{k}(E)$.
3. We set $e_n(S,T) := \frac{g(X+S)}{g(X)}$ for any point $X \in E$ where this quotient is defined and both functions are nonzero.

Here are some important properties of the Weil pairing.

Proposition 3.8.1. [Sil09, Proposition III.8.1] *The n-Weil pairing $e_n \colon E[n] \times E[n] \to \mu_n$ satisfies the following properties:*

a. It is biliinear:

$$e_n(S_1 + S_2, T) = e_n(S_1, T) \cdot e_n(S_2, T)$$

and

$$e_n(S, T_1 + T_2) = e_n(S, T_1) \cdot e_n(S, T_2).$$

b. It is alternating:

$$e_n(T,T) = 1,$$

and thus $e_n(S,T) = e_n(T,S)^{-1}$.

c. It is nondegenerate: *for a fixed* $T_0 \in E[n]$, *if*

$$e_n(S,T_0) = 1$$

for all $S \in E[n]$ *then* $T_0 = O$.

d. It is Galois invariant: *for all* $\sigma \in G_k$, *one has*

$$e_n(S,T)^\sigma = e_n(S^\sigma, T^\sigma).$$

e. It is compatible: *for* $n' \in \mathbb{Z}^+, S \in E[nn']$ *and* $T \in E[n]$, *one has*

$$e_{nn'}(S,T) = e_n(n'S,T).$$

Proof. We will only prove parts a. and d. To check linearity in the first coordinate, observe that our definition for $e_n(S,T)$ only involves S at the final step, i.e., the function g depends only on T. In computing $e_n(S_1+S_2,T)$, we check that

$$\begin{aligned}\frac{g(X+S_1+S_2)}{g(X)} &= \frac{g((X+S_1)+S_2)}{g(X+S_1)} \cdot \frac{g(X+S_1)}{g(X)} \\ &= e_n(S_2,T)\cdot e_n(S_1,T),\end{aligned}$$

where we have chosen $X \in E$ such that g is defined and nonzero at $X, X+S_1$ and $X+S_1+S_2$. It follows that $e_n(S_1+S_2,T) = e_n(S_1,T)\cdot e_n(S_2,T)$.

For linearity in the other coordinate, let us assume that our construction of e_n for each of T_1, T_2 and $T_3 := T_1+T_2$ involve corresponding functions f_1, g_1, f_2, g_2 and f_3, g_3. Thus, for each $1 \le i \le 3$, we have

$$n((T_i)-(O)) = \operatorname{div}(f_i)$$

and

$$[n]^*((T_i)-(O)) = \operatorname{div}(g_i),$$

as well as

$$e_n(S,T_i) = \frac{g_i(X+S)}{g_i(X)}.$$

We note that under the isomorphism $\kappa\colon E \xrightarrow{\sim} \operatorname{Pic}^0(E)$ from Proposition 3.3.4 ([Sil09, Proposition III.3.4]), we have $\kappa(T_1+T_2) = \kappa(T_1)+\kappa(T_2)$, i.e., $(T_3)-(O) \sim (T_1)-(O)+(T_2)-(O)$, i.e., $(T_3) \sim (T_1)+(T_2)-(O)$. Thus, there exists a rational function $h \in \overline{k}(E)$ with

$$\operatorname{div}(h) = (T_3)-(T_1)-(T_2)+(O).$$

Since each $\operatorname{div}(f_i) = n(T_i)-n(O)$, it follows that

$$\operatorname{div}(h^n) = \operatorname{div}\left(\frac{f_3}{f_1 f_2}\right).$$

Therefore, we have

$$f_3 = c\cdot f_1 f_2 h^n$$

for some $c \in \overline{k}^\times$. On the other hand, we know from the construction of $e_n(S, T_3)$ that $[n]^*(f_3) = g_3^n$ (see (9)). Applying $[n]^*$ to both sides in the above equality, we check that

$$\begin{aligned}[n]^*(f_3) &= [n]^*(c \cdot f_1 f_2 h^n) \\ &= c \cdot [n]^*(f_1) \cdot [n]^*(f_2) \cdot [n]^*(h^n) \\ &= c g_1 g_2 \cdot [n]^*(h^n).\end{aligned}$$

Since $[n]^*(f_3) = g_3$, we take n'th roots of both sides and deduce that

$$g_3 = c' \cdot g_1 g_2 \cdot [n]^*(h)$$

for some $c' \in \overline{k}^\times$. We can use this to compute $e_n(S, T_1 + T_2)$:

$$\begin{aligned}e_n(S, T_1 + T_2) &= \frac{g_3(X+S)}{g_3(X)} \\ &= \frac{c' \cdot g_1(X+S) g_2(X+S) \cdot h(nX+nS)}{c' \cdot g_1(X) g_2(X) \cdot h(nX)} \\ &= \frac{g_1(X+S)}{g_1(X)} \cdot \frac{g_2(X+S)}{g_2(X)} \cdot \frac{h(nX)}{h(nX)} \qquad \text{(note that } nS = O\text{)} \\ &= e_n(S, T_1) \cdot e_n(S, T_2).\end{aligned}$$

This proves part a.

For part d., let f and g be functions for T. Thus, $e_n(S, T) = \frac{g(X+S)}{g(X)}$. One can check that f^σ and g^σ are functions for T^σ in the computation of $e_n(S^\sigma, T^\sigma)$. Furthermore, one has

$$e_n(S^\sigma, T^\sigma) = \frac{g^\sigma(X^\sigma + S^\sigma)}{g^\sigma(X^\sigma)} = \left(\frac{g(X+S)}{g(X)}\right)^\sigma = e_n(S, T)^\sigma. \qquad \square$$

There are a number of consequences of the existence of the Weil pairing. Here is one, which is a version of [Sil09, Corollary III.8.1.1].

Corollary 3.8.2. *If $\{P, Q\}$ is a basis of $E[n]$, then $e_n(P, Q)$ is a primitive n'th root of unity (denoted by ζ_n). In particular, if $P, Q \in E(k)$ then $\zeta_n \in k$.*

Proof. By the previous proposition, we know that the image $e_n(E[n], E[n])$ is a subgroup of μ_n. Since μ_n is cyclic, we can write this image as μ_d for some $d \mid n$. Thus, we have for all $S, T \in E[n]$ that $e_n(S, T)^d = 1$, which by bilinearity implies that $e_n(dS, T) = 1$. Thus, nondegeneracy of the Weil pairing forces $dS = O$. Since $S \in E[n]$ was arbitrary and $E[n]$ contains an *exact* order n point, we deduce that $d = n$. Thus, $e_n(E[n], E[n]) = \mu_n$.

Let $\{P, Q\}$ be a basis for $E[n]$. Then we can write $\zeta_d := e_n(P, Q)$ for some $d \mid n$. We claim that $d = n$. To see this, we will first show that any value in $e_n(E[n], E[n])$ can be written as a power of $e_n(P, Q)$. To this end, let $S, T \in E[n]$; since $\{P, Q\}$ is a basis,

we can write $S = aP + cQ$ and $T = bP + dQ$ for some $a, b, c, d \in \mathbb{Z}$. We check that

$$\begin{aligned}
e_n(S,T) &= e_n(aP + cQ, bP + dQ) \\
&= e_n(aP, bP + dQ)e_n(cQ, bP + dQ) && \text{(by bilinearity)} \\
&= e_n(aP, bP)e_n(aP, dQ)e_n(cQ, bP)e_n(cQ, dQ) && \text{(again, by bilinearity)} \\
&= e_n(P,P)^{ab}e_n(P,Q)^{ad}e_n(Q,P)^{cb}e_n(Q,Q)^{cd} && \text{(again!, by bilinearity)} \\
&= e_n(P,Q)^{ad}e_n(Q,P)^{bc} && \text{(by alternating property)} \\
&= e_n(P,Q)^{ad}e_n(P,Q)^{-bc} && \text{(by alternating consequence)} \\
&= e_n(P,Q)^{ad-bc}.
\end{aligned}$$

We deduce that all values in $e_n(E[n], E[n])$ are powers of $e_n(P,Q)$. Since we know that $e_n(E[n], E[n]) = \mu_n$ by the first paragraph, we conclude that $e_n(P,Q)$ is a primitive n'th root of unity.

We are left to show that if $P, Q \in E(k)$ then $\zeta_n \in k$, where ζ_n is some primitive n'th root of unity. This will follow from Galois invariance of e_n. Without loss of generality, we can assume that $\zeta_n = e_n(P,Q)$. Then $\zeta_n \in k$ if and only if for all $\sigma \in G_k$ we have $\sigma(\zeta_n) = \zeta_n$, i.e., $\sigma(e_n(P,Q)) = e_n(P,Q)$. However, by Galois invariance of e_n we know that

$$\sigma(e_n(P,Q)) = e_n(P^\sigma, Q^\sigma).$$

Since P and Q are k-rational, the result follows at once. □

Notes Exercise 3.8.1. The n-Weil pairing can detect bases for $E[n]$. Fix a basis $\{P,Q\}$ of $E[n]$. Let $P', Q' \in E[n]$, and write $P' = aP + cQ$ and $Q' = bP + dQ$. By the work in Corollary 3.8.2, we know that

$$e_n(P', Q') = e_n(P,Q)^{ad-bc}.$$

Prove that $\{P', Q'\}$ is a basis for $E[n]$ if and only if $ad - bc$ is in $(\mathbb{Z}/n\mathbb{Z})^\times$.

Notes Exercise 3.8.2. Show that for an elliptic curve $E_{/\mathbb{Q}}$, one has $E[n] \not\subseteq E(\mathbb{R})$ when $n \geq 3$.

There is another useful result which says that the determinant of the image of the mod-n Galois representation $\rho_{E,n} \colon G_k \to \mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$ is equal to the image of the mod-n cyclotomic character $\chi_n \colon G_k \to (\mathbb{Z}/n\mathbb{Z})^\times$.

Definition 3.8.1. Recall that the **mod-n cyclotomic character** is the homomorphism

$$\chi_n \colon G_k \to (\mathbb{Z}/n\mathbb{Z})^\times$$

which describes the action of G_k on μ_n: fixing a primitive n'th root ζ_n, we have for $\sigma \in G_k$ that $\chi_n(\sigma) := a_\sigma$ where

$$\sigma(\zeta_n) = \zeta_n^{a_\sigma}.$$

Notes Exercise 3.8.3. Show that the values of χ_n are independent of the choice of primitive n'th root ζ_n.

Here is a connection between $\rho_{E,n}$ and χ_n.

Proposition 3.8.3. *For an elliptic curve $E_{/k}$, one has for each $\sigma \in G_k$ that*

$$\det \rho_{E,n}(\sigma) = \chi_n(\sigma),$$

with respect to any basis of $E[n]$ and any primitive n'th root of unity. In particular, we have

$$\det \rho_{E,n}(G_k) = \chi_n(G_k).$$

Proof. Let us fix a basis $\{P, Q\}$ of $E[n]$. By Notes Exercise 3.8.3, the character χ_n describes the action of G_k on μ_n via $\zeta_n := e_n(P, Q)$ (note that $e_n(P, Q)$ is a primitive n'th root of unity by Proposition 3.8.2). For $\sigma \in G_k$, writing $P^\sigma = aP + cQ$ and $Q^\sigma = bP + dQ$, we have by definition that

$$\rho_{E,n}(\sigma) := \rho_{E,n,P,Q}(\sigma) := \begin{bmatrix} a & b \\ c & d \end{bmatrix}.$$

Thus, $\det \rho_{E,n}(\sigma) = ad - bc$.

We claim that $\chi_n(\sigma) = ad - bc$. Let us make some calculations towards this:

$$\begin{aligned} \sigma(\zeta_n) &= \sigma(e_n(P, Q)) \\ &= e_n(P^\sigma, Q^\sigma) && \text{(by Proposition 3.8.1, Galois invariance)} \\ &= e_n(aP + cQ, bP + dQ) \\ &= e_n(P, Q)^{ad-bc} && \text{(by Notes Exercise 3.8.1)} \\ &= \zeta_n^{ad-bc}. \end{aligned}$$

We conclude that $\det \rho_{E,n}(\sigma) = \chi_n(\sigma)$. From this, it also follows that $\det \rho_{E,n}(G_k) = \chi_n(G_k)$. Note that changing the basis of $E[n]$ conjugates elements of $\rho_{E,n}(G_k)$, and thus does not change their determinants. □

One can show that an isogeny $\phi\colon E \to E'$ and its dual are dual/adjoint with respect to the Weil pairing.

Proposition 3.8.4. [Sil09, Proposition III.8.2] *Let $\phi\colon E \to E'$ be an isogeny of elliptic curves. Then for all $S \in E[n]$ and $T' \in E'[n]$, one has*

$$e_n(S, \widehat{\phi}(T')) = e_n(\phi(S), T').$$

There is an extension of the Weil pairing to the Tate module of an elliptic curve. Let $p \neq \mathrm{char}(k)$ be a prime. For each $m \geq 1$, we have a p^m-Weil pairing

$$e_{p^m}\colon E[p^m] \times E[p^m] \to \mu_{p^m}.$$

Using the compatibility property of the Weil pairing, which is part e. of Proposition 3.8.1 ([Sil09, Proposition III.8.1]), we can show that

$$e_{p^{m+1}}(S, T)^p = e_{p^m}(pS, pT)$$

for all $S, T \in E[p^{m+1}]$. This then gives us a well-defined pairing

$$e_{p^\infty}\colon T_p(E) \times T_p(E) \to \varprojlim_{m \geq 1} \mu_{p^m}.$$

Proposition 3.8.5. [Sil09, Proposition III.8.3] *The pairing $e_{p^\infty}: T_p(E) \times T_p(E) \to \mu_{p^\infty}$ is bilinear, alternating, nondegenerate, and Galois invariant. Furthermore, if $\phi: E \to E'$ is an isogeny, then for all $x \in T_p(E)$ and $y' \in T_p(E')$, one has*

$$e_{p^\infty}(x, \widehat{\phi}(y')) = e_{p^\infty}(\phi(x), y').$$

To end this section, we will show how one can use the Weil pairing to understand the map an isogeny induces on Tate modules. Recall that an endomorphism $\phi \in \mathrm{End}(E)$ induces a $\mathbb{Z}_p$-linear map

$$\phi_p: T_p(E) \to T_p(E).$$

We've observed previously that $T_p(E) \cong_{\mathbb{Z}_p} \mathbb{Z}_p \times \mathbb{Z}_p$. Thus, ϕ_p can be realized as an element of $\mathrm{Mat}_{2\times 2}(\mathbb{Z}_p)$, i.e., as a 2×2 matrix over $\mathbb{Z}_p$. We let $\det(\phi_p)$ and $\mathrm{tr}(\phi_p)$ denote the determinant and trace of a matrix representative of ϕ_p, respectively. Note that these values are independent of the choice of basis for $T_p(E)$.

Proposition 3.8.6. [Sil09, Proposition III.8.6] *Let $\phi \in \mathrm{End}(E)$. Then*

$$\det(\phi_p) = \deg(\phi)$$

and

$$\mathrm{tr}(\phi_p) = 1 + \deg(\phi) - \deg(1 - \phi).$$

In particular, $\det(\phi_p)$ and $\mathrm{tr}(\phi_p)$ are in $\mathbb{Z}$, and are independent of p.

Proof. Fix a $\mathbb{Z}_p$-basis $\{x, y\}$ of $T_p(E)$. Let us write

$$\phi_p(x) = ax + cy$$

and

$$\phi_p(y) = bx + dy;$$

then the matrix representing ϕ_p with respect to this basis is

$$\phi_p = \begin{bmatrix} a & b \\ c & d \end{bmatrix}.$$

We check that

$$\begin{aligned}
e_{p^\infty}(x, y)^{\deg(\phi)} &= e_{p^\infty}(\deg(\phi)x, y) && \text{(by bilinearity of } e_{p^\infty}) \\
&= e_{p^\infty}((\widehat{\phi})_p(\phi_p(x)), y) \\
&= e_{p^\infty}(\phi_p(x), \phi_p(y)) && \text{(since } \widehat{\widehat{\phi}} = \phi, \text{ see Thm. 3.6.2 [Sil09, Theorem III.6.2];} \\
&&& \text{as well as Prop. 3.8.5 [Sil09, Proposition III.8.3])} \\
&= e_{p^\infty}(ax + cy, bx + dy) \\
&= e_{p^\infty}(x, y)^{ad-bc} && \text{(by similar calculations as those in Cor. 3.8.2)} \\
&= e_{p^\infty}(x, y)^{\det(\phi_p)}.
\end{aligned}$$

Since e_{p^∞} is nondegenerate, this forces $\det(\phi_p) = \deg(\phi) \in \mathbb{Z}$. The trace formula follows from the fact that for any matrix $A \in \mathrm{Mat}_{2\times 2}(k)$, one has

$$\mathrm{tr}(A) = 1 + \det(A) - \det(1 - A). \qquad \square$$

Remark 3.8.2. Let us consider the case where E is defined over a finite field $\mathbb{F}_q$ and $\phi := F_q$ is q-power Frobenius. We know by Proposition 2.2.7 ([Sil09, Proposition II.2.11]) that $\deg(F_q) = q$. One can also show that $\deg(1 - F_q) = \#E(\mathbb{F}_q)$. Thus, for any prime $\ell \neq p$, we have from Proposition 3.8.6 above that

$$\mathrm{tr}((F_q)_\ell) = 1 + q - \#E(\mathbb{F}_q).$$

This number is called the **trace of (q-power) Frobenius of E;** it is denoted by $a_q(E)$, and is independent of ℓ. In §5.1, we will prove the *Hasse-Weil bound,* which is a bound on $a_q(E)$; this also translates to a bound on the number of $\mathbb{F}_q$-rational points on E.

Exercise 3.8.1. [Sil09, Exercise 3.26] Let $E_{/k}$ be the elliptic curve $y^2 = x^3 + x$ having complex multiplication by $\mathbb{Z}[i]$, let $p \geq 3$ be a prime, and let $T \in E[p]$ be a point of order p. In each of the following situations, prove that $\{T, [i]T\}$ is a basis for $E[p]$, and thus $e_p(T, [i]T)$ is a primitive p'th root of unity.

a. $p \equiv 3 \pmod 4$.
b. $i \notin k$ and $T \in E(k)$.

The map $[i]$ is an example of a *distortion map.*

Exercise 3.8.2. **Prerequisite: algebraic number theory.** This exercise proves some properties that the mod-n Galois representation of an elliptic curve can satisfy.

Fix an integer $n \in \mathbb{Z}^+$ and an algebraic extension $F/\mathbb{Q}$. Let

$$\chi_n \colon G_F \to (\mathbb{Z}/n\mathbb{Z})^\times$$

denote the *mod-n cyclotomic character on G_F,* which describes the action of G_F on the group $\mu_n \subseteq \overline{\mathbb{Q}}$ of n'th roots of unity.

a. Prove that if each prime $p \mid n$ is unramified in F, then χ_n is surjective. Deduce that χ_n is always surjective when $F = \mathbb{Q}$.
b. Prove that for any elliptic curve $E_{/\mathbb{Q}}$ and any integer $n \in \mathbb{Z}^+$, one has $\det(\rho_{E,n}(G_\mathbb{Q})) = (\mathbb{Z}/n\mathbb{Z})^\times$.
c. Suppose that $F/\mathbb{Q}$ is a real algebraic extension. Prove that for any elliptic curve $E_{/F}$, there exists an order two element $m \in \rho_{E,n}(G_F)$ with trace 0 and determinant -1.

3.9. **The endomorphism ring.** In this section, we will further describe the endomorphism ring $\mathrm{End}(E)$ of an elliptic curve E. So far, we know the following hold:

1. $\mathrm{End}(E)$ has characteristic zero and no nonzero zero-divisors, and rank ≤ 4 as a $\mathbb{Z}$-module, by Proposition 3.4.1 ([Sil09, Proposition III.4.2]) and Corollary 3.7.3 ([Sil09, Theorem III.7.4]), respectively.
2. $\mathrm{End}(E)$ has an *anti-involution,* namely $\phi \mapsto \widehat{\phi}$.[10] See Theorem 3.6.2 ([Sil09, Theorem III.6.2]).
3. For $\phi \in \mathrm{End}(E)$, the product $\phi\widehat{\phi}$ is a non-negative integer, and $\phi\widehat{\phi} = [0]$ if and only if $\phi = [0]$. See Theorem 3.6.2.

[10]Recall that for a ring R, and *involution* on R is a map $\widehat{\cdot}\colon R \to R$ such that for all $a, b \in R$, one has $\widehat{\widehat{a}} = a$ and $\widehat{(a+b)} = \widehat{a} + \widehat{b}$. We say such an involution is an *anti-involution* if $\widehat{ab} = \widehat{b}\widehat{a}$.

4. If $\mathrm{char}(k) = 0$, then $\mathrm{End}(E)$ is commutative, by Corollary 3.5.6 ([Sil09, Corollary III.5.6]).

As it turns out, a ring with the first 3 properties is a specific type of ring. This will allow us to characterize $\mathrm{End}(E)$ even further.

Before we describe $\mathrm{End}(E)$, let us define some algebraic structures.

Definition 3.9.1. A ring R (not necessarily commutative) is called a **k-algebra** if there exists a ring homomorphism $k \to R$ such that k lies in the center of R, i.e., elements in the image of $k \to R$ commute with all elements of R. Note that R is then a k-vector space.

For example, if ℓ/k is a field extension, then ℓ is naturally a k-algebra via the inclusion $k \hookrightarrow \ell$.

Definition 3.9.2. Let $\mathcal{K}$ be a $\mathbb{Q}$-algebra that is finitely generated over $\mathbb{Q}$. Then an **order** of $\mathcal{K}$ is a subring $R \subseteq \mathcal{K}$ that is finitely generated as a $\mathbb{Z}$-module, and satisfies $R \otimes \mathbb{Q} = \mathcal{K}$.

Example 3.9.1. If F is a number field, then its ring of integers $\mathcal{O}_F$ is an order of F. More generally, any $\mathbb{Z}$-finitely generated subring of F which contains an integral basis of F is an order. For a more specific example, if $K = \mathbb{Q}(\sqrt{d})$ is a quadratic field, then for each $f \in \mathbb{Z}^+$, the ring

$$\mathbb{Z}[1, f\sqrt{d}] := \{a + bf\sqrt{d} : a, b \in \mathbb{Z}\}$$

is an order of K.

Definition 3.9.3. A **(definite) quaternion algebra over** $\mathbb{Q}$ is a $\mathbb{Q}$-algebra of the form

$$\mathcal{K} = \mathbb{Q}[1, \alpha, \beta, \alpha\beta]$$

whose multiplication satisfies

$$\alpha^2, \beta^2 \in \mathbb{Q}, \qquad \alpha^2 < 0, \qquad \beta^2 < 0, \qquad \beta\alpha = -\alpha\beta.$$

Remark 3.9.1. Let us briefly explain some of the adjectives above. While these definitions will not matter much in these notes, it might be interesting to know more about them. A great mathematical reference for quaternion algebras is [VoiQA].

A **quaternion** algebra over $\mathbb{Q}$ is one which satisfies the first and fourth properties above. This was named after *Hamilton's quaternions,* which is the $\mathbb{R}$-algebra $\mathbb{H} := \mathbb{R}[1, \alpha, \beta, \alpha\beta]$ satisfying the properties in Definition 3.9.3, as well as $\alpha^2 = \beta^2 = -1$.

The term *definite* refers to the splitting behavior of the "infinite place" of $\mathbb{Q}$, denoted by ∞, which corresponds to the usual complex absolute value $|\cdot| : \mathbb{C} \to \mathbb{R}$. In general, given a *place* $p \in \mathbb{Z}^+ \cup \{\infty\}$, one says that a quaternion algebra $\mathcal{K}$ over $\mathbb{Q}$ *splits* at p if $\mathcal{K} \otimes \mathbb{Q}_p \cong \mathrm{Mat}_{2\times 2}(\mathbb{Q}_p)$ (where we take $\mathbb{Q}_\infty := \mathbb{R}$). otherwise, $\mathcal{K}$ is said to be *ramified* at p. When $\mathcal{K}$ is ramified at ∞, we say that $\mathcal{K}$ is **definite.** One can show that $\mathcal{K}$ is definite if and only if $\mathcal{K} \otimes_{\mathbb{Q}} \mathbb{R} \cong \mathbb{H}$, iff $\alpha^2, \beta^2 < 0$ (see [VoiQA, Chapter 14]).

Theorem 3.9.1. [Sil09, Theorem III.9.3] *Let R be a ring with characteristic zero and no nonzero zero-divisors. Suppose that R has the following properties:*

1. R has rank ≤ 4 as a $\mathbb{Z}$-module.

2. R has an anti-involution $\widehat{\cdot}\colon R \to R$ satisfying

$$\widehat{\alpha+\beta} = \widehat{\alpha}+\widehat{\beta}, \qquad \widehat{\alpha\beta} = \widehat{\beta}\widehat{\alpha}, \qquad \widehat{\widehat{\alpha}} = \alpha, \qquad \widehat{a} = a \text{ for all } a \in \mathbb{Z}.$$

3. For $\alpha \in R$, the product $\alpha\widehat{\alpha} \in \mathbb{Z}_{\geq 0}$, and $\alpha\widehat{\alpha} = 0$ if and only if $\alpha = 0$.

Then R is one of the following types of rings:

1. $R \cong \mathbb{Z}$.
2. R is an order in an imaginary quadratic field.
3. R is an order in a quaternion algebra over $\mathbb{Q}$.

Corollary 3.9.2. [Sil09, Corollary III.9.4] *For an elliptic curve $E_{/k}$, one has that* $\mathrm{End}(E)$ *is either $\mathbb{Z}$, an order in an imaginary quadratic field, or an order in a quaternion algebra over $\mathbb{Q}$. If* $\mathrm{char}(k) = 0$*, then only the first two are possible.*

Proof. This is a consequence of the previous theorem, combined with our observations about $\mathrm{End}(E)$ at the start of this section. When $\mathrm{char}(k) = 0$, we know by Corollary 3.5.6 ([Sil09, Corollary III.5.6]) that $\mathrm{End}(E)$ is commutative; this concludes our proof, noting that quaternion algebras over $\mathbb{Q}$ cannot be commutative (double-check it!). □

Remark 3.9.2. It is worth noting that if k is a finite field, then $\mathrm{End}(E)$ is always larger than $\mathbb{Z}$, see [Sil09, Theorem V.3.1].

3.10. **The automorphism group.** In comparison to the description of the endomorphism ring $\mathrm{End}(E)$ of an elliptic curve E, the description of its automorphism group $\mathrm{Aut}(E)$ is much simpler.

Theorem 3.10.1. [Sil09, Theorem III.10.1] *Let E be an elliptic curve. Then* $\mathrm{Aut}(E)$ *is a group of order dividing 24. The order of* $\mathrm{Aut}(E)$ *is given in the following table:*

$\mathrm{Aut}(E)$	$j(E)$	$\mathrm{char}(k)$
2	$j(E) \neq 0, 1728$	–
4	$j(E) = 1728$	$\mathrm{char}(k) \neq 2, 3$
6	$j(E) = 0$	$\mathrm{char}(k) \neq 2, 3$
12	$j(E) = 0, 1728$	$\mathrm{char}(k) = 3$
24	$j(E) = 0, 1728$	$\mathrm{char}(k) = 2$

Proof. For simplicity, let us assume that $\mathrm{char}(k) \neq 2, 3$ (these cases are handled in Appendix A of [Sil09]). Then E has an equation

$$E : y^2 = x^3 + Ax + B.$$

Since every automorphism $\phi\colon E \to E$ takes this equation to itself, by the remarks preceding Figure 3.1.1 in §3.1, this implies that ϕ has the form

$$\phi(x, y) = (u^2 x, u^3 y)$$

for some $u \in \overline{k}^\times$. It follows by Figure 3.1.1 that this forces

$$u^4 A = A \qquad \text{and} \qquad u^6 = B.$$

If $AB \neq 0$, i.e., if $j(E) \neq 0, 1728$, then $u \in \mu_4 \cap \mu_6 = \mu_2$, i.e., $u = \pm 1$, and thus $\phi(x, y) = (x, \pm y) = [\pm 1](x, y)$, so that $\phi = [\pm 1]$. If $B = 0$, then $A \neq 0$, and thus $u^4 = 1$ (we also have $j(E) = 1728$ by the formulas). this gives 4 automorphisms of E,

corresponding to $(x, y) \mapsto (\zeta^2 x, \zeta^3 y)$ where $\zeta \in \mu_4$. Finally, if $A = 0$ then $B \neq 0$, and thus $u^6 = 1$ (we also find that $j(E) = 0$). Thus there are 6 automorphisms of E, given by $(x, y) \mapsto (\zeta^2 x, \zeta^3 y)$ where $\zeta \in \mu_6$. We conclude that $\mathrm{Aut}(E)$ is cyclic of order 2, 4 or 6, depending on whether $AB \neq 0$, $B = 0$ or $A = 0$, respectively. □

When E is defined over k, the proof of the above theorem gives the structure of $\mathrm{Aut}(E)$ as a G_k-module when $\mathrm{char}(k) \neq 2, 3$.

Corollary 3.10.2. [Sil09, Corollary III.10.2] *Assume that* $\mathrm{char}(k) \neq 2, 3$*, and let* $E_{/k}$ *be an elliptic curve. Set*

$$n := \begin{cases} 2 & \text{if } j(E) \neq 0, 1728 \\ 4 & \text{if } j(E) = 1728 \\ 6 & \text{if } j(E) = 0. \end{cases}$$

Then there is a natural isomorphism of G_k*-modules*

$$\mu_n \cong_{G_k} \mathrm{Aut}(E).$$

Proof. In the proof above, we demonstrated a group isomorphism

$$[\cdot] \colon \mu_n \to \mathrm{Aut}(E), \qquad [\zeta](x, y) := (\zeta^2 x, \zeta^3 y).$$

This is a G_k-module isomorphism since it commutes with the action of G_k, i.e., for all $\sigma \in G_k$ and for all $(x, y) \in E$, one has

$$[\zeta^\sigma](x, y) = [\zeta]^\sigma(x, y).$$

(Recall that for a smooth curve morphism $\phi = [f_0 : f_1 : \ldots : f_n] \colon C_1 \to C_2$, the morphism $\phi^\sigma \colon C_1 \to C_2$ is defined as $\phi^\sigma = [f_0^\sigma : f_1^\sigma : \ldots : f_n^\sigma]$, where f_i^σ is the rational function f_i with σ applied to its coefficients. In general, we have the formula $(\phi(P))^\sigma = \phi^\sigma(P^\sigma)$.) □

5. Elliptic Curves Over Finite Fields

We will spend a brief amount of time in this chapter, in the interest of spending more time in Chapters 7, 8 and 10. In this section, we will prove the *Hasse-Weil bound* for elliptic curves over finite fields, which is a bound on their point counts (as well as their trace of Frobenius). Throughout this section, fix a prime $p \in \mathbb{Z}^+$ and a power $q := p^r > 1$; we will let $k := \mathbb{F}_q$ denote the finite field of q elements.

5.1. **Number of rational points.** Given an elliptic curve $E_{/\mathbb{F}_q}$, its Mordell-Weil group $E(\mathbb{F}_q)$ is finite (and consequently $E(\mathbb{F}_q) = E(\mathbb{F}_q)[\text{tors}]$). Thus, one way to understand its Mordell-Weil group is to understand its size $\#E(\mathbb{F}_q)$.

Suppose we wish to bound the number of $\mathbb{F}_q$-rational points of an elliptic curve $E_{/\mathbb{F}_q}$ general Weierstrass form,

$$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6.$$

We have a crude upper bound $\#E(\mathbb{F}_q) \leq q^2+1$. In fact, observing that for each $x \in \mathbb{F}_q$, there are at most two points on E with x-coordinate x (by completing the square and solving for y), we have the better bound $\#E(\mathbb{F}_q) \leq 2q + 1$. However, a "random" quadratic equation has a 50% chance of being solvable in x, so we'd expect that the number $\#E(\mathbb{F}_q)$ is closer to q. This is confirmed by the *Hasse-Weil bound.*

Theorem 5.1.1 (Hasse-Weil)**.** [Sil09, Theorem V.1.1] *Let $E_{/\mathbb{F}_q}$ be an elliptic curve. Then*

$$|\#E(\mathbb{F}_q) - (q + 1)| \leq 2\sqrt{q}.$$

This section will be devoted to proving the Hasse-Weil bound.

Remark 5.1.1. Recall that for an elliptic curve $E_{/\mathbb{F}_q}$, its trace of Frobenius is

$$a_q(E) := 1 + q - \#E(\mathbb{F}_q).$$

Thus, the Hasse-Weil bound says that $|a_q(E)| \leq 2\sqrt{q}$.

Our proof of this theorem will use the following fact about positive definite quadratic forms, which is a sort of Cauchy-Schwarz inequality.

Lemma 5.1.2. [Sil09, Lemma V.1.2] *Let G be an abelian group, and let*

$$d\colon G \to \mathbb{Z}$$

be a positive definite quadratic form. Then for all $g, h \in G$, one has

$$|d(g - h) - d(g) - d(h)| \leq 2\sqrt{d(g)d(h)}.$$

With this lemma, let us prove the Hasse-Weil bound.

Proof. Fix a Weierstrass equation for E. Let

$$F_q\colon E \to E, \qquad\qquad F_q(x, y) := (x^q, y^q)$$

be q-power Frobenius. By abuse of notation, we let $F_q\colon \overline{\mathbb{F}_q} \to \overline{\mathbb{F}_q}$ also denote the q-power map on fields. Since $G_{\mathbb{F}_q}$ is (topologically) generated by F_q,[11] we have that $\alpha \in \overline{\mathbb{F}_q}$ is F_q-rational if and only if $\alpha \in \mathbb{F}_q$. It follows that a point $(x, y) \in E$ is $\mathbb{F}_q$-rational if and only if $F_q(x, y) = (x, y)$, iff $(x, y) \in \ker(1 - F_q)$, where $1 - F_q := [1] - F_q\colon E \to E$. In particular, we have

$$\#E(\mathbb{F}_q) = \#\ker(1 - F_q).$$

We recall by Corollary 3.5.5 ([Sil09, Corollary III.5.5]) that the endomorphism $1 - F_q\colon E \to E$ is separable. Thus, by Theorem 3.4.4 ([Sil09, Theorem III.4.10]), we have

$$\#E(\mathbb{F}_q) = \#\ker(1 - F_q) = \deg(1 - F_q). \tag{11}$$

Finally, we have previously shown that the degree map $\deg\colon \mathrm{End}(E) \to \mathbb{Z}_{\geq 0}$ is a positive definite quadratic form, see Corollary 3.6.4 ([Sil09, Corollary III.6.3]). Therefore, applying the Cauchy-Schwarz lemma above, we conclude that

$$|\deg(1 - F_q) - \deg([1]) - \deg(F_q)| \leq 2\sqrt{\deg([1])\deg(F_q)};$$

since $\deg(F_q) = q$ by Proposition 2.2.7 ([Sil09, Proposition II.2.11]), and since $\deg([1]) = 1$, this inequality simplifies to

$$|\deg(1 - F_q) - 1 - q| \leq 2\sqrt{q}.$$

Then (11) concludes our proof. □

Remark 5.1.2. While understanding point counts over finite fields is intrinsically interesting, it can also help us analyze torsion group sizes over number fields – we will see this in §7.3, when we explore the notion of *reduction* of an elliptic curve.

Exercise 5.1.1. This exercise gives a formula for point counts of elliptic curves base-changed over finite fields. If $q \in \mathbb{Z}^+$ is a prime power and $E_{/\mathbb{F}_q}$ is an elliptic curve, then writing

$$x^2 - a_q(E)x + q = (x - \alpha)(x - \beta)$$

where $\alpha, \beta \in \overline{\mathbb{Q}}$, this exercise shows that for all $n \in \mathbb{Z}^+$, one has

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

a. Writing $F_q\colon E \to E$ for q-power Frobenius, prove that

$$F_q^2 - a_q(E)F_q + q = [0].$$

b. For the polynomial

$$f_n(x) := (x^n - \alpha^n)(x^n - \beta^n),$$

show that $f_n(x) = x^{2n} - (\alpha^n + \beta^n)x^n + q$. Then prove that $x^2 - a_q(E)x + q$ divides $f_n(x)$ in $\mathbb{Z}[x]$.

[11] One way to see this is to note that every finite extension of $\mathbb{F}_q$ has the form $\mathbb{F}_{q^s}$ for some $s \geq 1$, and thus $\mathrm{Gal}(\mathbb{F}_{q^s}/\mathbb{F}_q) = \langle F_q \rangle$. Then note that $G_{\mathbb{F}_q}$ is the inverse limits of these Galois groups, where $F_q \in G_{\mathbb{F}_q}$ is defined on each $\mathbb{F}_{q^s}$ in a compatible way.

c. Deduce that we can write

$$f_n(x) = g_n(x) \cdot (x^2 - a_q(E)x + q)$$

for some $g_n(x) \in \mathbb{Z}[x]$. Use this and part a. to prove that

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

Exercise 5.1.2. Let $p > 2$ be a prime, and let $E_{/\mathbb{F}_p}$ be the elliptic curve

$$E : y^2 = x^3 + x.$$

a. Prove that if $p \equiv 1 \pmod 4$, then

$$4 \mid \#E(\mathbb{F}_p).$$

b. Prove that if $p \equiv 3 \pmod 4$, then

$$\#E(\mathbb{F}_p) = p + 1,$$

i.e., $a_p(E) = 0$.

Thus, in both cases we have $4 \mid \#E(\mathbb{F}_p)$.

c. Create a computer program that does the following: given a prime $p \in \mathbb{Z}^+$ and an elliptic curve $E_{/\mathbb{F}_p} : y^2 = x^3 + Ax + B$, it returns the set $E(\mathbb{F}_p)$, as well as the size $\#E(\mathbb{F}_p)$. What patterns do you notice for $E : y^2 = x^3 + x$ when $p \equiv 1 \pmod 4$, beyond part a.? Based on your calculations, make a reasonable conjecture – and prove it if you can!

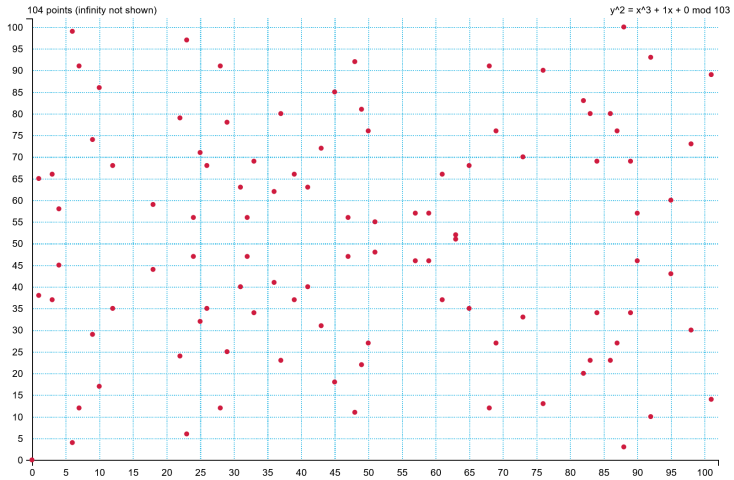


FIGURE 5.1.1. The elliptic curve $E : y^2 = x^3 + x$ over $\mathbb{F}_{103}$.

Exercise 5.1.3. Let $E_{/k}$ be an elliptic curve. This exercise explores the structure of $E(k)[\text{tors}]$ over various fields.

a. Prove there exist $m, n \in \mathbb{Z}^+$ with $m \mid n$, such that

$$E(k)[\text{tors}] \cong \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}.$$

b. Show that if $k = F$ is a real number field, then there exists $n \in \mathbb{Z}^+$ such that

$$E(F)[\text{tors}] \cong \begin{cases} \mathbb{Z}/n\mathbb{Z} \\ \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2n\mathbb{Z}. \end{cases}$$

c. Show that if $k = \mathbb{F}_q$ is a finite field, then there exist $m, n \in \mathbb{Z}^+$ with $m \mid n$ and $q \equiv 1 \pmod{m}$, such that

$$E(\mathbb{F}_q) \cong \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}.$$

d. Show that if $k = \overline{\mathbb{Q}}$, then

$$E(\overline{\mathbb{Q}})[\text{tors}] \cong (\mathbb{Q}/\mathbb{Z}) \times (\mathbb{Q}/\mathbb{Z}).$$

Exercise 5.1.4.

a. Suppose that $E_{/k}$ and $E'_{/k}$ are k-rationally isogenous elliptic curves. Prove that their k-endomorphism algebras are isomorphic, i.e., $\text{End}_k(E) \otimes \mathbb{Q} \cong \text{End}_k(E') \otimes \mathbb{Q}$.

b. Let $E_{/\mathbb{F}_q}$ and $E'_{/\mathbb{F}_q}$ be elliptic curves, and suppose there exists an $\mathbb{F}_q$-rational isogeny $\phi\colon E \to E'$. Prove that $\#E(\mathbb{F}_{q^r}) = \#E'(\mathbb{F}_{q^r})$ for all $r \geq 1$. (The converse is also true, see [Sil09, Exercise 5.4] or [Tat66].)

7. Elliptic Curves Over Local Fields

In this chapter, we will study rational points on elliptic curves over *local fields.* As we will see, this will allow us to determine information about elliptic curves over *global fields,* which for us will be number fields. A key idea we will explore is that of *reduction* of an elliptic curve. See Appendix A for a brief review of local fields.

A theorem we will work towards proving is the *Néron-Ogg-Shafarevich criterion,* which will connect the reduction type of an elliptic curve to its Galois representations. Note that we are black-boxing results on formal groups in these notes. Throughout this chapter, we will use the following notation and assumptions:

- K is a perfect local field, complete with respect to a discrete valuation $v\colon K \twoheadrightarrow \mathbb{Z} \cup \{\infty\}$.
- R is the discrete valuation ring of (K, v), i.e.,
$$R := \{x \in K : v(x) \geq 0\}.$$
- $R^\times = \{x \in K : v(x) = 0\}$ is the unit group of R.
- $M := \{x \in K : v(x) > 0\}$ is the maximal ideal of R.
- π is a uniformizer of R, i.e., $(\pi)R = M$.
- $k := R/M$ is the residue field of R. We assume that k is perfect.

Note that each element $x \in K^\times$ has the form $x = u\pi^n$, where $n \in \mathbb{Z}$ and $u \in R^\times$. Our canonical example of a local field is the field of p-adic numbers, denoted $\mathbb{Q}_p$, which is complete with respect to the p-adic valuation $v_p\colon \mathbb{Q} \twoheadrightarrow \mathbb{Z} \cup \{\infty\}$.

7.1. Minimal Weierstrass equations.

Ultimately, in this chapter we are interested in reducing elliptic curves defined over local fields into curves over finite fields. Different types of equations for an elliptic curve will give different reduced equations, some of which can be singular. However, with *minimal equations,* the reduction type will be a well-defined invariant of the curve.

Let $E_{/K}$ be an elliptic curve in Weierstrass form:

$$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6,$$

where each $a_i \in K$. By §3.1, for $u \in \overline{K}^\times$ the change in variables $x \mapsto u^{-2}x$ and $y \mapsto u^{-3}y$ gives a new Weierstrass equation where each a_i is replaced with $u^i a_i$ (and Δ is replaced with $u^{12}\Delta$). Thus, if we choose $u \in R$ to be sufficiently divisible by π, then we can "clear denominators" and assume that each a_i is in R, so that our equation is R-integral. We call such an equation an *R-Weierstrass equation.*

Since our equation is R-Weierstrass, we can check with the formula in §3.1 that the discriminant $\Delta := \Delta_{E,K}$ satisfies $v(\Delta_{E,K}) \geq 0$, i.e., $\Delta_{E,K} \in R$. By well-ordering, there exists an R-Weierstrass equation for E with $v(\Delta)$ minimal in $\mathbb{Z}_{\geq 0}$. We call such an equation a **minimal Weierstrass equation for E with respect to v,** or a **minimal R-Weierstrass equation.** The value $v(\Delta)$ is the **valuation of the minimal discriminant of E at v.**

Remark 7.1.1. One way to spot whether you have a minimal equation is the following. By Figure 3.1.1 (see §3.1), we know that a change of variables $x \mapsto u^2x' + r$ and $y \mapsto u^3y' + u^2sx' + t$, where $r, s, t, u \in \overline{K}$ and $u \neq 0$, will change the discriminant into

$\Delta' = u^{-12}\Delta$; in particular, $v(\Delta)$ changes by adding or subtracting multiples of 12. We conclude that

$$a_i \in R \text{ and } v(\Delta) < 12 \qquad \Rightarrow \qquad \text{the equation is minimal.}$$

Also recall there are invariants c_4 and c_6 in terms of the a_i, where a change of variables gives new values $c_4' = u^{-4}c_4$ and $c_6' = u^{-6}c_6$. One can use this and the relation $1728\Delta = c_4^3 - c_6^2$ to show that

$$a_i \in R \text{ and } v(c_4) < 4 \qquad \Rightarrow \qquad \text{the equation is minimal,}$$
$$a_i \in R \text{ and } v(c_6) < 6 \qquad \Rightarrow \qquad \text{the equation is minimal.}$$

If $\mathrm{char}(k) \neq 2, 3$, then the converse holds: i.e., if the equation is minimal, then $v(\Delta) < 12$ or $v(c_4) < 4$. "Tate's algorithm" also determines whether an equation is minimal, see e.g. [Sil94, Chapter IV, §9].

Example 7.1.1. Fix a prime p, and consider the elliptic curve

$$E : y^2 + xy + y = x^3 + x^2 + 22x - 9$$

over $\mathbb{Q}_p$. Then $\Delta = -2^{15} \cdot 5^2$. Thus, if $p > 2$ then this is a minimal equation by the remark above, since $v_p(\Delta) < 12$. One checks that $c_4 = -5 \cdot 211$, and so it is also minimal when $p = 2$ by our remark.

For another example, consider

$$E : y^2 = x^3 + 3.$$

Then $\Delta = -2^4 \cdot 3^5$, which means that E is minimal for all p.

We summarize some observations concerning minimal Weierstrass equations (which essentially follow from Weierstrass equation facts, combined with K being a local field).

Proposition 7.1.1. [Sil09, Proposition VII.1.3]

a. Every elliptic curve $E_{/K}$ has a minimal R-Weierstrass equation.

b. A minimal equation is unique up to change of coordinates

$$x := u^2x' + r \qquad \text{and} \qquad y := u^3y' + u^2sx' + t,$$

where $r, s, t, u \in R$ and $u \in R^\times$.

c. The invariant differential

$$\omega = \frac{dx}{2y + a_1x + a_3}$$

for a minimal equation is unique up to multiplication by an element of $R^\times$.

d. Conversely, any change of coordinates

$$x := u^2x' + r \qquad \text{and} \qquad y := u^3y' + u^2sx' + t,$$

between two minimal R-Weierstrass equations satisfies $r, s, t, u \in R$.

7.2. **Reduction modulo π.** Given an elliptic curve $E_{/K}$ with an R-Weierstrass equation

$$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6,$$

we can obtain a new curve $\tilde{E}$ over the residue field $k := R/M$ by reducing the coefficients modulo π:

$$\tilde{E} : y^2 + \tilde{a_1}xy + \tilde{a_3}y = x^3 + \tilde{a_2}x^2 + \tilde{a_4}x + \tilde{a_6}.$$

This curve $\tilde{E}$ is called the **reduction of E modulo π.** If we assume the equation of E is minimal, then this equation for $\tilde{E}$ is *unique* up to change of coordinates over k by part b. of Proposition 7.1.1 ([Sil09, Proposition VII.1.3]). Furthermore, two R-minimal equations E_1 and E_2 for E will have equal discriminant valuation $v(\Delta)$ when $v(\Delta) < 12$. Therefore, $\tilde{E_1}$ is nonsingular if and only if $\tilde{E_2}$ is nonsingular, iff $v(\Delta) = 0$.

It is important to note that $\tilde{E}$ might not be an elliptic curve, since it could be singular. For example, for prime $p > 2$, the elliptic curve

$$E_{/\mathbb{Q}_p} : y^2 = x^3 + 3$$

is $\mathbb{Z}_p$-minimal since, as noted in the previous section, we have $\Delta = -2^4 \cdot 3^5$, and so $v_p(\Delta) < 12$. However, if $p = 3$, then reducing the coefficients modulo 3 gives the singular (cuspidal) curve

$$\tilde{E} : y^2 = x^3.$$

Despite this, any curve given by a Weierstrass equation will still have a group law via the chord and tangent method, *as long as we exclude the singular points.*

Notes Exercise 7.2.1. Show that for a field k with $\mathrm{char}(k) \neq 2$, a curve in short Weierstrass form,

$$C : y^2 = x^3 + Ax + B,$$

has at most one singular point, and it must have the form $(\alpha, 0)$. Also show that the point at infinity is always nonsingular.

Let us review some of §3.2 on singular Weierstrass equations. Here is a proposition from §3.1 that we partially stated, see Proposition 3.1.1.

Proposition 7.2.1. [Sil09, Proposition III.1.4] *Let C be a curve in Weierstrass form over a field k.*

i. C is nonsingular if and only if $\Delta \neq 0$.
ii. C is singular with a node if and only if $\Delta = 0$ and $c_4 \neq 0$.
iii. C is singular with a cusp if and only if $\Delta = 0$ and $c_4 = 0$.

In cases ii. and iii., there is exactly one singular point.

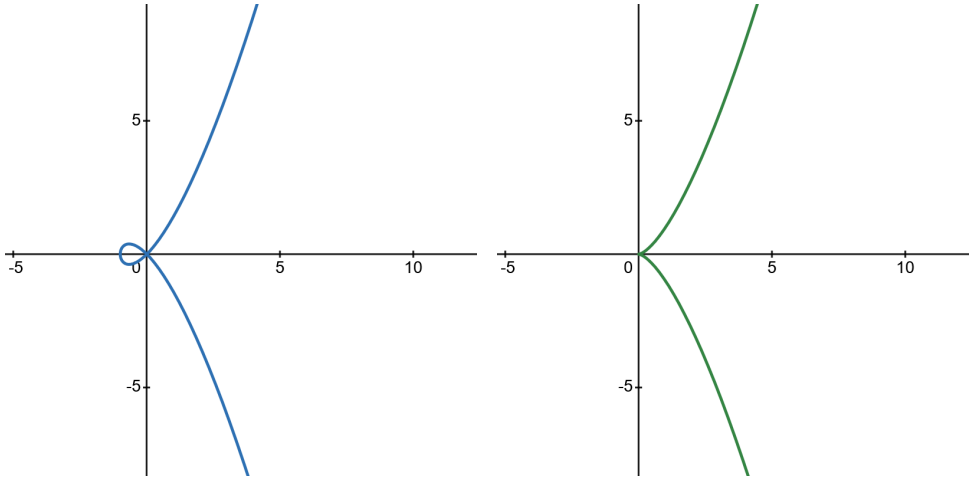


FIGURE 7.2.1. The curves $C_1 : y^2 = x^3 + x^2$ (nodal) and $C_2 : y^2 = x^3$ (cuspidal).

As mentioned, the chord and tangent method still gives a group law on nodal and cuspidal Weierstrass equations, so long as we exclude the single singular point. For a curve C, we write C_{ns} to denote the set of nonsingular points on C.

Proposition 7.2.2. [Sil09, Proposition III.2.5] *Let C be a curve given by a singular Weierstrass equation, i.e., assume that $\Delta = 0$. Let $S \in C$ be its singular point; then $C_{\text{ns}} := C \smallsetminus \{S\}$ is a group under the chord and tangent method.*

a. Suppose that C has a node, i.e., suppose that $c_4 \neq 0$. Let

$$y = m_1 x + b_1 \qquad \text{and} \qquad y = m_2 x + b_2$$

be the distinct tangent lines to C at S. Then the map

$$C_{\text{ns}} \to \overline{k}^{\times}, \qquad (x, y) \mapsto \frac{y - m_1 x - b_1}{y - m_2 x - b_2}$$

is an isomorphism of groups.

b. Suppose that C has a cusp, i.e., suppose that $c_4 = 0$. Let

$$y = mx + b$$

be the tangent line to C at S. Then the map

$$C_{\text{ns}} \to \overline{k}, \qquad (x, y) \mapsto \frac{x - x(S)}{y - mx - b}$$

is an isomorphism.

Remark 7.2.1. It is worth noting that for a singular curve $C_{/k}$ in Weierstrass form, there is an analogous description of $C(k)$ – see Exercise 7.2.1 ([Sil09, Exercise 3.5]).

Back to §7.2, with local field notation. We observed that an elliptic curve $E_{/K}$ given by an R-Weierstrass equation

$$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$

can be reduced modulo π, to obtain a new curve over k,

$$\tilde{E} : y^2 + \tilde{a_1}xy + \tilde{a_3}y = x^3 + \tilde{a_2}x^2 + \tilde{a_4}x + \tilde{a_6}.$$

We have a *reduction map* from E to $\tilde{E}$: given a point $P \in E(K)$, we can write $P = [x_0 : y_0 : z_0]$ where $x_0, y_0, z_0 \in R$ and at least one of x_0, y_0 or z_0 is in $R^\times$ (multiply all terms by the appropriate power of π). It follows that

$$\tilde{P} := [\tilde{x_0} : \tilde{y_0} : \tilde{z_0}] \in \tilde{E}(k).$$

This gives the **reduction map**

$$\text{red}\colon E(K) \to \tilde{E}(k)$$

by $P \mapsto \tilde{P}$. This is a special case of an identically defined reduction map

$$\text{red}\colon \mathbb{P}^n(K) \to \mathbb{P}^n(k).$$

We know that $\tilde{E}_{\text{ns}}$ is a group under the chord and tangent method; thus, it is natural to ask whether reduction is a group homomorphism. As it turns out, it is if we change the domain to the subgroup of $E(K)$ of points which reduce to nonsingular points on $\tilde{E}$. In fact, we can show more: let us define both

$$E_0(K) := \{P \in E(K) : \tilde{P} \in \tilde{E}_{\text{ns}}(k)\}$$

and

$$E_1(K) := \{P \in E(K) : \tilde{P} = \tilde{O}\}.$$

Proposition 7.2.3. [Sil09, Proposition VII.2.1] *The sequence of maps*

$$0 \to E_1(K) \to E_0(K) \xrightarrow{\text{red}} \tilde{E}(k) \to 0$$

is a short exact sequence of abelian groups.

Proof. It is clear that if $E_0(K)$ is a subgroup of $E(K)$, and if $\text{red}\colon E_0(K) \to \tilde{E}_{\text{ns}}(k)$ is a surjective homomorphism, then the sequence is an exact sequence of abelian groups. Let us first prove that reduction is surjective. Choose a minimal R-Weierstrass equation

$$E : f(x, y) = 0.$$

It follows that $\tilde{E}$ has equation

$$\tilde{E} : \tilde{f}(x, y) = 0,$$

where $\tilde{f} \in k[x, y]$ is the polynomial obtained by reducing the coefficients of $f(x, y)$ modulo π. Let $q = (\alpha, \beta) \in \tilde{E}_{\text{ns}}(k)$ be a point; we must show there exists $Q = (x_0, y_0) \in E(K)$ with $\tilde{Q} = q$, i.e., $(\tilde{x_0}, \tilde{y_0}) = (\alpha, \beta)$.

Since q is a nonsingular point on $\tilde{E}$, we have

$$\left.\frac{\partial \tilde{f}}{\partial x}\right|_q \neq 0 \qquad \text{or} \qquad \left.\frac{\partial \tilde{f}}{\partial y}\right|_q \neq 0.$$

Assume that the second partial is nonzero (the other case is similar). Fix a representative x_0 of α in R; thus $\tilde{x_0} = \alpha$. Consider the single-variable equation $g(y) := f(x_0, y) \in R[y]$. Since $(\alpha, \beta) \in \tilde{E}$, we have $\tilde{g}(\beta) = \tilde{f}(\alpha, \beta) = 0$; however, by the second partial condition, we know that $\tilde{g}'(\beta) \neq 0$. It follows by Hensel's Lemma (Exercise A.0.4) that there exists a lift $y_0 \in R$ of β to a root of $g(y)$; thus, $\tilde{y_0} = \beta$ and $g(y_0) = 0$. The latter condition implies $f(x_0, y_0) = 0$, and thus $(x_0, y_0) \in E_0(K)$ maps to $(\alpha, \beta) \in \tilde{E}(k)$. We deduce that the reduction map is surjective.

Next, we must show that $E_0(K)$ is a group (i.e., the sum of two points which reduce to nonsingular points, also reduces to a nonsingular point), and that reduction is a homomorphism. These can be shown simultaneously: that is, one can show that if $P, Q \in E_0(K)$ and $R \in E(K)$ are collinear points on a line L, then $\tilde{P}, \tilde{Q}$ and $\tilde{R}$ are on the line $\tilde{L}$ with the correct multiplicities. This follows through checking several cases for $\tilde{P}, \tilde{Q}$ and $\tilde{R}$.

We describe the easier case: suppose that $\tilde{P}, \tilde{Q}$ and $\tilde{R}$ are distinct. Then this forces

$$\tilde{L} \cap \tilde{E} = \{\tilde{P}, \tilde{Q}, \tilde{R}\}.$$

Since $\tilde{P}$ and $\tilde{Q}$ are in $\tilde{E}_{\text{ns}}(k)$ by assumption, so is $\tilde{R}$ by the collinearity theorem (Theorem 0.7.4, which also applies to $\tilde{E}_{\text{ns}}$), since $-\tilde{R} = \tilde{P} + \tilde{Q}$ and $\tilde{E}_{\text{ns}}(k)$ is a group by Proposition 7.2.2 ([Sil09, Proposition III.2.5]) (alternatively, note that singular points on curves have intersection multiplicity ≥ 2, see e.g. [Sil09, Exercise 3.28]). We deduce that $R \in E_0(K)$. The main thing checked in this case was that the third point R lies in $E_0(K)$, and not just $E(K)$.

The next case to check is where $\tilde{P} = \tilde{Q} \neq \tilde{R}$. This is where the subtlety appears: it is reasonable to expect that since $\tilde{P} = \tilde{Q}$, one could have $\tilde{L} \cap \tilde{E}_{\text{ns}} \supsetneq \{\tilde{P}, \tilde{R}\}$, i.e., that $\tilde{L}$ is not a tangent line at $\tilde{P}$. However, additional work shows that this $\tilde{L}$ must be such a tangent line, and that $R \in E_0(K)$ and not just $R \in E(K)$. The other cases are also left as an exercise, see [Sil09, Exercise 7.15]. □

Remark 7.2.2. We note that for an elliptic curve $E_{/K}$ in Weierstrass form, if $v(\Delta) = 0$, then $\tilde{\Delta} \neq 0$, and thus $\tilde{E}$ is nonsingular. Therefore, $E_0 = E$ and $\tilde{E}_{\text{ns}} = \tilde{E}$, and our short exact sequence in Proposition 7.2.3 becomes

$$0 \to E_1(K) \to E(K) \xrightarrow{\text{red}} \tilde{E}(k) \to 0.$$

This gives more direct information about $E(K)$. This is the case of *good reduction.* This is discussed in more detail in the upcoming sections.

Can we make better sense of the groups in our short exact sequence of Proposition 7.2.3? When k is a finite field, by Proposition 7.2.2 ([Sil09, Proposition III.2.5]) and the Hasse-Weil bound, we have a decent understanding of the size of $\tilde{E}_{\text{ns}}(k)$. As it turns out, we also have a good understanding of $E_1(K)$. This group is the group associated to the **formal group** associated to E. Chapter 4 of [Sil09] is devoted towards understanding formal groups and their connection to elliptic curves. However, in the interest of time, we have opted not to go over this topic. Thus, we will content ourselves to stating the necessary properties of this formal group.

Proposition 7.2.4. [Sil09, Proposition IV.3.2] *Let $\mathcal{F}_{/R}$ be a formal group. Then writing $p := \mathrm{char}(k)$, the associated group $\mathcal{F}(M)$ has that $\mathcal{F}(M)[\mathrm{tors}] = \mathcal{F}(M)[p^\infty]$, i.e., every torsion element of $\mathcal{F}(M)$ has order a power of p.*

Proposition 7.2.5. [Sil09, Proposition VII.2.2] *Let $E_{/K}$ be an elliptic curve given by a minimal R-Weierstrass equation, let $\widehat{E}_{/R}$ be the formal group associated to E as in* [Sil09, Section 4.2]*, and let $w(z) \in R[[z]]$ be the power series from* [Sil09, Section 4.1]*. Then the map*

$$\widehat{E}(M) \to E_1(K), \qquad z \mapsto \left(\frac{z}{w(z)}, -\frac{1}{w(z)}\right)$$

is an isomorphism of groups (where $0 \mapsto O$). For the definition of $\widehat{E}(M)$, see [Sil09, Section 4.3].

We will soon see that knowing $E_1(K)$ is a formal group over R immediately implies more information about the reduction SES from Proposition 7.2.3.

Exercise 7.2.1. [Sil09, Exercise 3.5] Let k be a perfect field, and let $E_{/k}$ be a singular curve in Weierstrass form.

a. Suppose that E has a node, and let the tangent lines at the node be

$$y = m_1 x + b_1 \qquad \text{and} \qquad y = m_2 x + b_2.$$

   i. If $m_1 \in k$, prove that $m_2 \in k$ and
   $$E_{\mathrm{ns}}(k) \cong k^\times.$$
   (This is the *split* case, see Section 7.5.)
   ii. If $m_1 \notin k$, prove that $\ell := k(m_1, m_2)$ is a quadratic extension of k. Note that i. tells us that $E_{\mathrm{ns}}(k) \subseteq E_{\mathrm{ns}}(\ell) \cong \ell^\times$. Prove that
   $$E_{\mathrm{ns}}(k) \cong \{a \in \ell^\times : N_{\ell/k}(a) = 1\}.$$
   (This is the *nonsplit* case, see Section 7.5.)

b. Suppose that E has a cusp. Prove that
$$E_{\mathrm{ns}}(k) \cong (k, +).$$

Exercise 7.2.2. [Sil09, Exercise 7.1] Assume that $\mathrm{char}(k) \neq 2, 3$.

a. Let $E_{/K}$ be an elliptic curve given by a Weierstrass equation with coefficients $a_i \in R$. Prove that the equation is minimal if and only if either $v(\Delta) < 12$ or $v(c_4) < 4$.

b. Let $E_{/K}$ be given by a minimal Weierstrass equation of the form
$$E : y^2 = x^3 + Ax + B.$$
Prove that E has
   i. *good reduction,* i.e., $\tilde{E}$ is nonsingular, $\iff 4A^3 + 27B^2 \in R^\times$,
   ii. *multiplicative reduction,* i.e., $\tilde{E}$ has a node, $\iff 4A^3 + 27B^2 \in M$ and $AB \in R^\times$,
   iii. *additive reduction,* i.e., $\tilde{E}$ has a cusp, $\iff A \in M$ and $B \in M$.

7.3. **Points of finite order.** Given an elliptic curve $E_{/K}$ in minimal R-Weierstrass form, we proved in Proposition 7.2.3 ([Sil09, Proposition VII.2.1]) there exists a short exact sequence

$$0 \to E_1(K) \to E_0(K) \xrightarrow{\text{red}} \tilde{E}_{\text{ns}}(k) \to 0.$$

We also noted that $E_1(K)$ was a formal group, and thus $E_1(K)[\text{tors}] = E_1(K)[p^\infty]$ where $p := \text{char}(k)$. This lets us prove the following.

Proposition 7.3.1. [Sil09, Proposition VII.3.1] *Let $E_{/K}$ be an elliptic curve and $n \geq 1$ an integer coprime to* $\text{char}(k)$.

a. The subgroup $E_1(K)$ has no nontrivial points of order dividing n.

b. If $\tilde{E}_{/k}$ is nonsingular, then the reduction map

$$\text{red}\colon E(K)[n] \to \tilde{E}(k)$$

is injective.

Proof. Part a. follows by our remark on $E_1(K)$ being a formal group, so it suffices to prove part b. Suppose that $P \in E(K)$ has order dividing n. If P is in the kernel of reduction, then $P \in E_1(K)$; however, by part a. we know that $E_1(K)[n] = \{O\}$, which forces $P = O$. □

This proposition gives us a nice way to compute the torsion group of an elliptic curve E over a number field F. For a nonzero prime ideal $\mathfrak{P} \subseteq F$, one has a natural embedding $F \hookrightarrow F_{\mathfrak{P}}$ where $F_{\mathfrak{P}}$ is the completion at (the discrete valuation on F associated to) $\mathfrak{P}$; thus, we also have an injection $E(F) \hookrightarrow E(F_{\mathfrak{P}})$. The idea is then to show that for some $n \in \mathbb{Z}^+$, one has

$$E(F)[\text{tors}] = E(F)[n^\infty] := \left\{ P \in E(F) : |P| = \prod_{p|n} p^{e_p} \right\}$$

by embedding $E(F_{\mathfrak{P}})[\text{tors}]$ into one of its reductions $\tilde{E}(k)[\text{tors}]$, which has a finite size. Then $E(F)[n^\infty]$ can be analyzed separately, e.g. by embedding $E(F)[n^\infty]$ into another completion $E(F_{\mathfrak{Q}})$ and then applying the same techniques, and/or by computing the number of rational points of reductions $\tilde{E}_{/(\mathcal{O}_F/\mathfrak{Q})}$ and comparing them to the remaining possible orders of torsion points over F.

Example 7.3.1. Consider the elliptic curve

$$E_{/\mathbb{Q}} : y^2 + y = x^3 - x + 1.$$

See its LMFDB page: 611.a1. We compute $\Delta = -611 = -13 \cdot 47$. For each prime $p \in \mathbb{Z}^+$, we have $v_p(\Delta) < 12$, and thus this is a $\mathbb{Z}_p$-minimal model. For any prime $p \neq 13, 47$, since $v_p(\Delta) = 0$ we also see that $\tilde{E}_{/\mathbb{F}_p}$ is nonsingular. In particular, when $p = 2$ we have by Proposition 7.3.1 ([Sil09, Proposition VII.3.1]) that for each odd $n \in \mathbb{Z}^+$,

$$E(\mathbb{Q})[n] \subseteq E(\mathbb{Q}_2)[n] \hookrightarrow \tilde{E}(\mathbb{F}_2).$$

It is easy to check that $\tilde{E}(\mathbb{F}_2) = \{\tilde{O}\}$. We deduce that

$$E(\mathbb{Q})[\text{tors}] = E(\mathbb{Q})[2^\infty].$$

On the other hand, one can show that $E(\mathbb{Q})[2] = \{O\}$, e.g. by noting that order two points on E have vertical tangent lines, see Exercise 0.7.6. We conclude that $E(\mathbb{Q})[\text{tors}] = \{O\}$.

Example 7.3.2. Consider the elliptic curve

$$E_{/\mathbb{Q}} : y^2 = x^3 + 3.$$

See its LMFDB page: 3888.i2. We compute $\Delta = -3888 = -2^4 \cdot 3^5$, thus $\tilde{E}$ is nonsingular mod p for every prime $p \geq 5$. We check that

$$\#E(\mathbb{F}_5) = 6 \qquad \text{and} \qquad \#E(\mathbb{F}_7) = 13.$$

We claim that $E(\mathbb{Q})[\text{tors}] = \{O\}$. To see this, first observe that for $P \in E(\mathbb{Q})[\text{tors}]$, if $n := |P|$ is coprime to 35, then by Proposition 7.3.1 we have $E(\mathbb{Q})[n] \hookrightarrow \tilde{E}(\mathbb{F}_5)$ and $E(\mathbb{Q})[n] \hookrightarrow \tilde{E}(\mathbb{F}_7)$, which implies that $n \mid \gcd(\#\tilde{E}(\mathbb{F}_5), \#\tilde{E}(\mathbb{F}_7)) = 1$. We deduce that $E(\mathbb{Q})[\text{tors}] = E(\mathbb{Q})[35^\infty]$. On the other hand, given $P \in E(\mathbb{Q})[7^\infty]$, setting $n := |P|$ we have $E(\mathbb{Q})[n] \hookrightarrow \tilde{E}(\mathbb{F}_5)$, and so $n \mid \#\tilde{E}(\mathbb{F}_5) = 6$, forcing $P = O$; thus, $E(\mathbb{Q})[7^\infty] = \{O\}$, i.e., $E(\mathbb{Q})[35^\infty] = E(\mathbb{Q})[5^\infty]$. A similar argument shows that $E(\mathbb{Q})[5^\infty] = \{O\}$.

We conclude that $E(\mathbb{Q})[\text{tors}] = \{O\}$. However, we visibly spot the rational point $(1, 2) \in E(\mathbb{Q})$; we conclude that $(1, 2)$ has infinite order on E, and so $\#E(\mathbb{Q}) = \infty$.

Example 7.3.3. Consider the elliptic curve

$$E_{/\mathbb{Q}} : y^2 = x^3 + x.$$

See its LMFDB page: 64.a4. We have $\Delta = -64 = -2^6$. We find that $\#\tilde{E}(\mathbb{F}_3) = 4$ and $\#\tilde{E}(\mathbb{F}_5) = 4$, and thus deduce that $E(\mathbb{Q})[\text{tors}] = E(\mathbb{Q})[2^\infty]$. We also find that $\#\tilde{E}(\mathbb{F}_7) = 8$, so it is not immediately clear whether the previous techniques will work. (In general, for this elliptic curve we have $4 \mid \#\tilde{E}(\mathbb{F}_p)$ for each odd prime p, see Exercise 5.1.2.)

However, the group structure of the reductions mod p tells us a bit more. For example, we can check that $\tilde{E}(\mathbb{F}_5) \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. Thus, for each $e \geq 1$, we know that $E(\mathbb{Q})[2^e]$ embeds into $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, which forces $E(\mathbb{Q})[2^\infty] = E(\mathbb{Q})[2]$ (group exponent argument). We check that $E[2] = \{O, (0, 0), (i, 0), (-i, 0)\}$ (see Exercise 0.7.6), and thus conclude that $E(\mathbb{Q})[\text{tors}] = \{O, (0, 0)\}$.

Here is a theorem which further describes torsion points on elliptic curves over local fields (and consequently applies to number fields). The proof of this in [Sil09] uses formal groups, so we will not describe it here.

Theorem 7.3.2. [Sil09, Theorem VII.3.4] *Assume that* $\text{char}(K) = 0$ *and* $p := \text{char}(k) > 0$. *Let* $E_{/K}$ *be an elliptic curve given by an* R*-Weierstrass equation. Let* $P \in E(K)$ *be a point with exact order* $n \geq 2$.

a. If n *is not a power of* p, *then* $x(P), y(P) \in R$.
b. If $n = p^e$, *then*

$$\pi^{2r} x(P), \pi^{3r} y(P) \in R \qquad \text{with} \qquad r = \left\lfloor \frac{v(p)}{p^{e-1}(p-1)} \right\rfloor.$$

Application. Suppose that $E_{/\mathbb{Q}}$ is an elliptic curve given by a Weierstrass equation whose coefficients lie in $\mathbb{Z}$, and let $P \in E(\mathbb{Q})$ be a torsion point of order $n \geq 2$. If n is not a prime power, then for all primes $p \in \mathbb{Z}^+$, part a. of this theorem says that $v_p(n) \geq 0$; it follows that P is integral, i.e., $P \in E(\mathbb{Z})$. If $n = p^e$ is some prime power, then letting v_p denote the usual p-adic valuation (so $v_p(p) = 1$), part b. implies that

$$v_p(x(P)) \geq -2\left\lfloor \frac{1}{p^{e-1}(p-1)} \right\rfloor \qquad \text{and} \qquad v_p(y(P)) \geq -3\left\lfloor \frac{1}{p^{e-1}(p-1)} \right\rfloor.$$

These floor values equal 0 unless $p^e = 2$, in which case we only have $v_2(x(P)) \geq -2$ and $v_p(y(P)) \geq -3$, i.e., we have

$$P = \left(\frac{x_0}{2^a}, \frac{y_0}{2^b}\right) \in E(\mathbb{Q})$$

for some $x_0, y_0 \in \mathbb{Z}$ where $0 \leq a \leq 2$ and $0 \leq b \leq 3$. This is best-possible in terms of integrality of torsion points, since the elliptic curve

$$E : y^2 + xy = x^3 + 4x + 1$$

has the 2-torsion point $\left(-\frac{1}{4}, \frac{1}{8}\right) \in E(\mathbb{Q})$ (see its LMFDB page: 65.a2).

This application is summarized in the following corollary.

Corollary 7.3.3. *Let $E_{/\mathbb{Q}}$ be an elliptic curve given by a Weierstrass equation with coefficients in $\mathbb{Z}$. Then for any torsion point $P \in E(\mathbb{Q})$ of order n, if $n \geq 3$ then $P \in E(\mathbb{Z})$. If $n = 2$, then $P = (x, y)$ with $v_2(x) \geq -2$ and $v_2(y) \geq -3$. This is best-possible in terms of integrality.*

Remark 7.3.1. It is worth noting that if $E_{/\mathbb{Q}}$ is in *short* Weierstrass form over $\mathbb{Z}$, then in fact all rational torsion points on E are integral. This is a consequence of a theorem of Nagell and Lutz, see §8.7 of [Sil09].

Here is a useful consequence of our integrality results, applied towards understanding torsion groups of rational elliptic curves (it also has an analog for general number fields). Given an elliptic curve $E_{/\mathbb{Q}}$ with an equation over $\mathbb{Z}$, and a prime $p \in \mathbb{Z}^+$, say that E has **good reduction at** p if the reduced curve for $E_{/\mathbb{Q}_p}$ is nonsingular.

Theorem 7.3.4. *Let $E_{/\mathbb{Q}}$ be an elliptic curve. If $p \geq 3$ is a prime of good reduction for E, then the torsion reduction map*

$$\text{red}\colon E(\mathbb{Q})[\text{tors}] \to \tilde{E}(\mathbb{F}_p)$$

is injective.

Proof. Suppose that E has good reduction at p. Then we know by Proposition 7.3.1 ([Sil09, Proposition VII.3.1]) that $\text{red}\colon E(\mathbb{Q})[p]' \to \tilde{E}(\mathbb{F}_p)$ is injective, where $E(\mathbb{Q})[p]'$ is the subgroup of $E(\mathbb{Q})$ of torsion points whose orders are coprime to p.

It thus suffices to show that $\text{red}\colon E(\mathbb{Q})[p^\infty] \to \tilde{E}(\mathbb{F}_p)$ is injective. If $P \in \ker \text{red} \cap E(\mathbb{Q})[p^\infty]$ is nontrivial, then writing $P = (x, y) = \left(\frac{a}{b}, \frac{c}{d}\right)$ where $a, b, c, d \in \mathbb{Z}$, we have $[\tilde{x}, \tilde{y} : 1] = [0 : 1 : 0]$, i.e.,

$$[\tilde{ad} : \tilde{bc} : \tilde{bd}] = [0 : 1 : 0].$$

It follows that $p \mid ad, p \mid bd$ and $bc \equiv 1 \pmod{p}$, whence we have $p \mid d$. However, by the Application following Theorem 7.3.2, this is impossible unless $|P| = p = 2$. We conclude that if E has good reduction at $p > 2$, then $\ker(\text{red}\colon E(\mathbb{Q})[p^\infty] \to \tilde{E}(\mathbb{F}_p)) = \{O\}$. (This also shows that if E has good reduction at $p = 2$, then $\ker(\text{red}\colon E(\mathbb{Q})[2^\infty] \to \tilde{E}(\mathbb{F}_2)) \subseteq E[2]$.) □

Exercise 7.3.1. [Sil09, Exercise 7.3] Describe all Weierstrass equations

$$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$

with $a_i \in \mathbb{Z}$ and $\Delta \neq 0$ such that $E(\mathbb{Q})$ contains a torsion point P with $x(P) \notin \mathbb{Z}$. (*Hint:* see the Application in §7.3.)

Exercise 7.3.2.

a. Prove that the elliptic curve

$$E : y^2 + y = x^3 - x$$

has trivial torsion subgroup, but positive rank over $\mathbb{Q}$. (This is the first elliptic curve of minimal *conductor*[12] and positive rank. See its LMFDB page: 37.a1. See also [Sil09, Exercise 9.13].)

b. Prove that the elliptic curve

$$E : y^2 - y = x^3 - x^2$$

has $E(\mathbb{Q})[\text{tors}] \cong \mathbb{Z}/5\mathbb{Z}$. (This is "the first elliptic curve in nature": it has minimal conductor and is a model for the *modular curve* $X_1(11)$. See its LMFDB page: 11.a3.)

c. Prove that the elliptic curve

$$E : y^2 + xy + y = x^3 - x^2 - 5x + 5$$

has $E(\mathbb{Q})[\text{tors}] \cong \mathbb{Z}/3\mathbb{Z}$. (This curve corresponds to a *sporadic* point of degree 3 on the modular curve $X_1(21)$. Up to $\overline{\mathbb{Q}}$-isomorphism, it is the only elliptic curve which has the torsion group $\mathbb{Z}/21\mathbb{Z}$ over a cubic number field, namely $\mathbb{Q}(\zeta_9)^+$. See its LMFDB page: 162.c3.)

7.4. **The action of inertia.** In this section, we will connect ramification of elliptic curve torsion groups to the Galois action of inertia.

Let K^{nr} denote the maximal unramified extension of K: this is the compositum of all unramified extensions of K. Recall by Exercise A.0.5 that an unramified extension L/K is Galois, with Galois group isomorphic to the Galois group of its residue field ℓ/k (essentially Hensel's Lemma). It follows that

$$\text{Gal}(K^{\text{nr}}/K) \cong G_k;$$

in fact, this isomorphism is given by reduction of automorphisms, just like in the case of inertia groups over number fields. More precisely, for a finite unramified extension L/K with residue field $\ell := S/(\Pi)$ (where S is the discrete valuation ring for L and Π

[12]The **conductor** of an elliptic curve $E_{/\mathbb{Q}}$ is a specific integer divisible precisely by the primes of *bad reduction* for E, i.e., the primes p for which $\tilde{E}_{/\mathbb{F}_p}$ is singular.

is its uniformizer), for $\sigma \in \mathrm{Gal}(L/K)$ we have $\tilde{\sigma}\colon \ell \xrightarrow{\sim} \ell$ via $\tilde{\sigma}(\alpha + (\Pi)) := \sigma(\alpha) + (\Pi)$. Thus, we have a short exact sequence

$$1 \to \mathrm{Gal}(\overline{K}/K^{\mathrm{nr}}) \to G_K \xrightarrow{\mathrm{red}} G_k \to 1.$$

The Galois group $I_v := \mathrm{Gal}(\overline{K}/K^{\mathrm{nr}})$ is called the *inertia group* of K. Thus, the SES above becomes

$$1 \to I_v \to G_K \xrightarrow{\mathrm{red}} G_k \to 1. \tag{12}$$

To reiterate, the inertia group of K is the subgroup of G_K of automorphisms which act trivially on $\overline{k}$.

Remark 7.4.1. Observe that the short exact sequence above mimics the usual short exact sequence of inertia and decomposition groups for number fields: given a Galois extension M/F of number fields, for primes $\mathfrak{p} \subseteq F$ and $\mathfrak{P} \subseteq M$ where $\mathfrak{P} \mid \mathfrak{p}$, one has

$$1 \to I_{\mathfrak{P}|\mathfrak{p}} \to D_{\mathfrak{P}|\mathfrak{p}} \xrightarrow{\mathrm{red}} \mathrm{Gal}((\mathcal{O}_M/\mathfrak{P})/\mathcal{O}_F/\mathfrak{p}) \to 1.$$

Here, the *decomposition group* of $\mathfrak{P} \mid \mathfrak{p}$ is

$$D_{\mathfrak{P}|\mathfrak{p}} := \{\sigma \in \mathrm{Gal}(M/F) : \sigma(\mathfrak{P}) = \mathfrak{P}\}$$

and the *inertia group* of $\mathfrak{P} \mid \mathfrak{p}$ is

$$\begin{aligned} I_{\mathfrak{P}|\mathfrak{p}} :&= \{\sigma \in \mathrm{Gal}(M/F) : \tilde{\sigma} = 1_{(\mathcal{O}_M/\mathfrak{P})}\} \\ &= \{\sigma \in \mathrm{Gal}(M/F) : \forall \alpha \in \mathcal{O}_M,\ \sigma(\alpha) \equiv \alpha \pmod{\mathfrak{P}}\}. \end{aligned}$$

In fact, one can show that $D_{\mathfrak{P}|\mathfrak{p}} \cong \mathrm{Gal}(M_{\mathfrak{P}}/F_{\mathfrak{p}})$, and the local SES (12) is a generalization of this one.

Definition 7.4.1. Let G_K act on a set X. Say that X is **unramified (at v)** if the action of I_v on X is trivial.

The following proposition connects good reduction to ramification of elliptic curve torsion groups; it is part of the *Néron-Ogg-Shafarevich criterion,* which we will prove at then end of this chapter.

Proposition 7.4.1. [Sil09, Proposition VII.4.1] *Let $E_{/K}$ be an elliptic curve with good reduction, i.e., such that $\tilde{E}_{/k}$ is nonsingular.*

a. *Let $n \geq 1$ be an integer coprime to $p := \mathrm{char}(k)$, i.e., $v(n) = 0$. Then $E[n]$ is unramified at v.*
b. *Let $\ell \neq \mathrm{char}(k)$ be a prime. Then $T_\ell(E)$ is unramified at v.*

Proof. Part b. quickly follows from part a., since $T_\ell(E)$ is the inverse limit of the ℓ-primary torsion groups $E[\ell^k]$ for $k \geq 1$. To prove part a., let us set $L := K(E[n])$ to be the n-division field of E over K. Let w be the unique extension of v to L: this is given by $w(x) := \frac{1}{n} \cdot v(N_{L/K}(x))$ (see the appendix for a citation of this fact). say Π is a uniformizer of L at w, let S be the associated DVR of Π, and let $\ell := S/(\Pi)$ be its residue field. We will use that $E(L)[n] = E[n]$ to show $E[n]$ is unramified at v.

Since E has good reduction at v, any minimal R-Weierstrass equation of E satisfies $v(\Delta) = 0$. It follows that $w(\Delta) = 0$ (since $w|_K = v$), and thus such an R-equation is

also S-minimal, and $E_{/L}$ has good reduction at w. Proposition 7.3.1 ([Sil09, Proposition VII.3.1]) then implies that

$$\text{red}\colon E(L)[n] = E[n] \hookrightarrow \tilde{E}(\ell) \tag{13}$$

is injective.

We want to show that I_v acts trivially on $E[n]$, i.e., $\forall \sigma \in I_v$ and $\forall P \in E[n]$, one has $P^\sigma = P$. By definition of the inertia group (see Equation (12)),

$$I_v = \{\sigma \in G_K : \forall \text{ subextensions } k \subseteq \ell \subseteq \overline{k},\ \tilde{\sigma} = 1_\ell\}.$$

In particular, $\tilde{\sigma}$ acts trivially on $\tilde{E}(\ell)$, which means

$$(\tilde{P})^{\tilde{\sigma}} = \tilde{P};$$

however, by definition $(\tilde{P})^{\tilde{\sigma}} := \widetilde{P^\sigma}$, i.e., the reduction of sigma applied to the reduction of P is the reduction of [σ applied to P]. Thus we have $\widetilde{P^\sigma} = \tilde{P}$. Since reduction of points is a homomorphism (see Proposition 7.2.3 [Sil09, Proposition VII.2.1]), this means that

$$\widetilde{P^\sigma - P} = \tilde{O}.$$

However, since $P \in E[n]$, it follows that $P^\sigma - P \in E[n]$, and so $P^\sigma - P \in \ker(\text{red}\colon E[n] \to \tilde{E}(k))$, which is trivial by (13). Thus $P^\sigma = P$, whence we conclude that $E[n]$ is unramified at v. □

The Néron-Ogg-Shafarevich criterion says that the converse of this proposition is also true. We will prove this in Section 7.

Remark 7.4.2. Let us make more clear the connection between Proposition 7.4.1 and ramification in division fields and Galois representations. Given an elliptic curve $E_{/K}$, for each $n \in \mathbb{Z}^+$ we have the mod-n Galois representation

$$\rho_{E,n}\colon G_K \to \mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z}).$$

By definition, $E[n]$ is unramified at v if and only if $\rho_{E,n}(I_v) = 1$. Furthermore,the kernel of this representation is $\mathrm{Gal}(\overline{K}/K(E[n])$, where $K(E[n])$ is the **n-division field of E,** i.e.,

$$K(E[n]) = \{x(P), y(P) : P \in E[n]\}.$$

Thus $K(E[n])/K$ is Galois, and modding out by the kernel gives a faithful representation

$$\rho_{E,n}\colon \mathrm{Gal}(K(E[n])/K) \hookrightarrow \mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z}).$$

Therefore, E is unramified at v if and only if the inertia group of $K(E[n])/K$ is trivial; here, the inertia group is like the usual finite one from algebraic number theory, just for a local field instead.

7.5. **Good and bad reduction.** In this section, we describe the various reduction types of an elliptic curve, culminating in the *semistable reduction theorem.* As noted previously, for an elliptic curve $E_{/K}$, the reduction $\tilde{E}$ being nonsingular is independent of choice of R-minimal Weierstrass equation.

Definition 7.5.1. Let $E_{/K}$ be an elliptic curve given by an R-minimal Weierstrass equation; let $\tilde{E}$ denote the curve given by the reduction of this equation.

a. E has **good** (or **stable**) reduction if $\tilde{E}$ is nonsingular.
b. E has **multiplicative** (or **semistable**) reduction if $\tilde{E}$ is singular with a node.
c. E has **additive** (or **unstable**) reduction if $\tilde{E}$ is singular with a cusp.

These three cases are called the **reduction types** of E. In the latter two cases, we say that E has **bad reduction.** If E has multiplicative reduction, we say the reduction is *split* if the slopes of the two distinct tangent lines at the node of $\tilde{E}$ are in k; otherwise, we say it is *nonsplit.*

The following proposition summarizes some of our previous results on the reduction type. It also explains why "additive" and "multiplicative" reduction are named so.

Proposition 7.5.1. [Sil09, Proposition VII.5.1] *Let $E_{/K}$ be an elliptic curve given in R-minimal Weierstrass form*

$$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6.$$

Let Δ be the discriminant of this equation, and c_4 its other invariant.

a. *E has good reduction if and only if $v(\Delta) = 0$, i.e., $\Delta \in R^\times$. In this case, $\tilde{E}_{/k}$ is an elliptic curve.*
b. *E has multiplicative reduction if and only if $v(\Delta) > 0$ and $v(c_4) = 0$, i.e., $\Delta \in M$ and $c_4 \in R^\times$. In this case, $\tilde{E}_{\text{ns}}$ is the* multiplicative *group,*

$$\tilde{E}_{\text{ns}}(\overline{k}) \cong \overline{k}^\times.$$

c. *E has additive reduction if and only if $v(\Delta) > 0$ and $v(c_4) > 0$, i.e., $\Delta, c_4 \in M$. In this case, $\tilde{E}_{\text{ns}}$ is the* additive *group,*

$$\tilde{E}_{\text{ns}}(\overline{k}) \cong (\overline{k}, +).$$

Example 7.5.1. Over $\mathbb{Q}_p$, consider the elliptic curves

$$E_1 : y^2 = x^3 + px^2 + 1, \qquad E_2 : y^2 = x^3 + x^2 + p \qquad \text{and} \qquad E_3 : y^2 = x^3 + p.$$

Assuming that $p \geq 5$, we have that E_1 has good reduction since $\Delta_{E_1} = -4p^3 - 27$; similarly checked, E_2 has multiplicative reduction ($\Delta_{E_2} = -16p(4 + 27p)$ and $c_4 = 16$), and E_3 has additive reduction ($\Delta_{E_3} = -2^4 \cdot 3^3 \cdot p^2$ and $c_4 = 0$). However, over the finite extension $\mathbb{Q}_p(p^{1/6})$, we find that E_3 attains good reduction, with a new minimal equation given by the substitution

$$x \mapsto p^{1/3} \cdot x', y \mapsto p^{1/2} \cdot y' :$$

this new equation over $\mathbb{Q}_p$ is explicitly

$$py'^2 = p(x')^3 + p,$$

i.e.,

$$y'^2 = (x')^3 + 1.$$

On the other hand, E_2 will always have multiplicative reduction over algebraic extensions of $\mathbb{Q}_p$ (we will see why in a moment).

The example above gives a moral explanation for the terms stable, semistable and unstable: additive reduction can turn into good or multiplicative reduction, whereas good and multiplicative reduction do not change. This also prompts the following definition.

Definition 7.5.2. Say that an elliptic curve $E_{/K}$ has **potential good reduction** if there exists a finite extension L/K such that $E_{/L}$ has good reduction over L.

Remark 7.5.1. A CM elliptic curve $E_{/K}$ always has potential good reduction, see [Sil09, Exercise 7.10].

The next proposition shows how reduction type can change upon base extension.

Proposition 7.5.2 (Semistable Reduction Theorem)**.** [Sil09, Proposition VII.5.4] *Let $E_{/K}$ be an elliptic curve.*

a. *If L/K is an unramified extension, then the reduction type of E over L (good, multiplicative or additive) is the same as the reduction type of E over K.*
b. *If L/K is a finite extension, then if E has good or multiplicative reduction over K, then the reduction type stays the same over L.*
c. *There exists a finite extension L/K such that $E_{/L}$ has good or (split) multiplicative reduction over L.*

Proposition 7.5.3. [Sil09, Proposition VII.5.5] *Let $E_{/K}$ be an elliptic curve. Then E has potential good reduction if and only if its j-invariant is integral, i.e., $j(E) \in R$.*

Exercise 7.5.1. [Sil09, Exercise 7.3] Show that the following elliptic curves have good reduction over a field of the indicated form by writing down a minimal equation for E over that field.

a. $E : y^2 = x^3 + x$, $\quad \mathbb{Q}_2(\eta, i), \eta^8 = 2, i^2 = -1.$
b. $E : y^2 + y = x^3$, $\quad \mathbb{Q}_3(\pi, \eta), \pi^2 = \sqrt{-3}, \eta^3 = 2.$
c. $E : y^2 = x^3 + x^2 - 3x - 2$, $\quad \mathbb{Q}_5(\pi), \pi^4 = 5.$

Exercise 7.5.2. Let F be a number field and $E_{/F}$ an elliptic curve. For a nonzero prime ideal $\mathfrak{P} \subseteq \mathcal{O}_F$, say that E has *good reduction at* $\mathfrak{P}$ if $E_{/F_\mathfrak{P}}$ has good reduction, where $F_\mathfrak{P}$ is the completion of F at the discrete valuation $v_\mathfrak{P}$ associated to $\mathfrak{P}$. We also use $\mathcal{O}_{F,\mathfrak{P}}$ to denote the discrete valuation ring in $F_\mathfrak{P}$ associated to $v_\mathfrak{P}$.

a. Assume that E is given by a Weierstrass equation over $\mathcal{O}_F$ that is minimal over $F_\mathfrak{P}$. Prove that E has good reduction at $\mathfrak{P}$ if and only if $\mathfrak{P} \nmid \Delta_{E,F}$.
b. Prove that no elliptic curve $E_{/\mathbb{Q}}$ has good reduction at every prime $p \in \mathbb{Z}^+$. (*Hint:* see [Sil09, Exercise 8.15].)

Note that a Weierstrass equation of an elliptic curve $E_{/F}$ with coefficients in $\mathcal{O}_F$ need not be a minimal equation over each completion $F_\mathfrak{P}$; in fact, such a "global minimal equation" for E is not guaranteed to exist unless F has class number 1 – see §8.8 of [Sil09]. Thus, a global minimal equation always exists when $F = \mathbb{Q}$.

7.6. **The group E/E_0.** Recall that for an elliptic curve $E_{/K}$, we have a short exact sequence

$$0 \to E_1(K) \to E_0(K) \to \tilde{E}_{\mathrm{ns}}(k) \to 0.$$

We know that $E_1(K) \cong \widehat{E}(M)$ is a formal group, which lets us describe its torsion points; we also know the structure of $\tilde{E}_{\mathrm{ns}}(k)$. Thus, we can describe $E_0(K)$; to better understand $E(K)$, we are left to then study $E(K)/E_0(K)$.

As it turns out, the index $[E(K) : E_0(K)]$ is finite, which is what we need to know towards proving the Néron-Ogg-Shafarevich criterion. In fact, one can say more about this quotient.

Theorem 7.6.1 (Kodaira, Néron)**.** [Sil09, Theorem VII.6.1] *Let $E_{/K}$ be an elliptic curve. If E has split multiplicative reduction over K, then $E(K)/E_0(K)$ is cyclic of order $v(\Delta) = -v(j)$. In all other cases, the quotient $E(K)/E_0(K)$ is finite of order at most 4.*

The usual proof for this theorem involves Néron models and their classification. However, if k is a finite field, then finiteness of $[E(K) : E_0(K)]$ can be proven using topological methods; see [Sil09, Exercise 7.6].

There is an interesting application of this theorem which uses formal groups to further describe the Mordell-Weil group $E(K)$.

Proposition 7.6.2. [Sil09, Proposition VII.6.3] *Let $K = F_{\mathfrak{P}}$ be a finite extension of $\mathbb{Q}_p$. Then $E(K)$ contains a finite index subgroup that is isomorphic to $(\mathcal{O}_{F,\mathfrak{P}}, +)$, where $\mathcal{O}_{F,\mathfrak{P}}$ denotes the discrete valuation ring of $F_{\mathfrak{P}}$ associated to $v_{\mathfrak{p}}$.*

7.7. **The criterion of Néron-Ogg-Shafarevich.** We have previously shown that if $E_{/K}$ has good reduction, then for all integers $n \in \mathbb{Z}^+$ coprime to $p := \mathrm{char}(k)$, one has that $E[n]$ is unramified. The converse is also true, and is part of the **Néron-Ogg-Shafarevich criterion.** This can be considered the main result of this chapter.

Theorem 7.7.1 (Néron-Ogg-Shafarevich criterion)**.** *Let $E_{/K}$ be an elliptic curve. Then the following are equivalent.*

a. E has good reduction.
b. $E[n]$ is unramified at v for all integers $n \in \mathbb{Z}^+$ coprime to p, i.e., $v(n) = 0$.
c. $T_\ell(E)$ is unramified at v for all primes $\ell \neq p$.
d. $E[n]$ is unramified at v for infinitely many integers $n \in \mathbb{Z}^+$ coprime to p.

Proof. a. $\Rightarrow$ b. was Proposition 7.4.1 ([Sil09, Proposition VII.4.1]). b. $\Rightarrow$ c. $\Rightarrow$ d. is clear. Thus, it suffices to show that E has good reduction if infinitely many $E[n]$ are unramified at v.

This proof is slightly different than that in [Sil09], since that proof is incorrect. There is a correction in the errata which we will follow, see `https://www.math.brown.edu/~jhs/AEC/AECErrata.pdf`. Let $\widehat{K^{\mathrm{nr}}}$ denote the completion of the maximal unramified extension of K. By the *proof* of the semistable reduction theorem (this is where the correction is made), since $\widehat{K^{\mathrm{nr}}}$ has the same value group as K^{nr} (i.e., $w(\widehat{K^{\mathrm{nr}}}) = w(K^{\mathrm{nr}})$ where w extends v to $\widehat{K^{\mathrm{nr}}}$)), we can deduce that the reduction type of E over $\widehat{K^{\mathrm{nr}}}$ is

the same as that of E over K^{nr}, which is the same as that of E over K (this latter part is also by the semistable reduction theorem!).

Since we are assuming part d., we can fix an integer $n \in \mathbb{Z}^+$ such that the following holds:

i. $p \nmid n$;
ii. $n > [E(\widehat{K^{\mathrm{nr}}}) : E_0(\widehat{K^{\mathrm{nr}}})]$;
iii. $E[n]$ is unramified at v.

(Note that the index in ii. is finite since $\widehat{K^{\mathrm{nr}}}$ is a complete local field, so the results of the previous section apply to it.)

Let us consider two short exact sequences:

$$0 \to E_0(\widehat{K^{\mathrm{nr}}}) \to E(\widehat{K^{\mathrm{nr}}}) \to E(\widehat{K^{\mathrm{nr}}})/E_0(\widehat{K^{\mathrm{nr}}}) \to 0$$

and

$$0 \to E_1(\widehat{K^{\mathrm{nr}}}) \to E_0(\widehat{K^{\mathrm{nr}}}) \xrightarrow{\mathrm{red}} \tilde{E}_{\mathrm{ns}}(\overline{k}) \to 0$$

(note that the residue field of both $\widehat{K^{\mathrm{nr}}}$ and K^{nr} is $\overline{k}$). By assumption, $E[n]$ is unramified at v, and so

$$E[n] \subseteq E(K^{\mathrm{nr}}) \subseteq E(\widehat{K^{\mathrm{nr}}}).$$

In particular, $E(\widehat{K^{\mathrm{nr}}})$ contains a subgroup isomorphic to $(\mathbb{Z}/n\mathbb{Z})^2$. However, since $n > [E(\widehat{K^{\mathrm{nr}}}) : E_0(\widehat{K^{\mathrm{nr}}})]$, from the first SES this forces the left term $E_0(\widehat{K^{\mathrm{nr}}})$ to contain $\mathbb{F}_\ell^2$ for some prime $\ell \mid n$.[13]

In the second SES, we know that the formal group $E_1(\widehat{K^{\mathrm{nr}}})$ has no nontrivial ℓ-torsion by Proposition 7.3.1 ([Sil09, Proposition VII.3.1]). Therefore, since $E_0(\widehat{K^{\mathrm{nr}}})$ contains $\mathbb{F}_\ell^2$, this forces $\tilde{E}_{\mathrm{ns}}(\overline{k})$ to also contain $\mathbb{F}_\ell^2$. However, if E has bad reduction, then by Proposition 7.5.1 ([Sil09, Proposition VII.5.1]) we know that $\tilde{E}_{\mathrm{ns}}(\overline{k})$ is either $\overline{k}^\times$ or $(\overline{k}, +)$, neither of which contains $\mathbb{F}_\ell^2$ (since $\overline{k}^\times[\ell] = \mu_\ell$, which is cyclic of order ℓ, and $(\overline{k}, +)[\ell] = 0$, since $\ell \neq p$). We conclude that E has good reduction over $\widehat{K^{\mathrm{nr}}}$, which concludes our proof by our initial comments on $\widehat{K^{\mathrm{nr}}}$. □

This criterion has a number of interesting applications, the first of which concerns rationally isogenous elliptic curves.

Corollary 7.7.2. [Sil09, Corollary VII.7.2] *Let $E_{/K}$ and $E'_{/K}$ be K-rationally isogenous elliptic curves. Then E has good reduction if and only if E' has good reduction.*

Proof. Let $\phi\colon E \to E'$ be a K-rational isogeny. For any integer $n \in \mathbb{Z}^+$ coprime to both $p := \mathrm{char}(k)$ and $\deg(\phi)$, we have an isomorphism of G_K-modules,

$$\phi\colon E[n] \xrightarrow{\sim} E'[n].$$

[13]To see this claim, it might help if we do it in more generality. Suppose that $0 \to A \to B \to B/A \to 0$ is a SES of abelian groups such that B has a subgroup H that is isomorphic to $(\mathbb{Z}/n\mathbb{Z})^2$. Let us write $H \cap A \cong \mathbb{Z}/m_1\mathbb{Z} \times \mathbb{Z}/m_2\mathbb{Z}$ for some $m_1 \mid m_2 \mid n$. If $m_1 \neq 1$, then taking any prime $\ell \mid m_1$, it follows that $\mathbb{F}_\ell^2 \subseteq H \cap A$, and we are done. Suppose to the contrary this is not the case: thus, we can write $H \cap A \cong \mathbb{Z}/m\mathbb{Z}$ for some $m \mid n$. It follows that $[H : H \cap A] = n \cdot \frac{n}{m}$; thus, $[H : H \cap A] \geq n > [B : A]$. However, for a subgroup $K \subseteq B$, we always have $[K : K \cap A] \leq [B : A]$ (check it directly with coset representatives). We deduce that $n \leq [H : H \cap A] \leq [B : A] < n$, which is impossible.

This implies that $E[n]$ is unramified if and only if $E'[n]$ is unramified (compare mod-n Galois representations). Since there are infinitely many integers n coprime to both p and $\deg(\phi)$, we conclude by the Néron-Ogg-Shafarevich criterion that E has good reduction if and only if E' has good reduction. □

Corollary 7.7.3. *Let $E_{/\mathbb{Q}}$ and $E'_{/\mathbb{Q}}$ be $\mathbb{Q}$-rationally isogenous elliptic curves. Then for any prime $p \in \mathbb{Z}^+$, one has that E has good reduction at p if and only if E' has good reduction at p.*

The above corollary technically uses the fact that a *global minimal model* exists for elliptic curves over $\mathbb{Q}$. In general, such a model exists for elliptic curves over number fields of class number one – see §8.8 of [Sil09].

Here is one more corollary to finish this chapter.

Corollary 7.7.4. [Sil09, Corollary VII.7.3] *Let $E_{/K}$ be an elliptic curve. Then E has potential good reduction if and only if for some (all) prime(s) $\ell \neq p := \mathrm{char}(k)$, the inertia group I_v acts on $T_\ell(E)$ through a finite quotient, i.e., the kernel of its ℓ-adic Galois representation intersects I_v in a finite index subgroup of I_v, i.e., $[K^{\mathrm{nr}}(E[\ell^\infty]) : K^{\mathrm{nr}}] < \infty$.*

Exercise 7.7.1. [Sil09, Exercise 7.9] Let $E_{/K}$ be an elliptic curve with potential good reduction. Let $n \in \mathbb{Z}^+$ be an integer coprime to $p := \mathrm{char}(k)$, and let $K(E[n])$ be the n-division field of E, obtained by adjoining to K the coordinates of points in $E[n]$.

a. Prove that the inertia group of $K(E[n])/K$ is independent of n. (*Hint:* for each prime $\ell \neq p$, let $\ell' := \ell$ if $\ell \geq 3$ and let $\ell' := 4$ if $\ell = 2$. Show that $\rho_{E,\ell^\infty} : I_v \to \mathrm{GL}_2(\mathbb{Z}_\ell)$ has trivial intersection with the kernel of the map
$$\mathrm{Aut}(T_\ell(E)) \to \mathrm{Aut}(T_\ell(E)/\ell' T_\ell(E)) \cong \mathrm{GL}_2(\mathbb{Z}/\ell'\mathbb{Z}).$$
Characterize the inertia group of $K(E[n])/K$ in terms of the kernels of the various ρ_{E,ℓ^∞}.)
b. Prove that $K(E[n])/K$ is unramified if and only if E has good reduction at v.
c. If $p \geq 5$, prove that $K(E[n])/K$ is *tamely ramified,* i.e., the ramification index is coprime to p.

8. Elliptic Curves Over Global Fields

The goal of this chapter will be to prove the *Mordell-Weil Theorem* over number fields; describing the group $E(F)$ can be considered the penultimate goal of these notes.

Theorem (Mordell-Weil)**.** *Let F be a number field and $E_{/F}$ an elliptic curve. Then $E(F)$ is finitely generated.*

The proof of this theorem breaks into two parts: the "weak Mordell-Weil theorem" (§8.1) and "infinite descent" using height functions (§8.3, 8.5, 8.6). Note that once we prove $E(F)$ is finitely generated, we get a decomposition

$$E(F) \cong \mathbb{Z}^r \times E(F)[\text{tors}].$$

For a given elliptic curve, we can use the local techniques we developed in Chapter 7 to compute $E(F)[\text{tors}]$; however, computing the *rank part* $\mathbb{Z}^r$ of $E(F)$ is generally more difficult. In Chapter 10, we will discuss some techniques to do this.

This chapter uses the following notation:

- F is a number field.
- $\mathcal{O}_F$ is the ring of integers of F.
- Σ_F is the set of inequivalent absolute values on F: this includes both the Archimedean and non-Archimedean absolute values.
  - Recall that an absolute value $|\cdot| \in \Sigma_F$ induces a valuation $v(x) := -\ln|x|$, and vice versa. Given this correspondence, we will use both terms interchangeably; we will also call them the *places* of F.
  - *Archimedean:* given by an embedding of F into $\mathbb{C}$.
  - *Non-Archimedean:* given by a nonzero prime ideal $\mathfrak{P} \subseteq \mathcal{O}_F$. These are discrete valuations.
- Σ_F^{Arch} is the set of (inequivalent) Archimedean places of F.
- Σ_F^{NA} is the set of (inequivalent) non-Archimedean places of F.
- Any discrete valuation $v \in \Sigma_F^{\text{NA}}$ we consider is normalized, i.e., surjects onto $\mathbb{Z}$. (This is a given with our definition of discrete valuation.)
- One can write $\mathcal{O}_F = \{x \in F : \forall v \in \Sigma_F^{\text{NA}}, v(x) \geq 0\}$.
- One has the unit group $\mathcal{O}_F^\times = \{x \in F : \forall v \in \Sigma_F^{\text{NA}}, v(x) = 0\}$.
- F_v is the completion of F at $v \in \Sigma_F$. When $v = v_\mathfrak{P}$ is discrete, we will often write $F_\mathfrak{P}$ instead.
- For $v := v_\mathfrak{P} \in \Sigma_F^{\text{NA}}$, we let $\mathcal{O}_{F,v} := \mathcal{O}_{F,\mathfrak{P}}$ denote the discrete valuation ring of $F_\mathfrak{P}$.
- For $v := v_\mathfrak{P} \in \Sigma_F^{\text{NA}}$, we let $M_v := M_\mathfrak{P}$ denote the maximal ideal of $F_\mathfrak{P}$.
- For $v := v_\mathfrak{P} \in \Sigma_F^{\text{NA}}$, we let $k_v := k_\mathfrak{P}$ denote the residue field of $F_\mathfrak{P}$.

8.1. The weak Mordell-Weil theorem.

The goal of this section is to prove the following.

Theorem 8.1.1 (Weak Mordell-Weil)**.** *Let $E_{/F}$ be an elliptic curve and $n \geq 2$ an integer. Then*

$$E(F)/nE(F)$$

is a finite group.

To prove this, we will first prove the following lemma, which lets us change the base field F.

Lemma 8.1.2. [Sil09, Lemma VIII.1.1.1] *Let L/F be a finite Galois extension. If $E(L)/nE(L)$ is finite, then so is $E(F)/nE(F)$.*

Proof. From $E(F) \subseteq E(L)$, we have a natural map

$$E(F)/nE(F) \to E(L)/nE(L).$$

Let Φ be the kernel of this map; since the codomain is finite, we have that Φ is finite if and only if $E(F)/nE(F)$ is finite.

We will show that Φ is finite by embedding it into a finite set of maps. Observe that

$$\Phi = \frac{E(F) \cap nE(L)}{nE(F)}.$$

Let $P \in \Phi$; thus, there exists $Q_P \in E(L)$ with $nQ_P = P$. This gives a map

$$\lambda_P \colon \mathrm{Gal}(L/F) \to E[n], \qquad \lambda_P(\sigma) := Q_P^\sigma - Q_P.$$

(This is an example of a *1-cocycle* from a certain cohomology group; more on this later.) Note that indeed $Q_P^\sigma - Q_p \in E[n]$, since

$$n(Q_P^\sigma - Q_P) = (nQ_P)^\sigma - nQ_P = P^\sigma - P = 0$$

(we used above that $P \in E(F) \Rightarrow P^\sigma = P$).

We thus have a map

$$\Phi \to \mathrm{Map}(\mathrm{Gal}(L/F), E[n]), \qquad P \mapsto \lambda_P.$$

We claim this map is injective: if $\lambda_P = \lambda_{P'}$, then for all $\sigma \in \mathrm{Gal}(L/F)$ one has

$$Q_P^\sigma - Q_P = Q_{P'}^\sigma - Q_{P'},$$

i.e.,

$$(Q_P - Q_{P'})^\sigma = (Q_P - Q_{P'}).$$

This implies that $Q_P - Q_{P'} \in E(F)$, and thus $n(Q_P - Q_{P'}) = P - P' \in nE(F)$, i.e., $P \equiv P' \pmod{nE(F)}$. We conclude that Φ, and thus $E(F)/nE(F)$, is finite. □

The lemma above lets us assume that $E[n] \subseteq E(F)$, which we will do for the rest of this section. Next, we will connect finiteness of $E(F)/nE(F)$ to a certain extension of F having finite degree. This extension will arise once we consider the *elliptic Kummer pairing,* which is similar to what we considered above.

Definition 8.1.1. The **(elliptic) (n-)Kummer pairing**

$$\kappa \colon E(F) \times G_F \to E[n]$$

is defined as follows. For a point $P \in E(F)$, choose any $Q \in E$ such that $nQ = P$. Then

$$\kappa(P, \sigma) := Q^\sigma - Q.$$

Here are some properties of this Kummer pairing.

Proposition 8.1.3. [Sil09, Proposition VIII.1.2]

a. *The Kummer pairing is well-defined, i.e., $\kappa(P,\sigma)$ is in $E[n]$ and is independent of choice of Q with $nQ = P$.*
b. *The Kummer pairing is bilinear.*
c. *The left kernel of the Kummer pairing is $nE(F)$.*
d. *The right kernel of the Kummer pairing is $G_L := \mathrm{Gal}(\overline{\mathbb{Q}}/L)$, where*

$$L := F([n]^{-1}(E(F)))$$

is the compositum of the fields $F(Q)$ for all $Q \in E$ where $nQ \in E(F)$.

Thus, the Kummer pairing induces a perfect bilinear pairing

$$E(F)/nE(F) \times \mathrm{Gal}(L/F) \to E[n]$$

where $L := F([n]^{-1}(E(F)))$.

Remark 8.1.1. In the above, under the assumption that $E[n] \subseteq E(F)$, we "adjoined all n'th roots of points in $E(F)$ to F" to construct L. This is analogous to the classic Kummer extension: under the assumption that $\mu_n \subseteq F$, one adjoins all n'th roots of elements from $F^\times$ to F to construct a field extension L/F, and gets a perfect bilinear pairing

$$F^\times/(F^\times)^n \times \mathrm{Gal}(L/F) \to \mu_n, \qquad (a,\sigma) \mapsto \frac{\sigma(a^{1/n})}{a^{1/n}}.$$

(Our elliptic Kummer pairing was $\kappa\colon (P,\sigma) \mapsto Q^\sigma - Q$, where $nQ = P$.)

Proof. Most of this proposition can be proved using basic Group cohomology – we will touch on this in the next section. Let us give a more direct proof here.

For part a., fixing $nQ = P$, we observe that

$$\begin{aligned} n \cdot \kappa(P,\sigma) :&= n \cdot (Q^\sigma - Q) \\ &= nQ^\sigma - nQ \\ &= (nQ)^\sigma - nQ \\ &= P^\sigma - P \\ &= O \qquad\qquad (\text{since } P \in E(F) \Rightarrow P^\sigma = P). \end{aligned}$$

Thus, κ takes values in $E[n]$. Additionally, κ is well-defined: if $nQ = nQ' = P$, then $\forall \sigma \in G_F$, one has $Q^\sigma - Q = Q'^\sigma - Q'$, i.e., $(Q-Q')^\sigma = Q - Q'$. Since $E[n] \subseteq E(F)$, it is enough to show that $Q - Q' \in E[n]$; however, this follows from $n\cdot(Q-Q') = P - P = O$. This proves part a.

For part b., we want to show that for all $P, P' \in E[n]$ one has

$$\kappa(P+P',\sigma) = \kappa(P,\sigma) + \kappa(P',\sigma),$$

and for all $\sigma, \tau \in G_F$ one has

$$\kappa(P,\sigma\tau) = \kappa(P,\sigma) + \kappa(P,\tau).$$

The first linearity condition is clear, since if $nQ = P$ and $nQ' = P'$, then $n(Q+Q') = P + P'$, and we also have $(Q+Q')^\sigma = Q^\sigma + Q'^\sigma$. For the second condition, we check

that if $nQ = P$, then

$$\begin{aligned}\kappa(P, \sigma\tau) :&= Q^{\sigma\tau} - Q \\ &= (Q^{\sigma} - Q)^{\tau} + (Q^{\tau} - Q) \\ &= \kappa(P, \sigma)^{\tau} + \kappa(P, \tau) \\ &= \kappa(P, \sigma) + \kappa(P, \tau) \qquad \text{(since } E[n] \subseteq E(F) \text{ and } \kappa(P, \sigma) \in E[n]).\end{aligned}$$

We conclude that κ is bilinear.

For part c., observe that for $P \in E(F)$, one has $\kappa(P, \sigma) = O$ for all $\sigma \in G_F$ if and only if for all $Q \in E$ with $nQ = P$, one has $Q \in E(F)$. Thus, if $\kappa(P, \sigma) = O$, then choosing any $Q \in E(F)$ with $nQ = P$, we have $P \in nE(F)$; and conversely, if $P \in nE(F)$, then we can choose some $Q \in E(F)$ with $nQ = P$, and thus for any $\sigma \in G_F$ we have $\kappa(P, \sigma) = Q^{\sigma} - Q = Q - Q = O$.

For part d., observe that for $\sigma \in G_F$, one has $\kappa(P, \sigma) = O$ for all $P \in E(F)$ if and only if for all $Q \in E$ with $nQ = P$, one has $Q^{\sigma} = Q$, which is iff σ fixes all points in $[n]^{-1}(E(F))$, iff $\sigma \in G_L$ where $L := F([n]^{-1}(E(F)))$. We also note that L/F is Galois, since automorphisms in G_F take $F([n]^{-1}(E(F)))$ to itself: if $Q \in E$ satisfies $nQ \in E(F)$, then $\forall \sigma \in G_F$, one has $n(Q^{\sigma}) \in E(F)$.

Modding out by the left and right kernel gives the desired perfect pairing. □

To reiterate: we are interesting in showing that $E(F)/nE(F)$ is finite; we can assume that $E[n] \subseteq E(F)$ (re-set $F := F(E[n])$). The Kummer pairing κ above is a perfect bilinear map

$$E(F)/nE(F) \times \mathrm{Gal}(L/F) \to E[n],$$

which means that it induces an injection

$$E(F)/nE(F) \hookrightarrow \mathrm{Hom}(\mathrm{Gal}(L/F), E[n]).$$

Thus, it suffices to show that $\mathrm{Gal}(L/F)$ is finite, i.e., that $[F([n]^{-1}(E(F))) : F] < \infty$. This might seem surprising at first, since $E(F)$ can have infinitely many points. This will be shown using classical Kummer theory from algebraic number theory, as well as our results from Chapter 7 on reduction types. We recall the notion of *good reduction.*

Definition 8.1.2. Let $E_{/F}$ be an elliptic curve and $v = v_{\mathfrak{p}} \in \Sigma_F^{\mathrm{NA}}$ a discrete valuation. Say E has **good reduction** (resp. **bad reduction**) at $\mathfrak{P}$ if $E_{/F_{\mathfrak{P}}}$ has good (resp. bad) reduction. We use $\tilde{E}_{/k_{\mathfrak{P}}}$ to denote the reduction of $E_{/F_{\mathfrak{P}}}$; in particular, it is the reduction of a minimal equation over $F_{\mathfrak{P}}$.

Remark 8.1.2. It might be worth re-noting that an elliptic curve $E_{/F}$ might not have an equation over $\mathcal{O}_F$ that is simultaneously minimal over all $F_{\mathfrak{P}}$ – however, it is possible when F has class number one (this includes $F = \mathbb{Q}$), see §8.8.

Remark 8.1.3. Let $E_{/F}$ have a Weierstrass equation

$$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6,$$

with discriminant Δ. Then for all but finitely many primes $\mathfrak{P} \in \Sigma_F^{\mathrm{NA}}$, one has that each $v_{\mathfrak{P}}(a_i) = 0$, as well as $v_{\mathfrak{P}}(\Delta) = 0$. In particular, such an equation will automatically be minimal over $F_{\mathfrak{P}}$ with good reduction for all but finitely many $\mathfrak{P}$. Thus, *E has good reduction at all but finitely many primes of F.*

Here is a proposition which describes the extension $L := F([n]^{-1}(E(F)))$, which we want to eventually show has finite degree. These properties will imply that $[L : F]$ must be finite, by pure algebraic number theory.

Proposition 8.1.4. [Sil09, Proposition VIII.1.5] *Let $L := F([n]^{-1}(E(F)))$. Assume that $E[n] \subseteq E(F)$.*

a. L/F is abelian with group exponent dividing n, i.e., $\mathrm{Gal}(L/F)$ is an abelian group whose elements have orders which divide n.

b. Let

$$S := \{\mathfrak{P} \in \Sigma_F^{\mathrm{NA}} : E \text{ has bad reduction at } \mathfrak{P}\} \cup \{\mathfrak{P} \in \Sigma_F^{\mathrm{NA}} : \mathfrak{P} \mid n\} \cup \Sigma_F^{\mathrm{Arch}}.$$

Then L/F is unramified away from S, i.e., for all valuations $v = v_{\mathfrak{P}} \notin S$, one has that L/F is unramified at $\mathfrak{P}$.

Remark 8.1.4. We have included the Archimedean places in the definition of S, since there is a notion of a *ramified* Archimedean place of an extension L/F: this is an Archimedean absolute value $|\cdot|$ on F induced from a real embedding $F \hookrightarrow \mathbb{R}$, such that any extension of $|\cdot|$ to L is strictly complex. For example, for odd prime $p \in \mathbb{Z}^+$, we know that $\mathbb{Q}(\zeta_p + \zeta_p^{-1})$ is the maximal totally real subfield of $\mathbb{Q}(\zeta_p)$; the former field is totally real, i.e., all embeddings of $\mathbb{Q}(\zeta_p + \zeta_p^{-1})$ into $\mathbb{C}$ embed it into $\mathbb{R}$; whereas $\mathbb{Q}(\zeta_p)$ is strictly complex, i.e., no embeddings of $\mathbb{Q}(\zeta_p)$ into $\mathbb{C}$ realize it as a subfield of $\mathbb{R}$. In particular, all Archimedean places of $\mathbb{Q}(\zeta_p + \zeta_p^{-1})$ must ramify in $\mathbb{Q}(\zeta_p)$.

Proof. Part a. follows from the elliptic Kummer pairing properties in Proposition 8.1.3 ([Sil09, Proposition VIII.1.2]), since we have an injection

$$\mathrm{Gal}(L/F) \hookrightarrow \mathrm{Hom}(E(F)/nE(F), E[n]), \qquad \sigma \mapsto \kappa(\cdot, \sigma),$$

and $\mathrm{Hom}(E(F)/nE(F), E[n])$ is an abelian group with exponent dividing n.

For part b., observe that L is the compositum of $F(Q)$ where $Q \in [n]^{-1}(E(F))$; thus, if each $F(Q)$ is unramified away from S, then so is L. To this end, fix $Q \in [n]^{-1}(E(F))$, and let $\mathfrak{P} \in \Sigma_F^{\mathrm{NA}} \smallsetminus S$; we want to show that $F(Q)$ is unramified above $\mathfrak{P}$.

Since $\mathfrak{P} \notin S$, we know that E has good reduction at $\mathfrak{P}$, and by Proposition 7.5.1 ([Sil09, Proposition VII.5.1]), we know that for any minimal model of E over $F_{\mathfrak{P}}$, one has $v_{\mathfrak{P}}(\Delta) = 0$. Let $\mathfrak{P}'$ be any prime in $F(Q)$ which divides $\mathfrak{P}$; then E also has good reduction at $\mathfrak{P}'$, and with the same minimal equation over $F_{\mathfrak{P}}$ since $v_{\mathfrak{P}'}(\Delta) = 0$.

To reiterate, we want to show that $F(Q)$ is unramified at $\mathfrak{P}'$, i.e., $e(\mathfrak{P}'|\mathfrak{P}) = 1$. This is equivalent to $K/F_{\mathfrak{P}}$ being an unramified local extension, where $K := (F(Q))_{\mathfrak{P}'}$. In particular, we want to show that the local inertia group $I_{\mathfrak{P}'|\mathfrak{P}}$ for $K/F_{\mathfrak{P}}$ is trivial, which is equivalent to the following: for any automorphism $\sigma \in \mathrm{Aut}(K/F_{\mathfrak{P}})$ which acts trivially on the residue field $k_{\mathfrak{P}'}$ of K, one has that σ acts trivially on $F(Q)$, which is equivalent to $Q^\sigma = Q$.

To this end, let $\sigma \in I_{\mathfrak{P}'|\mathfrak{P}}$; then σ acts trivially on $\tilde{E}_{/k_{\mathfrak{P}'}}$, so under the reduction map $\mathrm{red}\colon E(K) \to \tilde{E}(k_{\mathfrak{P}'})$, we have $(\tilde{Q})^{\tilde{\sigma}} = \tilde{Q}$, i.e.,

$$\widetilde{Q^\sigma - Q} = \tilde{O}.$$

Thus $Q^\sigma - Q$ is in the kernel of reduction. On the other hand, by definition of Q, we know that $nQ \in E(F)$, from which it follows that $Q^\sigma - Q \in E[n]$. However, by Proposition 7.3.1 ([Sil09, Proposition VII.3.1]), since $\mathfrak{P} \nmid n$, we know that $\mathrm{red}\colon E(K)[n] \to \tilde{E}(k_{\mathfrak{P}'})$ is injective. We deduce that $Q^\sigma = Q$. Since $\sigma \in I_{\mathfrak{P}'|\mathfrak{P}}$ was arbitrary, we conclude that $F(Q)$ is unramified at $\mathfrak{P}'$. Since $\mathfrak{P}' \mid \mathfrak{P}$ in $F(Q)$ was arbitrary, we conclude that $F(Q)$ is unramified above $\mathfrak{P}$, and thus $F(Q)/F$ is unramified away from S. □

Now we will prove that that $[L : F]$ is finite, where $L := F([n]^{-1}(E(F)))$. This proof utilizes finiteness of the ideal class group, Kummer theory and finite generation of the group of S-units of a number field.

Proposition 8.1.5. [Sil09, Proposition VIII.1.6] *Let $S \subseteq \Sigma_F$ be a finite set of places with $\Sigma_F^{\mathrm{Arch}} \subseteq S$, and let $n \geq 2$ be an integer. Let L/F be the maximal abelian extension of F having exponent dividing n that is unramified away from S. Then L/F is a finite extension.*

Remark 8.1.5. Recall that for an algebraic extension $F/\mathbb{Q}$ and an integer $n \in \mathbb{Z}^+$, *Kummer theory* describes abelian extensions of F whose Galois groups have exponent dividing n, in terms of subgroups of $F^\times/(F^\times)^n$. More precisely, suppose that $\mu_n \subseteq F$. Then for any subgroup $G \subseteq F^\times/(F^\times)^n$, one can check that $F(G^{1/n})/F$ is Galois, with an abelian Galois group of exponent dividing n; here,

$$G^{1/n} := \{a^{1/n} : \overline{a} \in G\}.$$

Conversely, Kummer theory says that for any abelian extension L/F of exponent dividing n, there exists a subgroup $G \subseteq F^\times/(F^\times)^n$ such that $L = F(G^{1/n})$; explicitly, one has

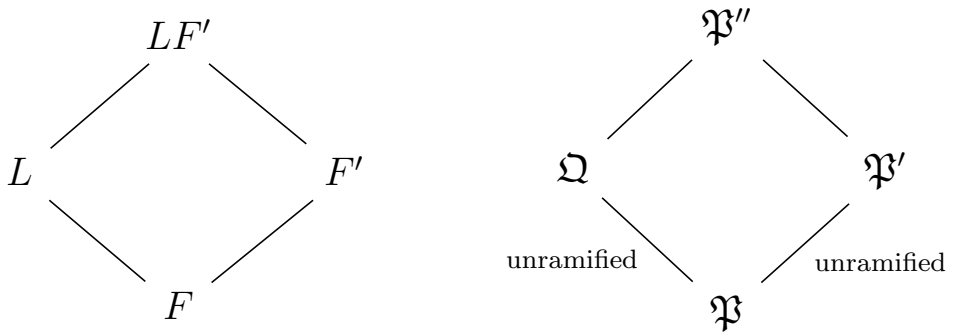
$$G = (F^\times \cap (L^\times)^n)/(F^\times)^n.$$

Thus, when $\mu_n \subseteq F$, we have a correspondence between abelian extensions of F with exponent dividing n, and subgroups of $F^\times/(F^\times)^n$.

Proof. First, some simplifications are in order. Suppose that for the extension $F' := F(\zeta_n)$ and the set S' of primes in F' above S, including those in F' that divide n, the maximal abelian extension L'/F' with exponent dividing n that is unramified away from S' satisfies $[L' : F'] < \infty$. We claim this implies $[L : F] < \infty$. To prove this, we will show by maximality of L' that $LF' \subseteq L'$. Thus, we will show that:

1. LF'/F' is abelian with exponent dividing n.
2. LF'/F' is unramified away from S'.

To see the first part: since L/F is Galois, it follows that LF'/F' is Galois, with $\mathrm{Gal}(LF'/F') \cong \mathrm{Gal}(L/L \cap F')$. Since $\mathrm{Gal}(L/L \cap F') \subseteq \mathrm{Gal}(L/F)$, we find that LF'/F' is abelian of exponent dividing n. For the second part, fix a prime $\mathfrak{P}' \in \Sigma_{F'} \smallsetminus S'$. Then writing $\mathfrak{P} := \mathfrak{P}' \cap F$, as well as $\mathfrak{P}'' \mid \mathfrak{P}'$ in LF'/F' and $\mathfrak{Q} \mid \mathfrak{P}$ in L/F, we have the diagrams



Note that $\mathfrak{Q}/\mathfrak{P}$ is unramified since L/F is unramified away from S, and $\mathfrak{P}'/\mathfrak{P}$ is unramified since $F(\zeta_n)/F$ can only ramify above primes in F which divide n. It follows that $e(\mathfrak{P}''|\mathfrak{P}') = e(\mathfrak{P}''|\mathfrak{Q})$. Thus, if $\mathfrak{P}'$ ramifies in LF', then it follows that $LF' = L(\zeta_n)$ is ramified above $\mathfrak{Q}$, which forces $\mathfrak{Q} \mid n$ – however, since $\mathfrak{Q} \cap F = \mathfrak{P}$, this implies that $\mathfrak{P} \mid n$ and thus $\mathfrak{P}' \mid n$, which is impossible. We deduce that LF'/F' is unramified away from S'. Therefore, maximality of L'/F' implies that $LF' \subseteq L'$. Since $[L' : F]$ is finite, so is $[L : F]$. This proves the claim; in particular, we can assume that $\mu_n \subseteq F$.

Towards proving finiteness of L, we can also add primes to S, since this only enlarges L (note that L ramifies at most at S; enlarging S means we allow more ramification). In particular, let $I_1, I_2, \ldots, I_k \subseteq \mathcal{O}_F$ be distinct integral ideal class representatives of the ideal class group $\mathrm{Cl}(\mathcal{O}_F)$. Adjoining to S all prime ideal divisors of each I_j, we claim that the *ring of S-integers*

$$\mathcal{O}_{F,S} := \{a \in F : v_{\mathfrak{P}}(a) \geq 0 \text{ for all } v_{\mathfrak{P}} \in \Sigma_F \smallsetminus S\},$$

which is the subring of algebraic numbers in F which are integral away from S, is a PID. To see this, note that any ideal $I \subseteq \mathcal{O}_{F,S}$ is a fractional $\mathcal{O}_F$-ideal, and so $[I] \in \mathrm{Cl}(\mathcal{O}_F)$ – thus, there exist $1 \leq j \leq k$ and $\alpha \in F^\times$ such that $I = \alpha \cdot I_j$. Since the class number $k = h_F$ of F is finite, for each prime divisor $\mathfrak{P} \mid I_J$ we know that $\mathfrak{P}^k$ is a *principal* fractional $\mathcal{O}_F$-ideal; we can write $\mathfrak{P}^k = \beta_{\mathfrak{P}}\mathcal{O}_F$ for some $\beta_{\mathfrak{P}} \in \mathcal{O}_F$. We observe that $\beta_{\mathfrak{P}}^{-1} \in \mathcal{O}_{F,S}$ since $v_{\mathfrak{Q}}(\beta_{\mathfrak{P}}) = 0$ for all $\mathfrak{Q} \neq \mathfrak{P} \in \Sigma_F^{\mathrm{NA}}$. In particular, $\mathfrak{P}\mathcal{O}_{F,S}$ contains a unit, and thus $\mathfrak{P}\mathcal{O}_{F,S} = \mathcal{O}_{F,S}$. Since this is true for every $\mathfrak{P} \mid I_j$, we deduce that $I = \alpha\mathcal{O}_{F,S}$, whence we conclude that $\mathcal{O}_{F,S}$ is a PID.

Since $\mu_n \subseteq F$, the fact that L/F is abelian of exponent dividing n implies by Kummer theory that L is the maximal subfield of

$$F(\{a^{1/n} : a \in F^\times\})$$

that is unramified away from S.[14] For $a \in F^\times$, consider the polynomial $x^n - a \in F[x]$. Its discriminant equals $\pm n^n a^{n-1}$ (see e.g. Exercise 0.4.2). Thus, for any prime $\mathfrak{P} \in \Sigma_F \smallsetminus S$, from $v_{\mathfrak{P}}(n) = 0$ we find that $\mathfrak{P}$ is unramified in $F(a^{1/n})$ if and only if $\mathfrak{P} \nmid \pm n^n a^{n-1}$, iff $v_{\mathfrak{P}}(a) = 0$. Therefore, setting

$$T_S := \{\overline{a} \in F^\times/(F^\times)^n : v_{\mathfrak{P}}(a) \equiv 0 \pmod{n} \text{ for all } \mathfrak{P} \in \Sigma_F \smallsetminus S\},$$

[14]For a proof that $F(\{a^{1/n} : a \in F^\times\})$ is the maximal abelian extension of F of exponent dividing n, see Exercise 8.2.1 ([Sil09, Exercise 8.4]).

it follows that $F(T_S^{1/n})/F$ is abelian with exponent dividing n, and is unramified away from S.[15] By maximality of L/F, this implies that $F(T_S^{1/n}) \subseteq L$, which by $L \subseteq F(\{a^{1/n} : a \in F^\times\})$ forces

$$L = F(T_S^{1/n}).$$

Therefore, if T_S is finite, then so is $[L : F]$.

Consider the natural map

$$\mathcal{O}_{F,S}^\times \to T_S, \qquad a \mapsto \overline{a} := a(F^\times)^n. \tag{14}$$

We claim this map is surjective: to this end, let $\overline{a} \in T_S$. Then by definition of T_S, for all $\mathfrak{P} \in \Sigma_F \smallsetminus S$ one has $v_{\mathfrak{P}}(a) = 0$. It follows that a is a unit in $\mathcal{O}_{F,S}$, whence we deduce that (14) is surjective. In fact, since this map contains $(\mathcal{O}_{F,S}^\times)^n$, we have a surjection

$$\mathcal{O}_{F,S}^\times/(\mathcal{O}_{F,S}^\times)^n \twoheadrightarrow T_S.$$

(This is an isomorphism, in fact!) Finally, *Dirichlet's S-unit theorem* says that $\mathcal{O}_{F,S}^\times$ is finitely generated. It follows that $\mathcal{O}_{F,S}^\times/(\mathcal{O}_{F,S}^\times)^n$ is finite, thus so is T_S. □

Proof of weak Mordell-Weil. Let $L := F([n]^{-1}(E(F)))$. Then Proposition 8.1.3 ([Sil09, Proposition VIII.1.2]) shows that $E(F)/nE(F)$ is finite if and only if $[L : F]$ is finite. From Proposition 8.1.4 ([Sil09, Proposition VIII.1.5]), we know that L/F is abelian with exponent dividing n, unramified away from a specific set S. Thus, the previous proposition implies that $[L : F]$ is finite. □

Remark 8.1.6. While the above proof highlights how Kummer theory can be used to show that $L := F([n]^{-1}(E(F)))$ has finite degree over F, there is a shorter proof using the *Hermite-Minkowski theorem,* which states that for any finite subset $S \subseteq \Sigma_F$, there are finitely many extensions of F of bounded degree that are unramified away from S. By Proposition 8.1.4 ([Sil09, Proposition VIII.1.5]), we know that L/F is unramified away from a specific S; thus, writing $L = \prod_{Q \in [n]^{-1}(E(F))} F(Q)$, it follows that each $F(Q)$ is also unramified away from S. However, each $F(Q)$ satisfies $[F(Q) : F] \leq n^2$. To see this, first note that for each $\sigma \in G_F$, we have $Q^\sigma - Q \in E[n]$, and since $E[n] \subseteq E(F)$, this means we can write $Q^\sigma = Q + T_\sigma$ for some $T_\sigma \in E[n] = E(F)[n]$. It follows that the orbit $\mathcal{O}_F(Q)$ of Q under the action of G_F on $E(\overline{\mathbb{Q}})$ has size at most $\#E[n] = n^2$, which proves the claim since $[F(Q) : F] = \#\mathcal{O}_F(Q)$. Therefore, there are finitely many possibilities for $F(Q)$ when $Q \in [n]^{-1}(E(F))$, and thus $[L : F]$ is finite.

Remark 8.1.7. Can we effectively compute $E(F)/nE(F)$? This is of interest if we are trying to compute $E(F)$. Recall that we have an injection from the Kummer pairing:

$$E(F)/nE(F) \hookrightarrow \mathrm{Hom}(G_{L/F}, E[n]), \qquad P + nE(F) \mapsto (\sigma \mapsto Q^\sigma - Q).$$

The proof of Proposition 8.1.4 ([Sil09, Proposition VIII.1.6]) can be made explicit, and thus we can explicitly compute $G_{L/F}$, see Exercise 8.1.1 ([Sil09, Exercise 8.1]); in particular, we can explicitly compute $\mathrm{Hom}(G_{L/F}, E[n])$. Thus, the remaining question

[15] In the definition of T_S, we have the condition $v_{\mathfrak{P}}(a) \equiv 0 \pmod{n}$ instead of $v_{\mathfrak{P}}(a) = 0$ to guarantee that this set is well-defined, since elements are cosets modulo $(F^\times)^n$, and changing representatives can increase/decrease the $\mathfrak{P}$-adic valuation. However, if $\mathcal{O}_F$ is a UFD/PID (such as $F = \mathbb{Q}$), then this congruence can be taken as an equality.

is which elements of this Hom group correspond to elements of $E(F)/nE(F)$. As it turns out, there is no known effective way to determine this; we will discuss this more in Chapter 10. Note, however, that this is the only ineffective part in computing $E(F)$: given generators of $E(F)/nE(F)$, we can effectively compute generators for $E(F)$, see [Sil09, Exercise 8.18].

Exercise 8.1.1. [Sil09, Exercise 8.1] Let $E_{/F}$ be an elliptic curve, let $n \geq 2$ be an integer, let $\mathrm{Cl}(\mathcal{O}_F)$ be the ideal class group of F, and let

$$S := \{v_{\mathfrak{P}} \in \Sigma_F^{\mathrm{NA}} : E \text{ has bad reduction at } \mathfrak{P}\} \cup \{v_{\mathfrak{P}} \in \Sigma_F^{\mathrm{NA}} : \mathfrak{P} \mid n\} \cup \Sigma_F^{\mathrm{Arch}}.$$

Assume that $E[n] \subseteq E(F)$. Prove the following quantitative version of the weak Mordell-Weil theorem:

$$\mathrm{rank}_{\mathbb{Z}/n\mathbb{Z}} E(F)/nE(F) \leq 2 \cdot \#S + 2 \cdot \mathrm{rank}_{\mathbb{Z}/n\mathbb{Z}}(\mathrm{Cl}(\mathcal{O}_F))[n].$$

Exercise 8.1.2. [Sil09, Exercise 8.2] For each integer $d \geq 1$, let $E_d/\mathbb{Q}$ be the elliptic curve

$$E_d : y^2 = x^3 - d^2 x.$$

Prove that

$$E_d(\mathbb{Q}) \cong \mathbb{Z}^r \times T,$$

where T is a finite group and $r \geq 0$ is an integer satisfying

$$r \leq 2\nu(2d),$$

where $\nu(N)$ denotes the number of distinct primes dividing N. (*Hint:* use Exercise 8.1.1 ([Sil09, Exercise 8.1])).

Exercise 8.1.3. [Sil09, Exercise 8.3] Let $E_{/F}$ be an elliptic curve and let L/F be an (infinite) algebraic extension. Suppose that the rank of $E(M)$ is bounded as M ranges over all finite subextensions of L/F, i.e., assume that

$$\sup_{\substack{F \subseteq M \subseteq L: \\ [M:F] < \infty}} \mathrm{rank}(E(M)) < \infty.$$

a. Prove that $E(L) \otimes \mathbb{Q}$ is a finite-dimensional $\mathbb{Q}$-vector space.
b. Assume further that L/F is Galois and that $E(L)[\mathrm{tors}]$ is finite. Prove that $E(L)$ is finitely generated.

8.2. **The Kummer pairing via cohomology.** In this section, we will reinterpret the Kummer pairing from the previous section in terms of Galois cohomology. Galois cohomology will not be used again until Chapter 10.

For a review of group and Galois cohomology, see Appendix B of [Sil09]. We will re-state some definitions and results here, focusing on the zeroth and first cohomology groups.

Definition 8.2.1. Let M be an abelian group, and G a group acting on M on the right. Thus, we have:

1. $m^{1_G} = m$, where $1_G \in G$ is the identity.
2. $m^{\sigma\tau} = (m^\sigma)^\tau$ for all $\sigma, \tau \in G$.

Say that M is a **(right) G-module** if one also has

3. $(m+m')^\sigma = m^\sigma + m'^\sigma$.

Both together are equivalent to putting a $\mathbb{Z}[G]$-module structure on M.

For G-modules M and N, a **G-module homomorphism** is a group homomorphism $\phi\colon M \to N$ that commutes with the action of G on both, i.e.,

$$\phi(m)^\sigma = \phi(m^\sigma).$$

Thus, G-module homomorphisms are equivalent to $\mathbb{Z}[G]$-module homomorphisms.

Example 8.2.1. There are numerous examples of G-modules. One of the more relevant ones for these notes is the G_F-module structure on $E(\overline{\mathbb{Q}})$ for an elliptic curve $E_{/F}$. In this setup, for two elliptic curves $E_{/F}$ and $E'_{/F}$, an F-rational isogeny $\phi\colon E \to E'$ induces a G_F-module homomorphism $\phi\colon E(\overline{\mathbb{Q}}) \to E'(\overline{\mathbb{Q}})$.

Definition 8.2.2. Given a G-module M, the **G-invariant submodule** of M is the G-submodule

$$M^G := \{m \in M : \forall \sigma \in G, m^\sigma = m\}.$$

We sometimes call the elements in M^G "G-rational".

Notes Exercise 8.2.1. Show that for a G-module M, one has a group isomorphism

$$M^G \cong \mathrm{Hom}_{\mathbb{Z}[G]}(\mathbb{Z}, M)$$

(where $\mathbb{Z}$ is considered a G-module with trivial action).

As it turns out, "taking G-invariants" is a left exact functor on the category of G-modules. In particular, a short exact sequence of G-modules

$$0 \to M \xrightarrow{f} N \xrightarrow{g} P \to 0$$

induces an exact sequence

$$0 \to M^G \xrightarrow{f} N^G \xrightarrow{g} P^G$$

(check it!). However, this is not necessarily right exact: that is, a surjective G-module homomorphism $N \to P$ need not induce a surjective homomorphism $N^G \to P^G$, i.e., preimages of G-rational elements need not be G-rational. However, one can use cohomology to extend this latter SES on the right, to attempt to better describe the map $N^G \to P^G$.

The following describes how to understand the cohomology groups of a G-module via cochains. Since we are only concerned with the zeroth and first cohomology groups for these notes (which we also describe later), **this digression can be skipped.** A nice textbook for learning about group and Galois cohomology is [Har20].

Recall that a *cochain complex of R-modules* is a sequence of R-modules and homomorphisms

$$C^\bullet := C_0 \xrightarrow{f^0} C_1 \xrightarrow{f^1} C_2 \xrightarrow{f^2} \dots$$

such that $f^i f^{i-1} = 0$ for all $i \geq 1$. From this, we can define the **i'th cohomology** of $C^\bullet$ as

$$H^i(C^\bullet) := \frac{\ker f^i}{\mathrm{im}\, f^{i-1}}$$

(where $f^{-1}\colon 0 \to M_0$).

Cohomology groups of a G-module can be constructed with the following free resolution of $\mathbb{Z}$. Observe that for each $i \geq 0$, G acts freely on G^{i+1}, hence the free $\mathbb{Z}$-module

$$P_i := \bigoplus_{(\sigma_0,\ldots,\sigma_i)\in G^{i+1}} \mathbb{Z}(\sigma_0,\ldots,\sigma_i)$$

is also a free $\mathbb{Z}[G]$-module, with rank $\#G^{i+1}$; it will have a basis of orbit representatives of G^{i+1} under G. We have maps $d_i\colon P_i \to P_{i-1}$ via

$$d_i(\sigma_0,\ldots,\sigma_i) := \sum_{j=0}^{i}(-1)^j(\sigma_0,\ldots,\hat{\sigma_j},\ldots,\sigma_i) \qquad \text{(delete } j\text{'th entry)}.$$

We also have a map $\epsilon\colon \mathbb{Z}[G] \to \mathbb{Z}$ via

$$\epsilon\left(\sum n_j\sigma_j\right) := \sum n_j,$$

the augmentation map. Then

$$\ldots \xrightarrow{d_3} P_2 \xrightarrow{d_2} P_1 \xrightarrow{d_1} P_0 \xrightarrow{\epsilon} \mathbb{Z} \to 0$$

is a free $\mathbb{Z}[G]$-resolution of $\mathbb{Z}$. Then applying the contravariant $\mathbb{Z}[G]$-functor $\mathrm{Hom}_{\mathbb{Z}[G]}(\cdot, M)$ to the augmented chain complex

$$\ldots P_2 \xrightarrow{d_2} P_1 \xrightarrow{d_1} P_0 \xrightarrow{d_0} 0,$$

we have a new chain complex

$$0 \xrightarrow{\circ d_0} \mathrm{Hom}_{\mathbb{Z}[G]}(P_0, M) \xrightarrow{\circ d_1} \mathrm{Hom}_{\mathbb{Z}[G]}(P_1, M) \xrightarrow{\circ d_2} \mathrm{Hom}_{\mathbb{Z}[G]}(P_2, M) \xrightarrow{\circ d_3} \ldots \tag{15}$$

where $\circ d_i$ denotes precomposition of maps in $\mathrm{Hom}_{\mathbb{Z}[G]}(P_i, M)$ with d_i, i.e., $\varphi\colon P_i \to M \rightsquigarrow \varphi \circ d_i\colon P_{i+1} \to M$. As it turns out, the cohomology of this chain complex is isomorphic to the one given by the "G-invariants" functor $(\cdot)^G$. That is to say, the i'th cohomology group $H^i(G, M)$ satisfies

$$H^i(G, M) \cong \frac{\ker(\circ d_i)}{\mathrm{im}\,(\circ d_{i-1})}.$$

This interpretation of $H^i(G, M)$ is more explicit. For each $i \geq 0$, writing $\mathcal{K}_i := \mathrm{Hom}_{\mathbb{Z}[G]}(P_i, M)$ and $\partial_i := \circ d_{i-1}$, our cochain complex (15) becomes

$$0 \to \mathcal{K}_0 \xrightarrow{\partial_0} \mathcal{K}_1 \xrightarrow{\partial_1} \mathcal{K}_2 \xrightarrow{\partial_2} \ldots.$$

We can check that

$$\mathcal{K}_i = \{G\text{-maps } f\colon G^{i+1} \to M\},$$

where for two G-modules M and N, a map $f\colon M \to N$ is called a **G-map** if it commutes with the action of G, i.e., $f(m^\sigma) = f(m)^\sigma$ (it need not be a homomorphism). The elements of $\mathcal{K}_i$ are called **homogeneous i-cochains with values in M.**

On the other hand, one checks that for an element $f \in \mathcal{K}_i$, i.e., for a homogeneous i-cochain $f\colon G^{i+1} \to M$, one has

$$\partial_i(f) = \sum_{j=0}^{i+1}(-1)^j f(\sigma_0,\ldots,\hat{\sigma_j},\ldots,\sigma_{i+1})$$

where the hat denotes exclusion. We can also write

$$H^i(G,M) = \frac{\ker \partial_i}{\operatorname{im} \partial_{i-1}},$$

where $\partial_{-1} := 0$.

There is one more simplification to be made here. Observe that a homogeneous i-cochain $f\colon G^{i+1} \to M$, being a G-map, is completely determined by its values on elements in G^{i+1} of the form $(1, \sigma_1, \ldots, \sigma_n)$. Noting this, there is an isomorphism of abelian groups $\mathcal{K}_i$ and K_i, where

$$K_i := \{G\text{-maps } f\colon G^i \to M\},$$

given by $(f\colon G^{i+1} \to M) \mapsto (\overline{f}\colon G^i \to M, \overline{f}(\sigma_1, \ldots, \sigma_n) := f(1, \sigma_1, \ldots, \sigma_n))$. Elements of K_i are called *inhomogeneous i-cochains with values in M*. We set $G^0 := 0$, so that $K_0 = M$.

By the commutative diagram

$$\begin{array}{ccc} \mathcal{K}_i & \xrightarrow{\partial_i} & \mathcal{K}_{i+1} \\ \downarrow\cong & & \downarrow\cong \\ K_i & & K_{i+1} \end{array}$$

we can define a new differential map

$$d_i : K_i \to K_{i+1}$$

via transport of structure. More precisely, if $f\colon G^i \to M$ is an inhomogeneous i-cochain, then $d_i f\colon G^{i+1} \to M$ is an inhomogeneous $i+1$-cochain via

$$d_i f(\sigma_1, \ldots, \sigma_{i+1}) := f(\sigma_2, \ldots, \sigma_{i+1})^{\sigma_1} + \sum_{j=1}^{i} (-1)^j f(\sigma_1, \ldots, \sigma_j \sigma_{j+1}, \ldots, \sigma_i) + (-1)^{i+1} f(\sigma_1, \ldots, \sigma_i).$$

It follows that in computing $H^i(G,M)$, we may compute cohomology of the chain complex

$$0 \to K_0 \xrightarrow{d_0} K_1 \xrightarrow{d_1} K_2 \xrightarrow{d_2} \ldots$$

instead. The *i-cocyles* are

$$Z^i(G,M) := \ker d_i = \{\text{maps } f : G^i \to M \mid d_i f = 0\},$$

and the *i-coboundaries* are

$$B^i(G,M) := \operatorname{im} d_{i-1} = \{d_{i-1} f \mid f : G^{i-1} \to M \text{ is a map}\}.$$

From this, we write the i'th cohomology group as

$$H^i(G,M) = \frac{Z^i(G,M)}{B^i(G,M)}.$$

One checks that $H^i(G,M)$ is a G-module.

Here are some examples of cohomology groups. Observe that for any map $f\colon 0 \to M$, we can write $f = m$ for some $m \in M$. Then $d_0 f\colon G \to M$ is defined by $d_0 f(\sigma) = m^\sigma -$

m, and thus $H^0(G,M) = M^G$. To compute $H^1(G,M)$, we observe that $d_1 \colon K_1 \to K_2$ is defined as follows: for a G-module homomorphism $f \colon G \to M$, we have

$$d_1(f(\sigma,\tau)) = f(\tau)^\sigma - f(\sigma\tau) + f(\sigma).$$

Thus, the set of 1-cocyles is

$$Z^1(G,M) = \{G\text{-module homomorphisms } f \colon G \to M : \forall \sigma,\tau \in G, f(\sigma\tau) = f(\tau)^\sigma + f(\sigma)\}$$

(these are also called *crossed homomorphisms*). We also check that the set of 1-coboundaries is

$$B^1(G,M) = \{G\text{-module homomorphisms } f \colon G \to M | \exists m \in M \text{ such that } \forall \sigma \in G, f(\sigma) = m^\sigma - m\}$$

(these are also called *principal crossed homomorphisms*). We can check directly that $B^1(G,M) \subseteq Z^1(G,M)$. Therefore, the first cohomology group of M is crossed homomorphisms modulo principal crossed homomorphisms.

It is worth noting that if M and N are G-modules, and there exists a G-module homomorphism $\phi \colon M \to N$, then ϕ induces a map between each of their cohomology groups. More precisely, for each $i \geq 0$, we have a G-module homomorphism

$$H^i(G,M) \xrightarrow{\phi\circ} H^i(G,N)$$

given by post-composition of i-cocycles.

End of digression. In our setup, we saw that a short exact sequence of G-modules

$$0 \to M \xrightarrow{f} N \xrightarrow{g} P \to 0$$

gave an exact sequence

$$0 \to M^G \xrightarrow{f} N^G \xrightarrow{g} P^G.$$

To measure the failure of this latter sequence being exact, it is extended using cohomological groups. Let us define the zeroth cohomology group as

$$H^0(G,M) := M^G.$$

A map $\xi \colon G \to M$ is called a *1-cochain;* the set $C^1(G,M) := \mathrm{Maps}(G,M)$ is called the *group of 1-cochains.* The *group of 1-cocycles* is

$$Z^1(G,M) := \{\text{maps } \xi \in C^1(G,M) : \xi_{\sigma\tau} = \xi_\sigma^\tau + \xi_\tau \text{ for all } \sigma,\tau \in G\}$$

(here, $\xi_\sigma := \xi(\sigma)$). The *group of 1-coboundaries* is

$$B^1(G,M) := \{\xi \in C^1(G,M) : \exists m \in M \text{ such that } \xi_\sigma = m^\sigma - m \text{ for all } \sigma \in G\}.$$

Then the **first cohomology group** is

$$H^1(G,M) := \frac{Z^1(G,M)}{B^1(G,M)}.$$

You can check that this agrees with the definitions in the digression.

Notes Exercise 8.2.2. Show that for a G-module M, one has $B^1(G,M) \subseteq Z^1(G,M)$. Then argue that $H^1(G,M)$ is a G-module.

Notes Exercise 8.2.3. Show that if M is a G-module for which G acts trivially, then one has $H^1(G,M) = Z^1(G,M) = \mathrm{Hom}_{\mathbb{Z}}(G,M)$.

The following fundamental result illustrates a natural place for cohomology to appear.

Proposition 8.2.1. [Sil09, Proposition B.1.2] *Given a short exact sequence of G-modules,*

$$0 \to M \xrightarrow{f} N \xrightarrow{g} P \to 0,$$

There exists an exact sequence of G-modules,

$$0 \to M^G \xrightarrow{f} N^G \xrightarrow{g} P^G \xrightarrow{\delta} H^1(G, M) \xrightarrow{f\circ} H^1(G, N) \xrightarrow{g\circ} H^1(G, P),$$

with connecting homomorphism $\delta\colon P^G \to H^1(G, M)$ defined as follows. For $p \in P^G$, choose $n \in N$ such that $g(n) = p$, and define a 1-cochain $\xi\colon G \to N$ by

$$\xi_\sigma := n^\sigma - n.$$

Then the values of ξ lie in $f(M)$, so that $\xi \in Z^1(G, P)$. We then define

$$\delta(p) := [\xi] \in H^1(G, M).$$

We are interested specifically in *Galois cohomology,* which is the case where our abelian group M is a *Galois module.* This is where M is a G_k-module where $G_k := \mathrm{Gal}(\overline{k}/k)$ is the absolute Galois group of a perfect field k. In this case, we want our action to be continuous for the profinite topology on G_k and the discrete topology on M; this is equivalent to requiring that for each $m \in M$, its stabilizer

$$\mathrm{Stab}(m) := \{\sigma \in G_k : m^\sigma = m\}$$

is a finite index subgroup of G_k, i.e., its fixed field is finite degree over k.

The previous discussion on group cohomology essentially ports over for Galois cohomology. However, there are important results on Galois modules that we should mention. We have natural Galois modules $(\overline{k}, +)$, $\overline{k}^\times$ and $\mu_n := \mu_n(\overline{k})$. What do we know about their cohomology?

Theorem 8.2.2. [Sil09, Proposition B.2.5] *Let k be a perfect field.*

a. $H^1(G_k, (\overline{k}, +)) = 0$.
b. $H^1(G_k, \overline{k}^\times) = 0$. *(This is* Hilbert's Theorem 90.*)*
c. If $\mathrm{char}(k) = 0$ *or is coprime to n, then*

$$H^1(G_k, \mu_n) \cong k^\times/(k^\times)^n.$$

Now we move on from Appendix B and return to §8.2. Given our observations above, for an elliptic curve $E_{/F}$, what do we know about the Galois cohomology of $E(\overline{\mathbb{Q}})$? Fix an integer $n \geq 2$; then we have a short exact sequence of Galois modules,

$$0 \to E[n] \to E(\overline{\mathbb{Q}}) \xrightarrow{[n]} E(\overline{\mathbb{Q}}) \to 0.$$

We take Galois cohomology to get an exact sequence

$$0 \to E(F)[n] \to E(F) \xrightarrow{[n]} E(F) \xrightarrow{\delta} H^1(G_F, E[n]) \xrightarrow{\iota\circ} H^1(G_F, E(\overline{\mathbb{Q}})) \xrightarrow{[n]\circ} H^1(G_F, E(\overline{\mathbb{Q}}))$$

where $\iota\circ$, induced from the inclusion $\iota\colon E[n] \hookrightarrow E(\overline{\mathbb{Q}})$, takes maps $\xi\colon G_F \to E[n]$ to $\xi\colon G_F \to E(\overline{\mathbb{Q}})$. Since $\mathrm{im}\,[n] = \ker\delta$, we have

$$0 \to E(F)/nE(F) \xrightarrow{\delta} H^1(G_F, E[n]) \xrightarrow{\iota\circ} H^1(G_F, E(\overline{\mathbb{Q}})) \xrightarrow{[n]\circ} H^1(G_F, E(\overline{\mathbb{Q}})).$$

We also check that

$$\operatorname{im}(\iota\circ) = \ker([n]\circ) = \{\text{1-cocycles } \xi\colon G_F \to E(\overline{\mathbb{Q}}) : n\xi = O\} = H^1(G_F, E(\overline{\mathbb{Q}}))[n].$$

However, we also have $\operatorname{im}\delta = \ker(\iota\circ)$. We conclude from the SES

$$0 \to \ker(\iota\circ) \to H^1(G_F, E(\overline{\mathbb{Q}})) \to \operatorname{im}(\iota\circ) \to 0$$

and $E(F)/nE(F) \cong \operatorname{im}\delta = \ker(\iota\circ)$ that we have

$$0 \to E(F)/nE(F) \xrightarrow{\delta} H^1(G_F, E[n]) \xrightarrow{\iota\circ} H^1(G_F, E(\overline{\mathbb{Q}}))[n] \to 0. \tag{16}$$

This is called the *Kummer sequence* for $E_{/F}$.

The connecting homomorphism $\delta\colon E(F)/nE(F) \hookrightarrow H^1(G_F, E[n])$ in the short exact sequence above is explicitly determined by Proposition 8.2.1 ([Sil09, Proposition B.1.2]). Let $P \in E(F)$, and choose $Q \in E(\overline{\mathbb{Q}})$ with $nQ = P$. then $\delta(P)$ is represented by a 1-cochain $\xi\colon G_F \to E[n]$ via $\xi_\sigma := Q^\sigma - Q$. However, this 1-cochain is precisely induced by the Kummer pairing on P, i.e., $\xi_\sigma = \kappa(P, \cdot)$. Thus, the connecting homomorphism in the Kummer sequence (16) is given by the Kummer pairing, and embeds $E(F)/nE(F)$ into $H^1(G_F, E[n])$. This gives an important way to understand the weak Mordell-Weil group.

Remark 8.2.1. If $E[n] \subseteq E(F)$ (this was a running assumption in Section 8.1), then $E[n]$ is a trivial G_F-module, and so by Notes Exercise 8.2.3 we have $H^1(G_F, E[n]) = \operatorname{Hom}_{\mathbb{Z}}(G_F, E[n])$. This implies by (16) that the connecting homomorphism δ induces an injection

$$\delta\colon E(F)/nE(F) \hookrightarrow \operatorname{Hom}_{\mathbb{Z}}(G_F, E[n]), \qquad \overline{P} \mapsto \kappa(P, \cdot).$$

This provides an alternate proof to part c. of Proposition 8.1.3 ([Sil09, Proposition VIII.1.2]).

There is an essentially identical Kummer sequence associated to the subgroup μ_n of n'th roots of unity in $\overline{\mathbb{Q}}$. We have a short exact sequence

$$1 \to \mu_n \to \overline{\mathbb{Q}}^\times \xrightarrow{(\cdot)^n} \overline{\mathbb{Q}}^\times \to 1, \tag{17}$$

which induces a Kummer sequence similar to (16):

$$1 \to F^\times/(F^\times)^n \xrightarrow{\delta} H^1(G_F, \mu_n) \xrightarrow{\iota\circ} H^1(G_F, \overline{\mathbb{Q}}^\times)[n] \to 1.$$

However, in this case, Hilbert's Theorem 90 (Theorem 8.2.2 ([Sil09, Proposition B.2.5])) says that $H^1(G_F, \overline{\mathbb{Q}}^\times) = 1$, which implies this connecting homomorphism δ is not only an injection, but an *isomorphism.* This means the "G_F-invariants" functor is exact on (17), and thus elements of $F^\times/(F^\times)^n$ are in 1-1 correspondence with elements of $H^1(G_F, \mu_n)$; furthermore, by Notes Exercise 8.2.3, when $\mu_n \subseteq F$ this cohomology group is just $\operatorname{Hom}_{\mathbb{Z}}(G_F, \mu_n)$. The simplicity in describing $F^\times/(F^\times)^n$ is in marked contrast to describing $E(F)/nE(F)$, where the connecting homomorphism does not necessarily tell us which elements of $H^1(G_F, E[n])$ come from $E(F)/nE(F)$. We will discuss this more in Chapter 10.

Proposition 8.2.3. [Sil09, Proposition VIII.8.2] *There is an isomorphism*

$$\delta\colon F^\times/(F^\times)^n \xrightarrow{\sim} H^1(G_F,\mu_n)$$

given by

$$\delta(\overline{a}) = \textit{cohomology class of the map } \sigma \mapsto \frac{\alpha^\sigma}{\alpha},$$

where $\alpha \in \overline{\mathbb{Q}}^\times$ is any element satisfying $\alpha^n = a$.

Remark 8.2.2. By the Weil pairing, we know that if $E[n] \subseteq E(F)$ then $\mu_n \subseteq F$. In this case, we have both $H^1(G_F, E[n]) = \mathrm{Hom}_{\mathbb{Z}}(G_F, E[n])$ and $H^1(G_F,\mu_n) = \mathrm{Hom}_{\mathbb{Z}}(G_F, E[n])$. The assumption that $E[n] \subseteq E(F)$ will be used in our first practical example for computing $E(F)$ for a specific example in Chapter 10.

To summarize: from the SES of G_F-modules

$$0 \to E[n] \xrightarrow{\iota} E(\overline{\mathbb{Q}}) \xrightarrow{[n]} E(\overline{\mathbb{Q}}) \to 0,$$

we get the SES

$$0 \to E(F)/nE(F) \xrightarrow{\delta_E} H^1(G_F, E[n]) \xrightarrow{\iota\circ} H^1(G_F, E(\overline{\mathbb{Q}}))[n] \to 0$$

where $\delta_E\colon E(F)/nE(F) \hookrightarrow H^1(G_F, E[n])$ is the connecting homomorphism from general group cohomology. This turns out to be the Kummer pairing, in the sense that

$$\delta_E(\overline{P}) = [\kappa(P,\cdot)].$$

This means we can describe the weak Mordell-Weil group $E(F)/nE(F)$ *if we know which elements of $H^1(G_F, E[n])$ are in* $\operatorname{im}\delta_E$. When $E[n] \subseteq E(F)$, we have $H^1(G_F, E[n]) = \mathrm{Hom}_{\mathbb{Z}}(G_F, E[n])$, which can simplify our analysis.

Similarly, we have a SES

$$1 \to \mu_n \to \overline{\mathbb{Q}}^\times \xrightarrow{(\cdot)^n} \overline{\mathbb{Q}}^\times \to 1,$$

which induces the SES

$$1 \to F^\times/(F^\times)^n \xrightarrow{\delta_F} H^1(G_F,\mu_n) \to H^1(G_F, \overline{\mathbb{Q}}^\times)[n] \to 1.$$

However, in this case the group $H^1(G_F, \overline{\mathbb{Q}}^\times)$ is trivial (by Hilbert's Theorem 90), and thus δ_F is an isomorphism:

$$\delta_F\colon F^\times/(F^\times)^n \xrightarrow{\sim} H^1(G_F,\mu_n), \qquad \delta_F(\overline{a}) := \left[\text{the map } \sigma \mapsto \frac{\alpha^\sigma}{\alpha},\ \text{where } \alpha^n = a\right].$$

Finally, if $E[n] \subseteq E(F)$ then $\mu_n \subseteq F$, and so we have both $H^1(G_F, E[n]) = \mathrm{Hom}_{\mathbb{Z}}(G_F, E[n])$ and $H^1(G_F,\mu_n) = \mathrm{Hom}_{\mathbb{Z}}(G_F, E[n])$.

Exercise 8.2.1. [Sil09, Exercise 8.4] Assume that $\mu_n \subseteq F$. Prove that the maximal abelian extension of F of exponent n is the field

$$F(\{a^{1/n} : a \in F\}).$$

(*Hint:* use [Sil09, Proposition VIII.2.2], which says that every homomorphism $\chi\colon G_F \to \mu_n$ has the form $\chi(\sigma) = \frac{\alpha^\sigma}{\alpha}$ for some $\alpha \in \overline{\mathbb{Q}}^\times$ satisfying $\alpha^n \in F^\times$.)

8.3. **The descent procedure.** As noted previously, the weak Mordell-Weil is necessary to prove that $E(F)$ is finitely generated. However, it is not enough on its own – for example, for any integer $n \geq 2$, the quotient $\mathbb{R}/n\mathbb{R}$ is finite, yet $\mathbb{R}$ is not finitely generated. However, $E(F)$ will be finitely generated because there will be finitely many points in $E(F)$ of a bounded *height,* and multiplication-by-n will generally increase the height of a point.

The following theorem will illustrate what type of height function is necessary to know that if $E(F)/nE(F)$ is finite, then $E(F)$ is finitely generated. We state and prove it in more generality.

Theorem 8.3.1 (Descent Theorem)**.** *Let G be an abelian group. Suppose there exists a height function*

$$h\colon G \to \mathbb{R}$$

with the following 3 properties:

1. *For any element $Q \in G$, there exists a constant $C_1 := C_1(Q)$ such that for all $P \in G$,*
$$h(P+Q) \leq 2h(P) + C_1(Q).$$
2. *There exists an integer $n \geq 2$ and a constant $C_2 := C_2(G)$ such that for all $P \in G$,*
$$n^2 h(P) \leq h(nP) + C_2(G),$$
i.e.,
$$h(nP) \geq n^2 h(P) - C_2(G).$$
3. *For any constant $C_3 \geq 0$, the set*
$$\{P \in G : h(P) \leq C_3\}$$
is finite.

Then if G/nG is finite, then G is finitely generated.

Proof. Let $Q_1, Q_2, \ldots, Q_r \in G$ represent the distinct cosets in G/nG. Let $P \in G$; then there exists $1 \leq i_1 \leq r$ such that $P \equiv Q_{i_1} \pmod{nG}$. Thus we can write

$$P = nP_1 + Q_{i_1}$$

for some $P_1 \in G$. Similarly, for some $1 \leq i_2 \leq r$ we have $P \equiv Q_{i_2} \pmod{nG}$, and so

$$P_1 = nP_2 + Q_{i_2}$$

for some $P_2 \in G$.

It follows that for $k \geq 1$, from a given point $P \in G$, we can produce a list of points

$$\begin{aligned} P &= nP_1 + Q_{i_1} \\ P_1 &= nP_2 + Q_{i_2} \\ &\vdots \\ P_{k-1} &= nP_k + Q_{i_k} \end{aligned} \tag{18}$$

(we also set $P_0 := P$). Observe that for any $1 \leq j \leq k$, we have

$$\begin{aligned} h(P_j) &\leq \frac{1}{n^2}(h(nP_j) + C_2) && \text{(by Property 2. of } h\text{)} \\ &= \frac{1}{n^2}(h(P_{j-1} - Q_{i_j}) + C_2) \\ &\leq \frac{1}{n^2}(2h(P_{j-1}) + C_1(-Q_{i_j}) + C_2) && \text{(by Property 1. of } h\text{)} \\ &\leq \frac{1}{n^2}(2h(P_{j-1}) + C_1' + C_2), \end{aligned}$$

where $C_1' := C_1'(G, n) := \max_{1 \leq i \leq r} C_1(-Q_i)$ depends on the chosen coset representatives of G/nG. Thus, the constant $C_1' + C_2$ is independent of P. This inequality inductively connects $h(P_k)$ to $h(P)$:

$$\begin{aligned} h(P_k) &\leq \frac{1}{n^2}(2h(P_{k-1}) + C_1' + C_2) \\ &\leq \frac{1}{n^2}\left(\frac{2}{n^2}[2h(P_{k-2}) + C_1' + C_2] + C_1' + C_2\right) \\ &= \frac{4}{n^4}h(P_{k-2}) + \left(\frac{1}{n^2} + \frac{2}{n^4}\right)(C_1' + C_2) \\ &\vdots \\ &\leq \left(\frac{2}{n^2}\right)^k h(P) + \left(\sum_{i=1}^{k} \frac{2^{i-1}}{n^{2i}}\right)(C_1' + C_2) \\ &< \left(\frac{2}{n^2}\right)^k h(P) + \left(\frac{1}{n^2 - 2}\right)(C_1' + C_2) && \left(\text{since } \sum_{i=1}^{\infty}\left(\frac{2}{n^2}\right)^i = \frac{2}{n^2 - 2}\right) \\ &\leq \frac{1}{2^k}h(P) + \frac{1}{2}(C_1' + C_2) && \text{(since } n \geq 2\text{)}. \end{aligned}$$

Thus, for k sufficiently large, we have the uniform bound

$$h(P_k) < 1 + \frac{1}{2}(C_1' + C_2).$$

On the other hand, by (18) we know that P is a linear combination of P_k and the $Q_1, Q_2, \ldots, Q_r$: explicitly,

$$P = n^k P_k + \sum_{j=1}^{k} n^{j-1} Q_{i_j}.$$

We conclude that G is generated by the set

$$\{Q_1, Q_2, \ldots, Q_r\} \cup \{R \in G : h(R) < 1 + \frac{1}{2}(C_1' + C_2)\}.$$

However, this latter set $\{R \in G : h(R) < 1 + \frac{1}{2}(C_1' + C_2)\}$ is finite by Property 3. of h. We thus conclude that G is finitely generated. $\square$

With the descent theorem proven, the goal for the rest of this chapter is to prove there exists such a height function on $E(F)$.

Remark 8.3.1. Given a height function h on G, this descent theorem will effectively determine generators for G if we can do the following:

1. Determine coset representatives $Q_1, Q_2, \ldots, Q_r$ for G/nG, and their constants $C_1(-Q_i)$.
2. Calculate the constant $C_2(G)$.
3. For any constant C_3, determine the elements in the set $\{R \in G : h(R) \leq C_3\}$.

By [Sil09, Exercise 8.18], given the height function for elliptic curves (which we describe in Sections 8.5 and 8.6), all of these constants are effectively computable *if we can find generators for* $E(F)/nE(F)$. However, there is no known procedure to give generators of this quotient. This will be discussed more in Chapter 10.

8.5. **Heights on projective space.** In this section, we will describe height functions on projective space, and in the next section we apply them to elliptic curves. Ultimately, we need a height function which satisfies the necessary properties for the descent theorem to apply to $E(F)$. Note that section 8.4 of [Sil09] provides a simpler description of such a height function on elliptic curves in the special case where $F = \mathbb{Q}$, using explicit equations.

Example 8.5.1. We start with defining a notion of height in the case $F = \mathbb{Q}$. Given a point $P \in \mathbb{P}^n(\mathbb{Q})$, we can write

$$P = [x_0 : x_1 : \ldots : x_n]$$

where each $x_i \in \mathbb{Z}$ and $\gcd(x_0, x_1, \ldots, x_n) = 1$; this is unique up to multiplying by ± 1 (check it!). Then the **height** of P is

$$H(P) := \max_{0 \leq i \leq n} |x_i|.$$

This function satisfies Property 3 on boundedness: for any constant $C \geq 0$, the set

$$\{P \in \mathbb{P}^n(\mathbb{Q}) : H(P) \leq C\}$$

is finite, bounded in size by $(2C+1)^{n+1}$ (when P is in integral form, each coordinate has $\leq 2C+1$ options).

When $F \neq \mathbb{Q}$, we might not have that $\mathcal{O}_F$ is a PID, and thus our definition involving GCD's might not make sense (note that UFD is equivalent to PID for Dedekind domains). We are thus led to an alternate definition which works for all number fields.

Definition 8.5.1. Given an absolute value $|\cdot| \in \Sigma_{\mathbb{Q}}$, we say $|\cdot|$ is **standard** if the following holds:

- $|\cdot| = |\cdot|_\infty$ is the usual Archimedean place on $\mathbb{Q}$; so $|\alpha| = \max\{\alpha, -\alpha\}$.
- $|\cdot|$ is equivalent to a non-Archimedean place $|\cdot|_p$ on $\mathbb{Q}$ (so p is prime), and is normalized such that
$$|\alpha| = p^{-v_p(\alpha)},$$
where $v_p(p) = 1$. (See Exercise A.0.3 for discrepancies between equivalent norms.)

We let $M_{\mathbb{Q}}$ denote the set of standard norms on $\mathbb{Q}$. For a number field F, we let M_F denote the set of **standard absolute values on F,** which are those absolute values in Σ_F whose restriction to $\mathbb{Q}$ is one of the standard absolute values in $M_{\mathbb{Q}}$.

Each (standard) absolute value $|\cdot|$ in M_F corresponds to a valuation v on F; we will often interchange $|\cdot|$ with v.

Definition 8.5.2. Let $v \in M_F$. The **local degree at v,** denoted by n_v, is

$$n_v := [F_v : \mathbb{Q}_v],$$

where F_v and $\mathbb{Q}_v$ are the completions of F and $\mathbb{Q}$ at $|\cdot|_v$ and $|\cdot|_v|_{\mathbb{Q}}$, respectively.

Here are results from algebraic number theory on local degrees and products of norms; see e.g. [Lan94, II §1 and V §1].

Theorem 8.5.1 (Extension formula)**.** *Let $L/F/\mathbb{Q}$ be a tower of number fields, and let $v \in M_F$. Then*

$$\sum_{\substack{w \in M_L: \\ w|v}} n_w = [L : F] n_v$$

(here, $w|v$ means that $w|_F = v$). Written differently, we have

$$\sum_{\substack{w \in M_L: \\ w|v}} [L_w : \mathbb{Q}_w] = [L : F] n_v.$$

Theorem 8.5.2 (Product formula)**.** *Let $\alpha \in F^\times$. Then*

$$\prod_{v \in M_F} |\alpha|_v^{n_v} = 1.$$

Example 8.5.2. Here is some intuition for the product formula over $\mathbb{Q}$. The standard absolute values on $\mathbb{Q}$ are the usual Archimedean absolute value $|\cdot|_\infty$, and the p-adic absolute value $|\alpha|_p := p^{-v_p(\alpha)}$. We check that the product

$$\prod_{\text{prime } p \in \mathbb{Z}^+} |\alpha|_p = \prod_{\text{prime } p \in \mathbb{Z}^+} p^{-v_p(\alpha)} = |\alpha|_\infty^{-1},$$

which agrees with what the product formula tells us.

We will now define the height of a projective point.

Definition 8.5.3. Let $P \in \mathbb{P}^n(F)$, and write

$$P = [x_0 : x_1 : \ldots : x_n]$$

with each $x_i \in F$. Then the **height** of P (relative to F) is

$$H_F(P) := \prod_{v \in M_F} \max_{0 \le i \le n} |x_i|_v^{n_v}.$$

Remark 8.5.1. Note that by our definition, for a point $P \in \mathbb{P}^n(F)$, a choice of coordinates $P = [x_0 : x_1 : \ldots : x_n]$ will have that each $v_{\mathfrak{P}}(x_i) = 0$ for all but finitely many primes $\mathfrak{P} \in \Sigma_F^{\mathrm{NA}}$. Thus, the height $H_F(P)$ is a finite value. It is worth remembering that a smaller $\mathfrak{P}$-adic norm corresponds to a higher $\mathfrak{P}$-adic divisibility.

Remark 8.5.2. We can check that this height function relative to $\mathbb{Q}$ agrees with our notion of height in $\mathbb{P}^n(\mathbb{Q})$. For $P \in \mathbb{P}^n(\mathbb{Q})$, let us write $P = [x_0 : x_1 : \ldots : x_n]$, where each $x_i \in \mathbb{Z}$ and $\gcd(x_0, x_1, \ldots, x_n) = 1$. Then our first notion of height is $H(P) = \max_{0 \le i \le n} |x_i|_\infty$. On the other hand, we observe that for each prime $p \in M_\mathbb{Q}$, we have each $|x_i|_p := p^{-v_p(x_i)} \le 1$, with at least one $|x_j|_p = 1$ by the coprimality condition; it follows that $\max_{0 \le i \le n} |x_i|_p = 1$. Therefore,

$$H_\mathbb{Q}(P) := \prod_{v \in M_\mathbb{Q}} \max_{0 \le i \le n} |x_i|_v = \max_{0 \le i \le n} |x_i|_\infty$$

(only the Archimedean place contributes to the product). We deduce that $H(P) = H_\mathbb{Q}(P)$, so the two heights coincide. Consequently, $H_\mathbb{Q}$ satisfies property 3 for height functions.

Let us prove some properties of this relative height function.

Proposition 8.5.3. [Sil09, Proposition VIII.5.4] *Let $P \in \mathbb{P}^n(F)$.*

a. The height $H_F(P)$ does not depend on the choice of projective coordinates for P.

b. The height satisfies

$$H_F(P) \ge 1.$$

c. Let L/F be a finite extension. Then

$$H_L(P) = H_F(P)^{[L:F]}.$$

Proof. To prove part a., suppose that $P = [x_0 : x_1 : \ldots : x_n]$ where each $x_i \in F$. Then any other choice of coordinates has the form $[\lambda x_0 : \lambda x_1 : \ldots : \lambda x_n]$ where $\lambda \in F^\times$. We check that

$$\begin{aligned}
\prod_{v \in M_F} \max_{0 \le i \le n} |\lambda x_i|_v^{n_v} &= \prod_{v \in M_F} \max_{0 \le i \le n} |\lambda|_v^{n_v} \cdot |x_i|_v^{n_v} \\
&= \prod_{v \in M_F} \max_{0 \le i \le n} |\lambda|_v^{n_v} \cdot \prod_{v \in M_F} \max_{0 \le i \le n} |x_i|_v^{n_v} \\
&= \prod_{v \in M_F} \max_{0 \le i \le n} |x_i|_v^{n_v} \qquad \text{(product formula).}
\end{aligned}$$

Thus, $H_F(P)$ is independent of the choice of coordinates for P.

Part b. follows from the fact that we can find a choice of coordinates for P such that at least one coordinate is 1. For part c., the idea is to partition the places in M_L by

which prime in M_F they lie over:

$$\begin{aligned}
H_L(P) :&= \prod_{w\in M_L} \max_{0\le i\le n} |x_i|_w^{n_w} \\
&= \prod_{v\in M_F} \prod_{\substack{w\in M_L:\\ w|v}} \max_{0\le i\le n} |x_i|_w^{n_w} \\
&= \prod_{v\in M_F} \prod_{\substack{w\in M_L:\\ w|v}} \max_{0\le i\le n} |x_i|_v^{n_w} && \text{(since } |\cdot|_w|_F = |\cdot|_F\text{)} \\
&= \prod_{v\in M_F} \left(\max_{0\le i\le n} |x_i|_v\right)^{\sum_{w|v} n_w} && \text{(the terms in the product over } w \mid v \text{ depend only on } v\text{)} \\
&= \prod_{v\in M_F} \left(\max_{0\le i\le n} |x_i|_v\right)^{[L:F]n_v} && \text{(Product formula)} \\
&= H_F(P)^{[L:F]}. && \square
\end{aligned}$$

We can also define a height function that is not relative to any particular number field.

Definition 8.5.4. Let $P \in \mathbb{P}^n(\overline{\mathbb{Q}})$. Then the **absolute height of** P is the positive root

$$H(P) := H_F(P)^{1/[F:\mathbb{Q}]},$$

where F is any number field for which P is F-rational. By the previous proposition, this is well-defined, and we always have $H(P) \ge 1$.

The next three theorems are towards showing that Property 3 holds for our absolute height function – namely, that there are finitely many points of bounded height. We will determine how heights can change under morphisms between projective spaces, which will be important when we study heights on elliptic curves. Recall our definition for morphisms of projective varieties.

Definition 8.5.5. For varieties $V_1 \subseteq \mathbb{P}^m$ and $V_2 \subseteq \mathbb{P}^n$, a **morphism of degree** d **from** V_1 **to** V_2 is a map

$$\phi\colon V_1 \to V_2, \qquad \phi(P) = [F_0(P) : F_1(P) : \ldots : F_n(P)],$$

where each $F_i \in \overline{\mathbb{Q}}[X_0, X_1, \ldots, X_m]$ is a homogeneous polynomial of degree d with no common zeros other than $(0, 0, \ldots, 0)$. If the F_i can be chosen with coefficients in F, then say that ϕ is **defined over** F**.**

Theorem 8.5.4. [Sil09, Theorem VIII.5.6] *Let*

$$\phi\colon \mathbb{P}^m \to \mathbb{P}^n$$

be a degree d morphism. Then there exist constants $C_1 := C_1(\phi), C_2 := C_2(\phi) > 0$ such that for all $P \in \mathbb{P}^n(\overline{\mathbb{Q}})$, one has

$$C_1 \cdot H(P)^d \le H(\phi(P)) \le C_2 \cdot H(P)^d.$$

We will skip this proof. Let us record a corollary for isomorphisms of projective space.

Corollary 8.5.5. [Sil09, Corollary VIII.5.8] *Let $A \in \mathrm{GL}_{n+1}(\overline{\mathbb{Q}})$, so that multiplication by the matrix A induces an automorphism $A\colon \mathbb{P}^n \to \mathbb{P}^n$. Then there exists constants $C_1 := C_1(A), C_2 := C_2(A) > 0$ such that for all $P \in \mathbb{P}^m(\overline{\mathbb{Q}})$, one has*

$$C_1 \cdot H(P)^d \leq H(A \cdot P) \leq C_2 \cdot H(P)^d.$$

Next, we state a result which relates the coefficients of a polynomial to the height of its roots. Given $\alpha \in \overline{\mathbb{Q}}$, we define the height of α as the height of the projective point $[\alpha : 1]$:

$$H(\alpha) := H([\alpha : 1]).$$

Theorem 8.5.6. [Sil09, Theorem VIII.5.9] *Let*

$$f(x) := a_0(x - \alpha_1)(x - \alpha_2)\cdots(x - \alpha_n) = a_0x^n + a_1x^{n-1} + \ldots + a_n$$

be a polynomial over $\overline{\mathbb{Q}}$. Then

$$2^{-n}\prod_{i=1}^{n} H(\alpha_i) \leq H([a_0 : a_1 : \ldots : a_n]) \leq 2^{n-1}\prod_{i=1}^{n} H(\alpha_i).$$

We will not prove this one either; however, we will prove boundedness property 3 for this height function, by applying these two theorems.

Finally, the following theorem shows that points in the same Galois orbit have equal height.

Theorem 8.5.7. [Sil09, Theorem VIII.5.10] *Let $P \in \mathbb{P}^n(\overline{\mathbb{Q}})$ and $\sigma \in G_{\mathbb{Q}}$. Then*

$$H(P^\sigma) = H(P).$$

Proof. Let F be a number field with $P \in \mathbb{P}^n(F)$ and $\sigma \in G_{\mathbb{Q}}$. Then we claim it suffices to show that the relative heights $H_{F^\sigma}(P^\sigma)$ and $H_F(P)$ are equal, where $F^\sigma := \sigma(F)$ is the image of F under σ. From the isomorphism $\sigma\colon F \xrightarrow{\sim} F^\sigma$, we have a bijection between the set of standard places for F and F^σ:

$$\sigma\colon M_F \to M_{F^\sigma} \qquad \text{by } v \mapsto v^\sigma,$$

where for $\beta = \alpha^\sigma \in F^\sigma$ we define $|\beta|_{v^\sigma} := |\alpha|_v$. Since σ also induces an isomorphism $\sigma\colon F_v \xrightarrow{\sim} F_{v^\sigma}^\sigma$, we have the local degree equality $n_v = n_{v^\sigma}$: for example, if v is non-Archimedean and lies above $p \in \mathbb{Z}$, then $[F_{v^\sigma} : \mathbb{Q}_p] = [F_v : \mathbb{Q}_{p^\sigma}]$ (note that σ fixes $\mathbb{Q}$, and thus $\mathbb{Q}_p$). Writing $P = [x_0 : x_1 : \ldots : x_n]$ with each $x_i \in F$, we then compute

$$\begin{aligned}
H_{F^\sigma}(P^\sigma) :&= \prod_{w \in M_{F^\sigma}} \max_{0\leq i\leq n} |x_i^\sigma|_w^{n_w} \\
&= \prod_{v \in M_F} \max_{0\leq i\leq n} |x_i^\sigma|_{v^\sigma}^{n_{v^\sigma}} \\
&= \prod_{v \in M_F} \max_{0\leq i\leq n} |x_i|_v^{n_v} \qquad \text{(each } n_{v^\sigma} = n_v, \text{ and } |x_i^\sigma|_{v^\sigma} = |x_i|_v\text{)} \\
&=: H_F(P). \qquad \square
\end{aligned}$$

We can now prove the boundedness property for H. Recall that for a point $P \in \mathbb{P}^n(\overline{\mathbb{Q}})$, its *field of definition,* denoted $\mathbb{Q}(P)$, is the least extension F of $\mathbb{Q}$ over which P is F-rational. Writing $P = [x_0 : x_1 : \ldots : x_n]$ with some $x_j = 1$, this field is explicitly $\mathbb{Q}(P) = \mathbb{Q}(x_0, x_1, \ldots, x_n)$.

Theorem 8.5.8. [Sil09, Theorem VIII.5.11] *For constants $C, d > 0$, one has that the set*

$$\{P \in \mathbb{P}^n(\overline{\mathbb{Q}}) : H(P) \leq C \text{ and } [\mathbb{Q}(P) : \mathbb{Q}] \leq d\}$$

is a finite set. In particular, for any number field F, the set

$$\{P \in \mathbb{P}^n(F) : H_F(P) \leq C\}$$

is finite.

Proof. The idea for this proof is to reduce to the case $n = 1$, which is precisely the case where we are computing heights of algebraic numbers via the projective line. Then we can use the previous two theorems to conclude our proof.

Let $P \in \mathbb{P}^n(\overline{\mathbb{Q}})$, and write $P = [x_0 : x_1 : \ldots : x_n]$ with some $x_j = 1$. Then $\mathbb{Q}(P) = (x_0, x_1, \ldots, x_n)$, and we have the following lower bound on the height of P in terms of the heights of its coordinates:

$$\begin{aligned} H_{\mathbb{Q}(P)}(P) :&= \prod_{v \in M_{\mathbb{Q}(P)}} \max_{0 \leq i \leq n} |x_i|_v^{n_v} \\ &= \prod_{v \in M_{\mathbb{Q}(P)}} \max_{0 \leq i \leq n} \{|x_i|_v, 1\}^{n_v} \qquad \text{(from some } x_j = 1\text{)} \\ &\geq \max_{0 \leq i \leq n} \left\{ \prod_{v \in M_{\mathbb{Q}(P)}} \max\{|x_i|_v, 1\}^{n_v} \right\} \\ &=: \max_{0 \leq i \leq n} H_{\mathbb{Q}(P)}(x_i) \end{aligned}$$

(Recall that for $\alpha \in \overline{\mathbb{Q}}$, we have $H(\alpha) := H([\alpha : 1])$). In particular, if $H(P) \leq C$ and $[\mathbb{Q}(P) : \mathbb{Q}] \leq d$, then from the definition $H(P) := H_{\mathbb{Q}(P)}(P)^{1/[\mathbb{Q}(P):\mathbb{Q}]}$, we deduce that

$$\max_{0 \leq i \leq n} H_{\mathbb{Q}(P)}(x_i) \leq C^d \qquad \text{and} \qquad \max_{0 \leq i \leq n} [\mathbb{Q}(x_i) : \mathbb{Q}] \leq d.$$

Thus, it suffices to prove that the set

$$\{\alpha \in \overline{\mathbb{Q}} : H(\alpha) \leq C \text{ and } [\mathbb{Q}(\alpha) : \mathbb{Q}] \leq d\} \tag{19}$$

is finite, where we have replaced C with C^d. Note that this is the case where $n = 1$.

Let α be in this set; set $e := [\mathbb{Q}(\alpha) : \mathbb{Q}]$, so that $e \leq d$. Let $\alpha_1 := \alpha, \alpha_2, \ldots, \alpha_e \in \overline{\mathbb{Q}}$ be the Galois conjugates of α. Then then write the minimal polynomial $m(x)$ of α as

$$m(x) = (x - \alpha_1)(x - \alpha_2) \cdots (x - \alpha_e) = x^e + a_1 x^{e-1} + \ldots + a_e;$$

we have $m(x) \in \mathbb{Q}[x]$. We estimate an upper bound on the point corresponding to the *coefficients* of $m(x)$:

$$\begin{aligned} H([1 : a_1 : \ldots : a_e]) &\leq 2^{e-1} \prod_{i=1}^{e} H(\alpha_i) && \text{(by Theorem 8.5.6 ([Sil09, Theorem VIII.5.9]))} \\ &= 2^{e-1} H(\alpha) && \text{(by Theorem 8.5.7 ([Sil09, Theorem VIII.5.10]))} \\ &\leq (2C)^d && \text{(since } H(\alpha) \leq C \text{ and } e \leq d\text{).} \end{aligned}$$

Therefore, we have a bound on the coefficients of the minimal polynomial of α in terms of C and d, since α is in (19). We deduce that the minimal polynomial of any element from (19) has bounded degree and coefficients, and thus there are finitely many options for such polynomials. We conclude that (19) is a finite set, which concludes our proof. □

8.6. **Heights on elliptic curves.** In this section, we apply the theory of heights between projective spaces towards developing the notion of heights on an elliptic curve. A key idea is that for an elliptic curve $E_{/F}$ and a nonconstant rational function $f \in \overline{\mathbb{Q}}(E)$, we have a morphism $f \colon E \to \mathbb{P}^1$, which lets us define the height in terms of heights of projective points.

Definition 8.6.1. For a set S and functions $f, g \colon S \to \mathbb{R}$, say that $f - g$ is **big-oh of 1,** and write

$$f = g + O(1),$$

if there exist constants C_1, C_2 such that for all $P \in S$,

$$C_1 \leq f(P) - g(P) \leq C_2.$$

In particular, $f - g$ is a bounded function.

For an elliptic curve $E_{/F}$, a nonconstant function $f \in \overline{\mathbb{Q}}(E)$ induces a morphism

$$f \colon E \to \mathbb{P}^1, \qquad P \mapsto \begin{cases} [1:0] & \text{if } P \text{ is a pole of } f, \\ [f(P):1] & \text{otherwise.} \end{cases}$$

We can try to define a height function $H_f \colon E(\overline{\mathbb{Q}}) \to \mathbb{R}$ via $H_f(P) := H(f(P))$; however, it is more convenient to have a function which behaves additively, so we take an alternate definition.

Definition 8.6.2. The **(absolute logarithmic) height** on project space is the function

$$h \colon \mathbb{P}^n(\overline{\mathbb{Q}}) \to \mathbb{R}, \qquad h(P) := \ln H(P).$$

Note that Proposition 8.5.3 ([Sil09, Proposition VIII.5.4]) implies that $h(P) \geq 0$ for all $P \in \mathbb{P}^n(\overline{\mathbb{Q}})$.

Definition 8.6.3. Let $E_{/F}$ be an elliptic curve, and let $f \in \overline{\mathbb{Q}}(E)$ be a nonconstant function. Then the **height on E (relative to f)** is the function

$$h_f \colon E \to \mathbb{R}, \qquad h_f(P) := \ln h(f(P)).$$

Finiteness of points of bounded height in projective space, implies finiteness of points of bounded height on our elliptic curve with respect to our new height function:

Proposition 8.6.1. [Sil09, Proposition VIII.6.1] *Let $E_{/F}$ be an elliptic curve and $f \in F(E)$ a nonconstant function. Then for any constant $C \geq 0$, the set*

$$\{P \in E(F) : h_f(P) \leq C\}$$

is finite.

Proof. Since f is defined over F, it induces an F-rational morphism $f\colon E(F) \to \mathbb{P}^1(F)$ in the usual way. In particular, f maps the set in question to the set

$$\{Q \in \mathbb{P}^1(F) : H(Q) \leq e^C\}.$$

However, this latter set is finite by Theorem 8.5.8 ([Sil09, Theorem VIII.5.11]); thus, since the morphism $f\colon E \to \mathbb{P}^1$ has finite fibers, we conclude that the set in question is also finite. □

The next theorem relates the height function on an elliptic curve to its group law.

Theorem 8.6.2. [Sil09, Theorem VIII.6.2] *Let $E_{/F}$ be an elliptic curve, and let $f \in F(E)$ be an even function, i.e., $f \circ [-1] = f$. Then for all $P, Q \in E(\overline{\mathbb{Q}})$, we have*

$$h_f(P+Q) + h_f(P-Q) = 2h_f(P) + 2h_f(Q) + O(1),$$

where the implicit constants in $O(1)$ depend only on E and f.

Similar to the proof of part c. of Theorem 3.6.2 ([Sil09, Theorem III.6.2]), the proof involves algebra with coordinates that is not very pleasant, so we will forgo it. Since we are only considering even functions, the proof reduces to taking $f := x$, the Weierstrass coordinate (since $F(x)$ is the subfield of $F(E)$ of even functions).

Here is a corollary of this theorem, which shows that h_f will satisfy the first two properties we require to show that $E(F)$ is finitely generated by the descent theorem.

Corollary 8.6.3. [Sil09, Corollary VIII.6.4] *Let $E_{/F}$ be an elliptic curve, and let $f \in F(E)$ be an even function.*

a. Let $Q \in E(\overline{\mathbb{Q}})$. Then for all $P \in E(\overline{\mathbb{Q}})$,

$$h_f(P+Q) \leq 2h_f(P) + O(1),$$

where $O(1)$ depends on E, f and Q.

b. Let $n \in \mathbb{Z}$. Then for all $P \in E(\overline{\mathbb{Q}})$,

$$h_f(nP) = n^2 h_f(P) + O(1),$$

where $O(1)$ depends on E, f and n.

Proof. Part a. is immediate by the previous theorem, which says that $h_f(P+Q) + h_f(P-Q) = 2h_f(P) + 2h_f(Q) + O(1)$, where $O(1)$ depends on E and f (note that $h_f(P-Q) \geq 0$). For part b., it suffices to consider $n \geq 0$ since f is even. This is clearly true for $n = 0, 1$, and we proceed by induction for the other n.

Suppose this result is true for $n-1$ and n. Then we wish to show that $h_f((n+1)P) = (n+1)^2 h_f(P) + O(1)$. Taking $P := nP$ and $Q := P$ in the theorem above, we have

$$\begin{aligned} h_f((n+1)P) &= 2h_f(nP) + 2h_f(P) - h_f((n-1)P) + O(1) \\ &= 2n^2 h_f(P) + 2h_f(P) - (n-1)^2 h_f(P) + O(1) \quad \text{(by inductive hypothesis)} \\ &= (2n^2 + 2 - (n-1)^2) h_f(P) + O(1) \\ &= (n+1)^2 h_f(P) + O(1). \end{aligned}$$

This completes the proof by induction. □

Remark 8.6.1. It is worth noting that this theorem and corollary also hold for odd functions $f \in F(E)$, since f^2 is even and $h_{f^2} = 2h_f$.

We are now able to prove the main theorem of these notes: the Mordell-Weil theorem.

Theorem 8.6.4 (Mordell-Weil)**.** *Let F be a number field and $E_{/F}$ an elliptic curve. Then $E(F)$ is finitely generated.*

Proof. Fix e.g. $n := 2$. We know by the weak Mordell-Weil theorem (Theorem 8.1.1) that $E(F)/2E(F)$ is finite. By the descent theorem (Theorem 8.3.1), $E(F)$ is finitely generated if there exists a function $h\colon E(F) \to \mathbb{R}$ such that the following holds:

1. For $Q \in E(F)$, there exists a constant $C_1 := C_1(E(F), Q)$ such that for all $P \in E(F)$,
$$h(P+Q) \leq 2h(P) + C_1.$$
2. There exists a constant $C_2 := C_2(E(F))$ such that for all $P \in E(F)$,
$$h(nP) \geq n^2 h(P) - C_2.$$
3. For every constant $C_3 \geq 0$, the set
$$\{P \in E(F) : h(P) \leq C_3\}$$
is finite.

However, for the associated height function $h_x\colon E(F) \to \mathbb{R}$, we know by Corollary 8.6.3 ([Sil09, Corollary VIII.6.4]) that Properties 1 and 2 hold for h_x, and Property 3 holds by Proposition 8.6.1 ([Sil09, Proposition VIII.6.1]). This concludes the proof of the Mordell-Weil theorem! □

Corollary 8.6.5. *For any elliptic curve $E_{/F}$, one has*

$$E(F) \cong \mathbb{Z}^r \oplus E(F)[\text{tors}]$$

for some $r := r_{E,F} \geq 0$.

In the next and final chapter for us (Chapter 10 of [Sil09]) we will focus on techniques for computing the Mordell-Weil group of an elliptic curve (in special cases).

8.9. **The canonical height.** Before wrapping this chapter up, there is one more interesting result to highlight. Given that our construction of the height function uses any even function, a natural question is whether there exists a "canonical" height function for an elliptic curve to study (possibly h_x). The height functions we described are more or less quadratic forms "up to $O(1)$" (see Section 3.6 for the definition of a quadratic form). However, the following height function is indeed a quadratic form on the free part of an elliptic curve Mordell-Weil group $E(F)$. This result is due to Tate.

Proposition 8.9.1. [Sil09, Proposition VIII.9.1] *Let $E_{/F}$ be an elliptic curve and $f \in F(E)$ a nonconstant even function. Then for a point $P \in E(\overline{\mathbb{Q}})$, the limit*

$$\frac{1}{\deg(f)} \lim_{n\to\infty} 4^{-n} h_f(2^n P)$$

exists and is independent of f.

This result lets us define a canonical height function.

Definition 8.9.1. The **canonical** (or **Néron-Tate) height on $E_{/F}$,** denoted by $\hat{h}$ or $\hat{h}_E$, is the function

$$\hat{h}\colon E(\overline{\mathbb{Q}}) \to \mathbb{R}$$

defined by

$$\hat{h}(P) := \frac{1}{\deg(f)} \lim_{n\to\infty} 4^{-n} h_f(2^n P),$$

where $f \in F(E)$ is any nonconstant even function.

Theorem 8.9.2. [Sil09, Theorem VIII.9.3] *Let $E_{/F}$ be an elliptic curve, and let $\hat{h}$ be the canonical height on E.*

a. For all $P, Q \in E(\overline{\mathbb{Q}})$, we have

$$\hat{h}(P+Q) + \hat{h}(P-Q) = 2\hat{h}(P) + 2\hat{h}(Q) \text{ (parallelogram law).}$$

b. For all $P \in E(\overline{\mathbb{Q}})$ and all $n \in \mathbb{Z}$,

$$\hat{h}(nP) = n^2 \hat{h}(P).$$

c. The canonical height $\hat{h}$ is a quadratic form on E, i.e., $\hat{h}$ is an even function and the pairing

$$\langle \cdot, \cdot \rangle\colon E(\overline{\mathbb{Q}}) \times E(\overline{\mathbb{Q}}) \to \mathbb{R}$$

via

$$\langle P, Q \rangle := \hat{h}(P+Q) - \hat{h}(P) - \hat{h}(Q)$$

is bilinear.

d. Let $P \in E(\overline{\mathbb{Q}})$. Then $\hat{h}(P) \geq 0$, and

$$\hat{h}(P) = 0 \Leftrightarrow P \text{ is a torsion point.}$$

e. Let $f \in F(E)$ be an even function. Then

$$\deg(f) \cdot \hat{h} = h_f + O(1),$$

where $O(1)$ depends on E and f.

Furthermore, if $\hat{h}' \colon E(\overline{\mathbb{Q}}) \to \mathbb{R}$ *is any other function satisfying part e. for some non-constant even function* f *and satisfying part b. for some integer* $n \geq 2$*, then* $\hat{h}' = \hat{h}$*.*

For more details on the canonical height, see §8.9 of [Sil09].

10. Computing the Mordell-Weil Group

While one of the main goals for these notes was to prove the Mordell-Weil theorem, another goal is to have techniques to compute the structure of the Mordell-Weil group. As seen in Chapter 8, given an elliptic curve E over a number field F and an integer $n \geq 2$, if we determine generators for $E(F)/nE(F)$ then we can effectively compute generators for $E(F)$, see [Sil09, Exercise 8.18]. However, there is no known algorithm to compute $E(F)/nE(F)$ in a finite amount of time. For the remainder of these notes, we will illustrate how one can make explicit the proof of the weak Mordell-Weil theorem to compute the quotient $E(F)/nE(F)$ in special cases, thus giving us the structure of $E(F)$. The specific case we will do an example for is where $E[2] \subseteq E(F)$; note that $E[n] \subseteq E(F)$ was a running assumption for most of §8.1.

Following this, we will discuss how the auxiliary spaces which show up in our techniques are *twists* of our starting elliptic curve, how the techniques can go wrong when the local-global principle fails for these twists, and how the *Selmer* and *Shafarevich-Tate groups* measure this failure.

For the rest of this chapter, we will adopt the same notation as in Chapter 8. It is worth noting that much of the content of Section 10.1 can be generalized to a perfect field k.

10.1. **An example.** Let $E_{/F}$ be an elliptic curve and $n \geq 2$ an integer. We will assume throughout this section that $E[n] \subseteq E(F)$; thus, we have from Section 8.2 that $H^1(G_F, E[n]) = \mathrm{Hom}_{\mathbb{Z}}(G_F, E[n])$. Recall that there exists a short exact sequence

$$0 \to E(F)/nE(F) \xrightarrow{\delta_E} \mathrm{Hom}_{\mathbb{Z}}(G_F, E[n]) \xrightarrow{\iota\circ} H^1(G_F, E(\overline{\mathbb{Q}}))[n] \to 0$$

where

$$\delta_E \colon E(F)/nE(F) \hookrightarrow \mathrm{Hom}_{\mathbb{Z}}(G_F, E[n])$$

is given via the elliptic Kummer pairing:

$$\delta_E(\overline{P}) := \kappa(P, -), \qquad \text{with } \kappa(P, \sigma) := Q^\sigma - Q \text{ where } nQ = P.$$

Since $E[n] \subseteq E(F)$ implies that $\mu_n \subseteq F$, by Hilbert's Theorem 90 we also have an isomorphism

$$\delta_F \colon F^\times/(F^\times)^n \xrightarrow{\sim} \mathrm{Hom}_{\mathbb{Z}}(G_F, \mu_n)$$

via

$$\delta_F(\overline{a})(\sigma) := \frac{\alpha^\sigma}{\alpha} \text{ where } \alpha^n = a.$$

One way to understand $\operatorname{im}\delta_E$, and thus $E(F)/nE(F)$, is to connect it to the better-understood δ_F via the Weil pairing. Recall that the n-Weil pairing

$$e_n \colon E[n] \times E[n] \to \mu_n$$

is a perfect bilinear pairing with a slew of nice properties, see Proposition 3.8.1 ([Sil09, Proposition III.8.1]). We spent some time going through its construction, which we summarize here:

1. Fix $S, T \in E[n]$; we would like to compute $e_n(S, T)$.

2. We can write $n(T) - n(O) = \operatorname{div}(f_T)$ and $[n]^*((T) - (O)) = \operatorname{div}(g_T)$ for some rational functions $f_T, g_T \in F(E)$ which depend on T. (Note that f_T, g_T can be chosen to be defined over F by [Sil09, Exercise 2.13].)
3. Thus (up to constants) we have $f_T \circ [n] = g_T^n$. It follows from this that the rational function $\frac{g_T \circ \tau_S}{g_T} \in \overline{\mathbb{Q}}(E)$ is constant with a fixed value in μ_n (recall that τ_S is the translation-by-S morphism on E). We set $e_n(S,T) := \frac{g_T(X+S)}{g_T(X)}$ for any point $X \in E$ where this rational function is defined and nonzero.

Remark 10.1.1. Note that $n(T) - n(O) = \operatorname{div}(f_T)$ implies f_T is unique up to scalar. However, $f_T \circ [n] = g_T^n$ with $g_T^n \in F(E)$ implies that f_T is well-defined up to scalar from $(F^\times)^n$. In particular, for any point $X \in E$ where f_T is defined, we know that $f_T(X)$ is well-defined modulo $(F^\times)^n$, regardless of scalar.

Given that $\delta_E \colon E(F)/nE(F) \hookrightarrow \operatorname{Hom}_{\mathbb{Z}}(G_F, E[n])$, we have the following. For any point $P \in E(F)$, we have a group homomorphism $\delta_E(\overline{P}) \colon G_F \to E[n]$; then for any torsion point $T \in E[n]$, we get a map

$$e_n(\delta_E(\overline{P})(-), T) \colon G_F \to \mu_n.$$

This is a homomorphism since $\delta_E(\overline{P})$ is a homomorphism, and e_n is linear in the first coordinate. On the other hand, we have an isomorphism

$$\delta_F \colon F^\times/(F^\times)^n \xrightarrow{\sim} \operatorname{Hom}_{\mathbb{Z}}(G_F, \mu_n);$$

thus, $e_n(\delta_E(\overline{P})(-), T)$ can be identified with the element

$$\delta_F^{-1}(e_n(\delta_E(\overline{P})(-), T)) \in F^\times/(F^\times)^n.$$

To summarize the above, we have a map

$$b \colon E(F)/nE(F) \times E[n] \to F^\times/(F^\times)^n$$

via

$$b(\overline{P}, T) := \delta_F^{-1}(e_n(\delta_E(\overline{P})(-), T)),$$

i.e., via the equivalence of homomorphisms

$$e_n(\delta_E(\overline{P})(-), T) = \delta_F(b(\overline{P}, T))(-)$$

as maps $G_F \to \mu_n$. We will show that this map is a bilinear pairing and is nondegenerate on the left, and has an explicit description via the definition of e_n. This will give us another way to describe $E(F)/nE(F)$. To ease notation, **for the rest of this section we will write elements $\overline{a} \in F^\times/(F^\times)^n$ simply as a.**

Theorem 10.1.1. [Sil09, Theorem X.1.1] *Define the map*

$$b \colon E(F)/nE(F) \times E[n] \to F^\times/(F^\times)^n$$

via

$$e_n(\delta_E(\overline{P})(-), T) = \delta_F(b(\overline{P}, T))(-) \tag{20}$$

as maps $G_F \to \mu_n$, i.e.,

$$b(\overline{P}, T) := \delta_F^{-1}(e_n(\delta_E(\overline{P})(-), T)). \tag{21}$$

a. This pairing is bilinear.

b. This pairing is nondegenerate on the left.

c. Let

$$S := \{\mathfrak{P} \in \Sigma_F^{\mathrm{NA}} : E \text{ has bad reduction at } \mathfrak{P}\} \cup \{\mathfrak{P} \in \Sigma_F^{\mathrm{NA}} : \mathfrak{P} \mid n\} \cup \Sigma_F^{\mathrm{Arch}}.$$

Then the image of b lies in the subgroup

$$F(S,n) := \{\overline{a} \in F^\times/(F^\times)^n : \forall \mathfrak{P} \in \Sigma_F \smallsetminus S, v_{\mathfrak{P}}(a) \equiv 0 \pmod{n}\}$$

of $F^\times/(F^\times)^n$.

d. Explicitly, when $\overline{P} \neq \overline{O}, \overline{T}$ we have

$$b(\overline{P}, T) = f_T(P) \mod (F^\times)^n. \tag{22}$$

We can also compute $b(\overline{T}, T)$ using linearity. For example, if $\overline{T} \neq \overline{O}$ and $2T \neq O$, then $b(\overline{T}, T) = f_T(-T)^{-1}$. More generally, let $Q \in E(F)$ satisfy $\overline{Q} \neq \overline{O}, \overline{T}$; then $b(\overline{T}, T) = f_T(T+Q) \cdot f_T(Q)^{-1}$.

Remark 10.1.2. The pairing b in Theorem 10.1.1 is a special case of the *Tate-Lichtenbaum pairing* where we assume $E[n] \subseteq E(F)$; this more general pairing has applications in cryptography. To read more about its applications, see §11.9 [Sil09].

Proof. For part a., we want to show that

$$b(\overline{P_1 + P_2}, T) = b(\overline{P_1}, T) \cdot b(\overline{P_2}, T).$$

This follows from (21), since δ_E is a homomorphism, e_n is linear in its left coordinate, and δ_F^{-1} is a homomorphism (in that order). We also want to show that

$$b(\overline{P}, T_1 + T_2) = b(\overline{P}, T_1) \cdot b(\overline{P}, T_2).$$

Similarly, this follows from (21) since e_n is linear in its second coordinate, and δ_F^{-1} is a homomorphism.

For part b., we need to show that b is injective in its left coordinate. To this end, suppose for $\overline{P} \in E(F)/nE(F)$ that for all $T \in E[n]$ we have $b(\overline{P}, T) = 1(F^\times)^n$. Then by (21), this says that

$$\delta_F^{-1}(e_n(\delta_E(\overline{P})(-), T)) = 1(F^\times)^n,$$

i.e.,

$$e_n(\delta_E(\overline{P})(-), T) = 1_{G_F}$$

where $1_{G_F} \colon G_F \to F^\times/(F^\times)^n$ is the constant homomorphism. This implies that for all $\sigma \in G_F$, we have

$$e_n(\delta_E(\overline{P})(\sigma), T) = 1;$$

since e_n is nondegenerate on the left (also on the right), this forces $\delta_E(\overline{P})(\sigma) = O$ for all $\sigma \in G_F$; thus $\delta_E(\overline{P})$ is the zero map. Since $\delta_E \colon E(F)/nE(F) \hookrightarrow \mathrm{Hom}_{\mathbb{Z}}(G_F, E[n])$ is injective, this forces $\overline{P} = \overline{O}$. This proves that b is nondegenerate on the left coordinate.

For part c., let us choose $\beta \in \overline{\mathbb{Q}}$ such that $\beta^n = b(\overline{P}, T)$. Then by definition of δ_F, we have for all $\sigma \in G_F$ that

$$\delta_F(b(\overline{P}, T))(\sigma) = \frac{\beta^\sigma}{\beta}.$$

We claim that $\beta \in L := F([n]^{-1}(E(F)))$, the extension we considered in Section 8.1. If this is the case, then from the proof of Proposition 8.1.5 ([Sil09, Proposition VIII.1.6]) it follows that for all $\mathfrak{P} \in \Sigma_F \smallsetminus S$, we have $v_{\mathfrak{P}}(b(\overline{P}, T)) \equiv 0 \pmod{n}$.

To show that $\beta \in L$, it is equivalent to show that for all $\sigma \in G_L$, we have $\beta^\sigma = \beta$. Fix $\sigma \in G_L$, and fix $Q \in E(\overline{\mathbb{Q}})$ with $nQ = P$; then by definition, we have $\delta_E(\overline{P})(\sigma) := Q^\sigma - Q$. As noted above, we have

$$\delta_F(b(\overline{P}, T))(\sigma) := \frac{\beta^\sigma}{\beta}.$$

However, we also check that

$$\begin{aligned} e_n(\delta_E(\overline{P})(\sigma), T) &= e_n(Q^\sigma - Q, T) && \text{(since } \delta_E \text{ is the elliptic Kummer pairing)} \\ &= e_n(O, T) && \text{(since } Q \text{ is } L\text{-rational)} \\ &= 1. \end{aligned}$$

We deduce by (20) that $\beta^\sigma = \beta$, whence we conclude that $\beta \in L$, which proves part c. by our previous discussion.

For part d., let us fix $Q \in E(\overline{\mathbb{Q}})$ and $\beta \in \overline{\mathbb{Q}}$ with $nQ = P$ and $\beta^n = b(\overline{P}, T)$, respectively. Then we expand (20):

$$\begin{aligned} \delta_F(b(\overline{P}, T))(\sigma) &= e_n(\delta_E(\overline{P})(\sigma), T) \\ &= e_n(Q^\sigma - Q, T) && \text{(by definition of } \delta_E) \\ &= \frac{g_T(X + Q^\sigma - Q)}{g_T(X)} && \text{(by definition of } e_n) \\ &= \frac{g_T(Q^\sigma)}{g_T(Q)} && \text{(taking } X := Q) \\ &= \frac{g_T(Q)^\sigma}{g_T(Q)} && \text{(since } g_T \text{ is defined over } F). \end{aligned}$$

Note that we can take $X := Q$ above, since from $\operatorname{div}(g_T) = [n]^*((T) - (O))$ we know that:

1. g_T has zeroes precisely at preimages of T under $[n]$. Thus Q is not a zero of g_T, since $nQ = P \neq T$.
2. g_T has poles precisely at points in $E[n]$. Thus Q is not a pole since $nQ = P \neq O$.

(See Definition 2.3.4 for our description of $[n]^*((T) - (O))$.) Since $g_T(Q)^n = f_T(nQ) = f_T(P)$, we have by definition of δ_F that $\delta_F(f_T(P))(\sigma) := \frac{g_T(Q)^\sigma}{g_T(Q)}$. This and the calculations above implies that

$$\delta_F(b(\overline{P}, T))(\sigma) = \delta_F(f_T(P))(\sigma),$$

for all $\sigma \in G_F$. Since $\delta_F \colon G_F \to F^\times/(F^\times)^n$ is an isomorphism, we conclude that $b(\overline{P}, T) = f_T(P) \mod (F^\times)^n$ when $P \neq T$.

We can also use linearity to compute $b(\overline{T}, T)$ when $\overline{T} \neq \overline{O}$ (of course, $b(\overline{O}, O) = 1(F^\times)^n$). For example, if $2T \neq O$ then $-T \neq T$, and thus

$$b(\overline{-T}, T) = f_T(-T) \mod (F^\times)^n;$$

however, bilinearity of b implies that $b(\overline{-T}, T) = b(\overline{T}, T)^{-1}$, which gives us the formula

$$b(\overline{T}, T) = f_T(-T)^{-1} \mod (F^\times)^n.$$

More generally, with an element $\overline{Q} \neq \overline{O}, \overline{T}$, bilinearity implies that

$$\begin{aligned} b(\overline{T}, T) &= b(\overline{T+Q} - \overline{Q}, T) \\ &= b(\overline{T+Q}, T) \cdot b(-\overline{Q}, T) \\ &= f_T(T+Q) \cdot f_T(Q)^{-1} \mod (F^\times)^n. \end{aligned}$$

□

Let us see how we can use this theorem to compute $E(F)$ when $E[n] \subseteq E(F)$. Since b is nondegenerate on the left and has its image contained in $F(S,n)$, it induces an embedding

$$E(F)/nE(F) \hookrightarrow \mathrm{Hom}_{\mathbb{Z}}(E[n], F(S,n)), \qquad \overline{P} \mapsto b(\overline{P}, -).$$

Furthermore, when $P \neq T$ we have $b(\overline{P}, T) = f_T(P) \mod (F^\times)^n$. Therefore, fixing a basis $\{T_1, T_2\}$ of $E[n]$, if we want to determine the distinct elements of $E(F)/nE(F)$, we can range over pairs $(b_1, b_2) \in F(S,n) \times F(S,n)$ and search for solutions $(P, z_1, z_2) \in E(F) \times F^\times \times F^\times$ to

$$b_1 z_1^n = f_{T_1}(P) \qquad \text{and} \qquad b_2 z_2^n = f_{T_2}(P).$$

Assuming E is in Weierstrass form, we can give coordinates $P = (x, y)$ and equivalently look for $(x, y, z_1, z_2) \in F \times F \times F^\times \times F^\times$ which satisfies

$$y^2 + a_1 xy + a_3 y = x^3 + a_2 x^2 + a_4 x + a_6,$$

$$b_1 z_1^n = f_{T_1}(x, y) \qquad \text{and} \qquad b_2 z_2^n = f_{T_2}(x, y).$$

This technique should be feasible since $F(S,n)$ is finite and relatively easy to compute, and the auxiliary functions $f_{T_1}, f_{T_2} \in E[n]$ should also be relatively easy to compute. Note that these 3 equations will define a new called curve a *homogeneous space for* $E_{/F}$, which is covered in §10.3 of [Sil09].

Remark 10.1.3. As noted in the beginning of the chapter, if we compute $E(F)/nE(F)$, then we can effectively compute $E(F)$ by [Sil09, Exercise 8.18]. However, even without this exercise, we can often compute the abstract group structure of $E(F)$ by using Theorem 10.1.1 and a computation of $E(F)[\mathrm{tors}]$ (the latter of which can be done with the local techniques described in Chapter 7). Observe that if we write $E(F) \cong \mathbb{Z}^r \times E(F)[\mathrm{tors}]$ with $r \geq 0$, then we have $E(F)/nE(F) \cong (\mathbb{Z}/n\mathbb{Z})^r \times E(F)[\mathrm{tors}]/nE(F)[\mathrm{tors}]$. One of our running assumptions is that $E(F)[\mathrm{tors}] \supseteq E[n]$; if $E(F)[\mathrm{tors}] = E[n]$, then it follows that $E(F)[\mathrm{tors}]/nE(F)[\mathrm{tors}] = E[n]$. Therefore, since $\mathrm{rank}_{\mathbb{Z}/n\mathbb{Z}} E[n] = 2$, if we find that $\mathrm{rank}_{\mathbb{Z}/n\mathbb{Z}}(E(F)/nE(F)) = s$, then it follows that $r = s - 2$, so that we have $E(F) \cong \mathbb{Z}^{s-2} \times E[n]$.

For the remainder of this section, we focus on the case where $n = 2$; since we are assuming that $E[n] \subseteq E(F)$, this is the case with the most mild assumption. There exists an equation for E of the form

$$E : y^2 = (x - e_1)(x - e_2)(x - e_3),$$

where each $e_i \in F$; note that $E[2] = \{O, (e_1, 0), (e_2, 0), (e_3, 0)\}$. We can choose any two nonzero elements of $E[2]$, and they will be a basis for $E[2]$, so let us set each $T_i := (e_i, 0)$.

We next compute f_{T_1} and f_{T_2}, since they can be used to compute the image of b. Observe that for each $1 \leq i \leq 3$, for the function $f_{T_i} := x - e_i \in F(E)$, we have

$$\operatorname{div}(f_{T_i}) = 2(T_i) - 2(O)$$

(see Example 2.3.1 and Notes Exercise 2.3.4 from Section 2.3). We can also check that

$$f_{T_i} \circ [2] = \left(\frac{x^2 - 2e_i x - 2e_i^2 + 2(e_1 + e_2 + e_3) \cdot e_i - (e_1 e_2 + e_1 e_3 + e_2 e_3)}{2y} \right)^2,$$

using e.g. the duplication formula. Thus, taking g_{T_i} to be the inner function on the right hand side, we have $f_{T_i} \circ [2] = g_{T_i}^2$, and as can be checked, $\operatorname{div}(g_{T_i}) = [2]^*((T_i) - (O))$. Thus, we can take $f_{T_1} := x - e_1$ and $f_{T_2} := x - e_2$.

Therefore, our problem of determining $E(F)/2E(F)$ reduces (in part) to the following: for each $(b_1, b_2) \in F(S, 2) \times F(S, 2)$, we must find all points $(x, y, z_1, z_2) \in F \times F \times F^\times \times F^\times$ such that

$$y^2 = (x - e_1)(x - e_2)(x - e_3),$$

$$b_1 z_1^2 = x - e_1 \qquad \text{and} \qquad b_2 z_2^2 = x - e_2.$$

(This will work if $P = (x, y) \neq T_1, T_2$ – we'll deal with the excluded cases in a moment.) We can transform this into just two equations. Let us define a new variable z_3 via $y := b_1 b_2 z_1 z_2 z_3$ (note that $b_1 b_2 z_1 z_2 \neq 0$). Substituting this into the elliptic curve equation and then canceling terms with the latter two equations, we get the three equations

$$b_1 b_2 z_3^2 = x - e_3,$$

$$b_1 z_1^2 = x - e_1 \qquad \text{and} \qquad b_2 z_2^2 = x - e_2.$$

Then substituting x out gives just two equations

$$b_1 z_1^2 - b_2 z_2^2 = e_2 - e_1 \qquad \text{and} \qquad b_1 z_1^2 - b_1 b_2 z_3^2 = e_3 - e_1. \tag{23}$$

This defines a curve in $\mathbb{P}^3$, where $(z_1, z_2, z_3) = [z_1 : z_2 : z_3 : 1]$. To summarize, for each pair $(b_1, b_2) \in F(S, 2) \times F(S, 2)$, we are looking for solutions $(z_1, z_2, z_3) \in F^\times \times F^\times \times F^\times$ to (23). If we find such a solution, then we can recover a corresponding point $\overline{P} \in E(F)/2E(F)$ by taking $P := (x, y) = (b_1 z_1^2 + e_1, b_1 b_2 z_1 z_2 z_3)$.

Note that the above technique implicitly assumes that we have $b(\overline{P}, T_i) = f_{T_i}(P) \bmod (F^\times)^2$; however, this is not true if our solution P satisfies $\overline{P} \in \{\overline{O}, \overline{T}\}$. In particular, it cannot be used to compute $b(\overline{T_1}, T_1)$ and $b(\overline{T_2}, T_2)$ (which is important to know if we are analyzing values of b). However, these values can be computed with bilinearity

of b: for example, we compute that

$$\begin{aligned} b(\overline{T_1}, T_1) &= b(\overline{T_1}, T_1 + T_2) \cdot b(\overline{T_1}, -T_2) \\ &= b(\overline{T_1}, T_1 + T_2) \cdot b(\overline{T_1}, T_2)^{-1} \\ &= b(\overline{T_1}, T_3) \cdot b(\overline{T_1}, T_2)^{-1} \\ &= f_{T_3}(T_1) \cdot f_{T_2}(T_1)^{-1} \mod (F^\times)^2 \\ &= \frac{(x-e_3)(T_1)}{((x-e_2)(T_1))^{-1}} \mod (F^\times)^2 \\ &= \frac{e_1 - e_3}{e_1 - e_2} \mod (F^\times)^2. \end{aligned}$$

Similarly, we can show that

$$b(\overline{T_2}, T_2) = \frac{e_2 - e_3}{e_2 - e_1} \mod (F^\times)^2.$$

This procedure is described as **complete 2-descent.**

Theorem 10.1.2 (Complete 2-descent)**.** *Let $E_{/F}$ be an elliptic curve with equation*

$$E : y^2 = (x - e_1)(x - e_2)(x - e_3)$$

where $e_1, e_2, e_3 \in F$; thus, $E[2] \subseteq E(F)$. Let us set

$$S := \{\mathfrak{P} \in \Sigma_F^{\mathrm{NA}} : E \text{ has bad reduction at } \mathfrak{P}\} \cup \{\mathfrak{P} \in \Sigma_F^{\mathrm{NA}} : \mathfrak{P} \mid 2\} \cup \Sigma_F^{\mathrm{Arch}},$$

as well as

$$F(S,2) := \{a \in F^\times/(F^\times)^2 : \forall \mathfrak{P} \in \Sigma_F \smallsetminus S, v_{\mathfrak{P}}(a) \equiv 0 \pmod 2\}.$$

Then there exists an injective homomorphism

$$E(F)/2E(F) \hookrightarrow F(S,2) \times F(S,2)$$

defined by

$$\overline{P} := \overline{(x,y)} \mapsto \begin{cases} (x - e_1, x - e_2) & \text{if } x \neq e_1, e_2 \\ \left(\frac{e_1 - e_3}{e_2 - e_3}, e_1 - e_2\right) & \text{if } x = e_1, \\ \left(e_2 - e_1, \frac{e_2 - e_3}{e_2 - e_1}\right) & \text{if } x = e_2, \\ (1,1) & \text{if } x = \infty, \text{ i.e., if } P = O. \end{cases}$$

Let $(b_1, b_2) \in F(S,2) \times F(S,2)$ be a pair that is not the image of the points $O, (e_1, 0), (e_2, 0)$ under this map. Then (b_1, b_2) is the image of an element $\overline{P} = \overline{(x,y)} \in E(F)/2E(F)$ if and only if the equations

$$b_1 z_1^2 - b_1 b_2 z_3^2 = e_3 - e_1 \qquad \text{and} \qquad b_1 z_1^2 - b_2 z_2^2 = e_2 - e_1 \tag{24}$$

have a solution $(z_1, z_2, z_3) \in F^\times \times F^\times \times F^\times$. If such a solution exists, then we can take

$$P := (x,y) := (b_1 z_1^2 + e_1, b_1 b_2 z_1 z_2 z_3).$$

Remark 10.1.4. The above theorem reduces the computation of $E(F)/2E(F)$ to a matter of checking for rational solutions to the equations in (24). This can be done with any techniques at our disposal, such as a v-adic point check (with v Archimedean or otherwise), or a computer calculation. We emphasize that once we have computed $E(F)/2E(F)$, we can then effectively compute $E(F)$ using [Sil09, Exercise 8.18]. However, even without this exercise, we can often compute the structure of $E(F)$; see Remark 10.1.3.

Example 10.1.1. Here is an example of using complete 2-descent to compute the structure of the Mordell-Weil group of a rational elliptic curve. Let us consider the curve

$$E : y^2 = x^3 - 12x^2 + 20x = x(x-2)(x-10).$$

We calculate its discriminant as $\Delta = 409600 = 2^{14} \cdot 5^2$.

We know that $E[2] \subseteq E(\mathbb{Q})$. We claim this is the entire torsion group, i.e., $E(\mathbb{Q})[\text{tors}] = E[2]$. To prove this, we cite Theorem 7.3.4: since E has good reduction at 3, we have that $E(\mathbb{Q})[\text{tors}] \hookrightarrow \tilde{E}(\mathbb{F}_3)$. However, it is easy to check that $\#\tilde{E}(\mathbb{F}_3) = 4$; we conclude that $E(\mathbb{Q})[\text{tors}] = E[2]$. In particular, by Remark 10.1.3, if we can compute $\#E(\mathbb{Q})/2E(\mathbb{Q})$, then we know the structure of $E(\mathbb{Q})$ as a finitely generated abelian group.

Let us work towards determining $E(\mathbb{Q})/2E(\mathbb{Q})$ explicitly with complete 2-descent. Our associated set S is

$$\begin{aligned} S &= \{p \in \mathbb{Z}^+ : E \text{ has bad reduction at } p\} \cup \{p \in \mathbb{Z}^+ : p \mid 2\} \cup \{\infty\} \\ &= \{2, 5, \infty\}; \end{aligned}$$

here, ∞ denotes the usual absolute value on $\mathbb{Q}$. In particular, we have

$$\mathbb{Q}(S,2) := \{\alpha \in \mathbb{Q}^\times/(\mathbb{Q}^\times)^2 : \forall p \notin \{2,5,\infty\}, v_p(\alpha) \equiv 0 \pmod 2\}.$$

Any element of $\mathbb{Q}(S,2)$ has a squarefree representative; thus, we see that

$$\mathbb{Q}(S,2) = \{\pm\overline{1}, \pm\overline{2}, \pm\overline{5}, \pm\overline{10}\}.$$

Let us set $e_1 := 0, e_2 := 2$ and $e_3 := 10$. By complete 2-descent, we know that $\overline{O}, \overline{(0,0)}, \overline{(2,0)}$ and $\overline{(10,0)}$ in $E(\mathbb{Q})/2E(\mathbb{Q})$ map to $(1,1), (5,-2), (2,-4) \equiv (2,-1)$ and $(10,8) \equiv (10,2)$ in the image of b, respectively. It thus remains to determine which of the remaining pairs $(b_1, b_2) \in \mathbb{Q}(S,2) \times \mathbb{Q}(S,2)$ come from elements of $E(\mathbb{Q})/2E(\mathbb{Q})$ under the 2-descent embedding. Since $\#\mathbb{Q}(S,2) = 8$, there are 64 pairs in $\mathbb{Q}(S,2) \times \mathbb{Q}(S,2)$. By (24), the pairs which come from elements of $E(\mathbb{Q})/2E(\mathbb{Q})$ will correspond to solutions $(z_1, z_2, z_3) \in \mathbb{Q}^\times \times \mathbb{Q}^\times \times \mathbb{Q}^\times$ to the system of equations

$$b_1 z_1^2 - b_2 z_2^2 = 2 \qquad \text{and} \qquad b_1 z_1^2 - b_1 b_2 z_3^2 = 10. \tag{25}$$

Once we have found such a solution for the pair (b_1, b_2), we get a corresponding element $\overline{P} \in E(\mathbb{Q})/2E(\mathbb{Q})$ given by $P := (b_1 z_1^2, b_1 b_2 z_1 z_2 z_3)$.

We will perform several techniques to determine the image of b and the corresponding points from $E(\mathbb{Q})/2E(\mathbb{Q})$; this is recorded in Figure 10.1.1. In this figure, we enumerate each box with a circled number, which will correspond to a technique below that we applied to analyze the pair(s) in that box.

Before we begin our analysis, we note that not all pairs (b_1, b_2) need to be checked with a particular technique: this is because b induces a *homomorphism* $E(\mathbb{Q})/2E(\mathbb{Q}) \hookrightarrow \mathbb{Q}(S,2)\times\mathbb{Q}(S,2)$. For example, if (b_1, b_2) and (b_1', b_2') both come from $E(\mathbb{Q})/2E(\mathbb{Q})$, then so does their product (b_1b_1', b_2b_2'). On the other hand, if (b_1, b_2) comes from $E(\mathbb{Q})/2E(\mathbb{Q})$ and (b_1', b_2') does *not,* then (b_1b_1', b_2b_2') does not.

(1) ($\mathbb{R}$-adic): if $b_1 < 0$ and $b_2 > 0$, then the first equation in (25) has no real solutions. This eliminates 16 possible pairs (b_1, b_2).

(2) ($\mathbb{R}$-adic): if $b_1 < 0$ and $b_2 < 0$, then the second equation in (25) has no real solutions. This eliminates 16 more possible pairs (b_1, b_2).

(3) As noted earlier, the four 2-torsion point elements $\overline{O}, \overline{(0,0)}, \overline{(2,0)}$ and $\overline{(10,0)}$ map under b to the pairs $(1,1), (5,-2), (2,-4) \equiv (2,-1)$ and $(10,8) \equiv (10,2)$, respectively. (See Theorem 10.1.2 for the map to $\mathbb{Q}(S,2) \times \mathbb{Q}(S,2)$.)

(4) Let us try $(b_1, b_2) := (1,-1)$: our equations in (25) become

$$z_1^2 + z_2^2 = 2 \qquad \text{and} \qquad z_1^2 + z_3^2 = 10.$$

By inspection, these have the solutions $(z_1, z_2, z_3) = (\pm 1, \pm 1, \pm 3)$. All of these solutions will induce the same element of $E(\mathbb{Q})/2E(\mathbb{Q})$, so we will simply choose $(1,1,3)$ and get the point $P = (x,y) = (b_1z_1^2, b_1b_2z_1z_2z_3) = (1,-3) \in E(\mathbb{Q})$.

(5) We can multiply $(b_1, b_2) := (1,-1)$ from (4) with the pair representatives for the 2-torsion points from (3); this corresponds to adding $(1,-3)$ with the 2-torsion points modulo $2E(\mathbb{Q})$. This gives new pairs $(b_1, b_2) = (5,2), (2,1)$ and $(10,-2)$ in $\mathbb{Q}(S,2)\times\mathbb{Q}(S,2)$, which correspond to the points $(20,60), (18,-48), \left(\frac{10}{9}, \frac{80}{27}\right) \in E(\mathbb{Q})$.

(6) (5-adic): fix a pair $(b_1, b_2) \in \mathbb{Q}(S,2) \times \mathbb{Q}(S,2)$ where $b_1 \not\equiv 0 \pmod 5$ and $5 \mid b_2$; these pairs are $(b_1, b_2) = (\pm 1, \pm 5), (\pm 1, \pm 10), (\pm 2, \pm 5)$ and $(\pm 2, \pm 10)$. We will show that no solution $(z_1, z_2, z_3) \in \mathbb{Q}^\times \times \mathbb{Q}^\times \times \mathbb{Q}^\times$ exists to (25) for such (b_1, b_2).

For the sake of contradiction, suppose we have such a solution. Then by computing the 5-adic valuations of the first equation, one can show that $v_5(z_1), v_5(z_2) \geq 0$ (check it, noting the domination principle, see Notes Exercise 2.1.1). From this, the second equation implies that $v_5(z_1) > 0$; however, this implies in the first equation that $v_5(2) > 0$, which is absurd. We conclude that no solutions exist for such (b_1, b_2). This implies 8 new non-solution pairs.

(7) (5-adic): if we multiply the non-solution pair from (6) with e.g. the solution pair $(b_1, b_2) = (5,2)$ from (5), then we get 8 new non-solution pairs.

(8) (5-adic): let us try $(b_1, b_2) := (1,2)$. Then (25) becomes

$$z_1^2 - 2z_2^2 = 2 \qquad \text{and} \qquad z_1^2 - 2z_3^2 = 10.$$

Suppose that such a solution $(z_1, z_2, z_3) \in \mathbb{Q}^\times \times \mathbb{Q}^\times \times \mathbb{Q}^\times$ exists; clearing denominators, we may assume instead that z_1, z_2 and z_3 are *integers* which satisfy

$$z_1^2 - 2z_2^2 = 2k \qquad \text{and} \qquad z_1^2 - 2z_3^2 = 10m$$

for some nonzero $k, m \in \mathbb{Z}$. The latter equation implies $z_1 \equiv 2z_3^2 \pmod 5$; since 2 is not a square modulo 5, this forces $z_3 \equiv 0 \pmod 5$, and thus $5 \mid z_1$. However,

this implies from the first equation that $1 \equiv 0 \pmod 2$, which is absurd. We conclude that (b_1, b_2) is a non-solution pair.

(9) (5-adic): taking the non-solution pair $(b_1, b_2) := (1, 2)$ from (8) and multiplying it with the 8 solution pairs from the previous parts gives 7 new non-solution pairs, which fills up the rest of the table.

<table>
<tr><td>b_1
b_2</td><td>1</td><td>2</td><td>5</td><td>10</td><td>-1</td><td>-2</td><td>-5</td><td>-10</td></tr>
<tr><td>1</td><td>0</td><td>$(18, -48)$ ⑤</td><td colspan="2">$\mathbb{Q}_5$ ⑨</td><td colspan="4" rowspan="3">$\mathbb{R}$ ①</td></tr>
<tr><td>2</td><td>$\mathbb{Q}_5$ ⑧</td><td>$\mathbb{Q}_5$ ⑨</td><td>$(20, 60)$ ⑤</td><td>$(10, 0)$ ③</td></tr>
<tr><td>5
10</td><td colspan="2">$\mathbb{Q}_5$ ⑥</td><td colspan="2">$\mathbb{Q}_5$ ⑦</td></tr>
<tr><td>-1</td><td>$(1, -3)$ ④</td><td>$(2, 0)$ ③</td><td colspan="2">$\mathbb{Q}_5$ ⑨</td><td colspan="4" rowspan="3">$\mathbb{R}$ ②</td></tr>
<tr><td>-2</td><td colspan="2">$\mathbb{Q}_5$ ⑨</td><td>$(0, 0)$ ③</td><td>$\left(\frac{10}{9}, -\frac{80}{27}\right)$ ⑤</td></tr>
<tr><td>-5
-10</td><td colspan="2">$\mathbb{Q}_5$ ⑥</td><td colspan="2">$\mathbb{Q}_5$ ⑦</td></tr>
</table>

FIGURE 10.1.1. Table of pairs $(b_1, b_2) \in \mathbb{Q}(S, 2) \times \mathbb{Q}(S, 2)$, and their corresponding point representatives from $E(\mathbb{Q})/2E(\mathbb{Q})$, if they exist [Sil09].

Tallying up the number of solution pairs in the chart shows that $\#E(\mathbb{Q})/2E(\mathbb{Q}) = 8$; since $E(\mathbb{Q})[\text{tors}] = E[2]$, we conclude that

$$E(\mathbb{Q}) \cong \mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}.$$

Given that we have explicitly computed the distinct elements of $E(\mathbb{Q})/2E(\mathbb{Q})$, we can also use [Sil09, Exercise 8.18] to effectively compute $E(\mathbb{Q})$, if desired.

Remark 10.1.5. Let us remark that, as illustrated in this example, we can translate the problem of determining elements of $E(F)/nE(F)$, to the problem of determining the existence of rational solutions to a finite set of systems of equations, each of which defines a curve. One issue that can arise with this procedure is that one of these curves can have a point over every v-adic completion of F, and yet no F-rational points. This possible failure of the *Hasse principle* is what makes the Mordell-Weil theorem ineffective. We will discuss this more in Section 10.4.

10.2. **Twisting–general theory.** Most of the rest of these notes on Chapter 10 were written after the class ended. They will often omit proofs from [Sil09]. To better analyze the homogeneous spaces which appear when we compute the Mordell-Weil group of an elliptic curve over a number field, we develop the theory of twists of curves, which allows an alternative description of these spaces. For this section and the next, we let k denote a perfect field.

Definition 10.2.1. Let $C_{/k}$ be a smooth projective curve. Then the **isomorphism group of** C**,** written as $\mathrm{Aut}_{\mathrm{Mor}}(C)$ (or $\mathrm{Isom}(C)$ in [Sil09]), is the group of $\overline{k}$-isomorphisms from C to itself. We write the product of elements in $\mathrm{Aut}_{\mathrm{Mor}}(C)$ as $\phi\psi$ instead of $\phi \circ \psi$.

Definition 10.2.2. A **twist** of $C_{/k}$ is a smooth curve $C'_{/k}$ that is $\overline{k}$-isomorphic to C. Say two twists are *equivalent* if they are k-isomorphic. The set of Twists of C modulo k-isomorphism is denoted $\mathrm{Twists}(C, k)$.

Since a twist $C'_{/k}$ of a curve $C_{/k}$ implicitly has an isomorphism $\phi\colon C' \xrightarrow{\sim} C$, we often write $(C', \phi) \in \mathrm{Twists}(C)$. For each such twist, we have an associated map $\xi\colon G_k \to \mathrm{Aut}_{\mathrm{Mor}}(C)$ defined as follows: for $\sigma \in G_k$, we set

$$\xi_\sigma := \phi^\sigma \phi^{-1}.$$

In a sense, this map measures the failure of ϕ to be k-rational (and thus the failure of C' to be k-isomorphic to C).

Remark 10.2.1. Intuitively, the 1-cocyle ξ from a twist (C', ϕ) transforms field automorphisms $\sigma \in G_k$ into curve automorphisms of C in the following way. Given a point $P \in C$, we have $\phi^{-1}(P) \in C'$. Then we send it back to C *under* ϕ^σ*,* which is not necessarily ϕ unless σ fixes ϕ. A key point to remember is the definition of ϕ^σ: for example, if we write ϕ with coordinate functions as $\phi = [f_0 : f_1 : f_2]$, then $\phi^\sigma(Q) := [f_0^\sigma(Q) : f_1^\sigma(Q) : f_2^\sigma(Q)]$, where f^σ is σ applied to the coefficients of f (see §1.3 of [Sil09]). On the other hand, we have $(\phi(Q))^\sigma = \phi^\sigma(Q^\sigma)$, which can be different from $\phi^\sigma(Q)$ unless $Q \in C(k)$.

Theorem 10.2.1. [Sil09, Theorem X.2.2] *Let $C_{/k}$ be a smooth projective curve. For each twist $(C', \phi) \in \mathrm{Twists}(C, k)$, define a map $\xi_\sigma := \phi^\sigma \phi^{-1} \in \mathrm{Aut}_{\mathrm{Mor}}(C)$ as above.*

a. The map ξ is a 1-cocyle, i.e.,

$$\xi_{\sigma\tau} = \xi_\sigma^\tau \xi_\tau \qquad \text{for all } \sigma, \tau \in G_k.$$

The associated cohomology class in $H^1(G_k, \mathrm{Aut}_{\mathrm{Mor}}(C))$ is denoted by $\{\xi\}$.

b. The cohomology class $\{\xi\}$ is determined by the k-isomorphism class of C', and in particular is independent of the choice of ϕ. We thus obtain a natural map

$$\mathrm{Twists}(C, k) \to H^1(G_k, \mathrm{Aut}_{\mathrm{Mor}}(C)).$$

c. The map in part b. is a bijection. *In other words, the twists of $C_{/k}$, up to k-isomorphism, are in 1-1 correspondence with elements of the cohomology set $H^1(G_k, \mathrm{Aut}_{\mathrm{Mor}}(C))$.*

Remark 10.2.2. The construction given to prove surjectivity of the map $\mathrm{Twists}(C, k) \to H^1(G_k, \mathrm{Aut}_{\mathrm{Mor}}(C))$ in the theorem above is worth detailing out. Given a 1-cocyle $\varphi \in H^1(G_k, \mathrm{Aut}_{\mathrm{Mor}}(C))$, how can we construct a twist $(C'_{/k}, \phi)$ of C such that its associated 1-cocyle $\xi_\sigma := \phi^\sigma \phi^{-1}$ is equal to φ_σ?

Given the function field $\overline{k}(C)$ of C, we define a φ*-twisted* action of G_k on $\overline{k}(C)$ as follows. To clarify which action we are considering in any given situation, we let L

denote an abstract field isomorphic to $\overline{k}(C)$, say by (k-isomorphism) $Z\colon \overline{k}(C) \xrightarrow{\sim} L$. We define a twisted G_k-action on L as follows: for $g = Z(f) \in L$, we set

$$g^\sigma = Z(f)^\sigma := Z(f^\sigma \varphi_\sigma).$$

(Recall that φ_σ is in $\mathrm{Aut}_{\mathrm{Mor}}(C)$, and that f and f^σ can be regarded as morphisms $C \to \mathbb{P}^1$, so that this composition makes sense.) This is a group action since φ is a 1-cocyle:

$$\begin{aligned} Z(f)^{\sigma\tau} :&= Z(f^{\sigma\tau}\varphi_{\sigma\tau}) \\ &= Z(f^{\sigma\tau}\varphi_\sigma^\tau \varphi_\tau) \\ &= Z((f^\sigma \varphi_\sigma)^\tau \varphi_\tau) \\ &= (Z(f)^\sigma)^\tau. \end{aligned}$$

Of course, we also have $Z(f)^{1_{\overline{k}}} = Z(f)$.

Let $\ell \subseteq L$ denote the subfield fixed by this twisted action: i.e.,

$$\begin{aligned} \ell :&= \{Z(f) \in L : \forall \sigma \in G_k, Z(f^\sigma \varphi_\sigma) = Z(f)\} \\ &= \{Z(f) \in L : \forall \sigma \in G_k, f^\sigma \varphi_\sigma = f\}. \end{aligned}$$

This fixed field will be the function field which corresponds to the desired twist $(C', \phi) \in \mathrm{Twists}(C)$ such that $\phi^\sigma \phi^{-1} = \varphi_\sigma$.

The first observation we make about ℓ is that $\ell \cap \overline{k} = k$ (keyword: defined over k). To see this, let $b = Z(a) \in \ell \cap \overline{k}$. From $b \in \ell$, for all $\sigma \in G_k$ we have $a^\sigma \varphi_\sigma = a$. However, since $a \in \overline{k}$, we know that a is constant, and thus $a^\sigma = a$; it follows that $a \in k$, and thus $b = Z(a) \in k$. We conclude that $\ell \cap \overline{k} = k$. The second observation is that $\overline{k}\ell = L$ (keyword: transcendence degree one). This follows from [Sil09, Lemma II.5.8.1], with respect to the twisted action on L.

By the correspondence between function fields of transcendence degree one and curves (more specifically, [Sil09, Theorem II.2.4.c]), the first observation implies there exists a smooth curve $C'_{/k}$, unique up to k-isomorphism, with $k(C') = \ell$; thus, $\overline{k}(C')$ admits this twisted action. We then check via the second observation that we have an isomorphism

$$Z\colon \overline{k}(C) \xrightarrow{\sim} L = \overline{k}\ell = \overline{k}(C').$$

Thus by [Sil09, Theorem II.2.4.b] and [Sil09, Corollary II.2.4.1], there exists a unique $\overline{k}$-isomorphism $\phi\colon C' \to C$ such that its pullback is given by Z:

$$\phi^* = Z\colon \overline{k}(C) \xrightarrow{\sim} \overline{k}(C').$$

We claim that for all $\sigma \in G_k$, one has $\phi^\sigma \phi^{-1} = \varphi_\sigma$. To see this, first note that from $\phi^* = Z$, the twisted action $Z(f)^\sigma := Z(f^\sigma \varphi_\sigma)$ can be rewritten as follows: for all $f \in \overline{k}(C)$ and $\sigma \in G_k$, one has

$$(\phi^*(f))^\sigma = \phi^*(f^\sigma \varphi_\sigma),$$

i.e.,

$$(f\phi)^\sigma = f^\sigma \varphi_\sigma \phi,$$

i.e.,

$$f^\sigma \phi^\sigma = f^\sigma \varphi_\sigma \phi.$$

Fixing $\sigma \in G_k$, the above is true for all $f \in \overline{k}(C)$, which forces equality of the inner terms, i.e.,

$$\phi^\sigma = \varphi_\sigma \phi,$$

i.e.,

$$\phi^\sigma \phi^{-1} = \varphi_\sigma.$$

We conclude that $\xi_\sigma = \phi^\sigma \phi^{-1}$, which shows that the map $\mathrm{Twists}(C,k) \to H^1(G_k, \mathrm{Aut}_{\mathrm{Mor}}(C))$ is surjective.

Example 10.2.1. [Sil09, Example X.2.4] Here is an important example, in which we compute the *quadratic twist* of an elliptic curve in Weierstrass form. Assume that $\mathrm{char}(k) \neq 2$; fix a number $d \in k \smallsetminus k^2$, and let

$$\chi := \chi^d \colon G_k \to \{\pm 1\}$$

be the quadratic character associated to $\sqrt{d}$. In particular, for $\sigma \in G_k$ we have

$$\chi(\sigma) = \frac{\sigma(\sqrt{d})}{\sqrt{d}}.$$

For an elliptic curve $E_{/k}$, we always have a 1-cocyle associated to χ, given by

$$\xi \colon G_k \to \mathrm{Aut}_{\mathrm{Mor}}(E), \qquad \xi_\sigma := [\chi(\sigma)],$$

where $[n]$ denotes multiplication-by-n. By the previous theorem, there exists a twist $(C_{/k}, \phi)$ of E which satisfies $\phi^\sigma \phi^{-1} = [\chi(\sigma)]$.

In our construction of the twist (C, ϕ) in Remark 10.2.2, we defined a twisted action on $\overline{k}(E)$ with ξ, and then computed the fixed subfield ℓ of $\overline{k}(E)$ under this twisted action. By abuse of notation, we will write $Z := \mathrm{id} \colon \overline{k}(E) \xrightarrow{\sim} \overline{k}(E)$ for our k-isomorphism, and the twisted action as

$$f^{\sigma,t} := f^\sigma \chi(\sigma) = [\chi(\sigma)]^*(f^\sigma).$$

Giving E a Weierstrass equation makes this more explicit. Let us assume that E is given in the form

$$E : y^2 = f(x).$$

We then have $\overline{k}(E) = \overline{k}(x,y)$ (see §3.3 of [Sil09]), and every element $f \in \overline{k}(E)$ can be expressed as a rational function in the Weierstrass coordinates x, y. It follows that each $f(x,y) \in \overline{k}(E)$ satisfies

$$(f(x,y))^{\sigma,t} = f^\sigma(x^{\sigma,t}, y^{\sigma,t}) = f^\sigma(x, \chi(\sigma) y)$$

(recall that $[-1](x,y) = (x,-y)$). We can check that $\left(\frac{y}{\sqrt{d}}\right)^{\sigma,t} = \frac{y}{\sqrt{d}}$. It follows that the functions $x' := x$ and $y' := \frac{y}{\sqrt{d}}$ lie in ℓ, which forces $\ell = k(x', y')$ (both fields have equal transcendence degree over k and equal field of constants). Furthermore, we observe the relation

$$dy'^2 = f(x'),$$

which defines an elliptic curve over k. We deduce that our twist $C' =: E'$ is an elliptic curve; our $\overline{k}$-isomorphism $\phi \colon E' \xrightarrow{\sim} E$ is then determined by $\phi^* = Z$. It suffices to take

$$\phi(x', y') := (x, \sqrt{d} y)$$

(so we take $Z(x) := x, Z(y) := \sqrt{d}y$ at the start). The inverse $\phi^{-1}\colon E \xrightarrow{\sim} E'$ is

$$\phi^{-1}(x, y) := \left(x, \frac{y}{\sqrt{d}}\right).$$

We can double-check directly that for all $\sigma \in G_k$, we have

$$\phi^\sigma \phi^{-1} = [\chi(\sigma)] :$$

this follows from $\phi(x', y') := (x, \sqrt{d}y) \Rightarrow \phi^\sigma(x', y') := (x, \sigma(\sqrt{d})y) = (x, \chi(\sigma)\sqrt{d}y)$.

The curve E' above is called the *quadratic twist of* E (by d or χ). These are the canonical examples of an elliptic curve twist: when $j(E) \neq 0, 1728$, any twist of E must be a quadratic twist.

10.3. **Homogeneous spaces.** In this section, we study the auxiliary spaces which came up in analyzing $E(F)$ for an elliptic curve $E_{/F}$ via 2-descent, which we called *homogeneous spaces.* These systems of two equations end up each defining particular twists of E. Recall in Theorem 10.2.1 ([Sil09, Theorem X.2.2]) that for a curve $C_{/k}$, we have a bijection

$$\mathrm{Twists}(C, k) \to H^1(G_k, \mathrm{Aut}_{\mathrm{Mor}}(C)),$$

where for a twist $\phi\colon C' \to C$, we have the 1-cocycle

$$(C'_{/k}, \phi) \mapsto (\sigma \mapsto \phi^\sigma \phi^{-1}).$$

With this identification, we will see that homogeneous spaces are the twists whose associated 1-cocycle's values are translation automorphisms. We will then wrap this section up with an important example of computing homogeneous spaces for an elliptic curve with a rational order two point, which will be important for describing descent via 2-isogeny.

Definition 10.3.1. Let $E_{/k}$ be an elliptic curve. Then a **(principal) homogeneous space for** $E_{/k}$ is a smooth curve $C_{/k}$ with a k-rational, simply transitive algebraic group action of E on C. Thus, a homogeneous space for E is a pair $(C_{/k}, \mu)$, where $C_{/k}$ is a smooth curve and

$$\mu\colon C \times E \to C$$

is a k-morphism of varieties with the following three properties:

a. $\mu(p, O) = p$ for all $p \in C$.
b. $\mu(\mu(p, P), Q) = \mu(p, P + Q)$ for all $p \in C$ and $P, Q \in E$.
c. For all $p, q \in C$, there exists unique $P \in E$ with $\mu(p, P) = q$.

We often write $p + P$ instead of $\mu(p, P)$, and if $\mu(p, P) = q$, then we write $q - p := P$. Then these properties are:

a. $p + P$ for all $p \in C$.
b. $(p + P) + Q = p + (P + Q)$ for all $p \in C$ and $P, Q \in E$.
c. For all $p, q \in C$, there exists unique $P \in E$ with $q - p = P$.

Principal homogeneous spaces for $E_{/k}$ are also called **k-torsors under E.**

Based on the above, we have an analogous "subtraction map" on C, written as

$$\nu\colon C \times C \to E$$

via

$$\nu(q,p) := q - p := (\text{the unique } P \in E \text{ satisfying } \mu(p,P) = q).$$

As it turns out, subtraction on C is a k-morphism, and using $+$ and $-$ signs for these maps provides the right intuition.

Lemma 10.3.1. [Sil09, Lemma X.3.1] *Let $C_{/k}$ be a homogeneous space for $E_{/k}$. Then for all $p, q \in C$ and all $P, Q \in E$:*

a. $\mu(p, O) = p$ *and* $v(p,p) = O$.
b. $\mu(p, \nu(q,p)) = q$ *and* $\nu(\mu(p,P),p) = P$.
c. $\nu(\mu(q,Q), \mu(p,P)) = \nu(q,p) + Q - P$.

Written with $+$ and $-$ instead, these become:

a. $p + O = p$ *and* $p - p = O$.
b. $p + (q - p) = q$ *and* $(p + P) - p = P$.
c. $(q + Q) - (p + P) = (q - p) + Q - P$.

The next lemma shows that a homogeneous space of $E_{/k}$ is a twist of E, and further describes subtraction on C in terms of a $\overline{k}$-isomorphism $E \xrightarrow{\sim} C$.

Proposition 10.3.2. [Sil09, Proposition X.3.2] *Let $E_{/k}$ be an elliptic curve and $C_{/k}$ a homogeneous space for $E_{/k}$. Fix a point $p_0 \in C$, and define a map*

$$\theta\colon E \to C, \qquad \phi(P) := p_0 + P.$$

a. The map θ is a $k(p_0)$-isomorphism. In particular, the curve C is a twist of E.
b. For all $p \in C$ and all $P \in E$,

$$p + P = \theta(\theta^{-1}(p) + P)$$

(the first $+$ is the action of E on C, and the second $+$ is addition on E.)
c. For all $p, q \in C$,

$$q - p = \theta^{-1}(q) - \theta^{-1}(p).$$

d. The subtraction map

$$\nu\colon C \times C \to E, \qquad \nu(q,p) := q - p$$

is a k-morphism.

Definition 10.3.2. Two homogeneous spaces $C_{/k}$ and $C'_{/k}$ for $E_{/k}$ are **equivalent** if there exists a k-isomorphism $\theta\colon C \xrightarrow{\sim} C'$ compatible with the action on E on C and C', i.e.,

$$\theta(p + P) = \theta(p) + P.$$

The equivalence class of the homogeneous space $E_{/k}$ acting on itself by translation is called the *trivial class.* The set of equivalence classes of homogeneous spaces for $E_{/k}$ is called the **Weil-Châtelet group for** $E_{/k}$, and is denoted by $\mathrm{WC}(E,k)$. Since homogeneous spaces for E are twists for E, we have a map $\mathrm{WC}(E,k) \to \mathrm{Twists}(E,k)$.

Proposition 10.3.3. [Sil09, Proposition X.3.3] *Let $C_{/k}$ be a homogeneous space for $E_{/k}$. Then $C_{/k}$ is trivial in $\mathrm{WC}(E,k)$ if and only if $C(k) \neq \emptyset$.*

Theorem 10.3.4. [Sil09, Theorem X.3.6] *Let $E_{/k}$ be an elliptic curve. Then there is a bijection*

$$\mathrm{WC}(E,k) \to H^1(G_k, E(\overline{k}))$$

as follows. Let $C_{/k}$ be a homogeneous space for $E_{/k}$ and choose any point $p_0 \in C$. Then the map

$$\sigma \mapsto p_0^\sigma - p_0$$

induces a 1-cocyle in $H^1(G_k, E(\overline{k}))$.

From the theorem above, we now have a group structure on $\mathrm{WC}(E,k)$ given by the group structure on $H^1(G_k, E(\overline{k}))$. It is worth proving surjectivity here, since this will allow us to construct homogeneous spaces from elements of $H^1(G_k, E(\overline{k}))$ – not unlike constructing twists from elements of $H^1(G_k, \mathrm{Aut}_{\mathrm{Mor}}(C))$.

Remark 10.3.1. To show that the map $\mathrm{WC}(E,k) \to H^1(G_k, E(\overline{k}))$ above is surjective, we utilize surjectivity of the map $\mathrm{Twists}(C,k) \to H^1(G_k, \mathrm{Aut}_{\mathrm{Mor}}(C))$ from [Sil09, Theorem X.2.2], which we explained in Remark 10.2.2. Let $\xi \in H^1(G_k, E(\overline{k}))$ be a 1-cocyle. Then ξ induces an element $\widetilde{\xi} \in H^1(G_k, \mathrm{Aut}_{\mathrm{Mor}}(E))$ via $\widetilde{\xi}_\sigma := \tau_{\xi_\sigma}$, where $\tau_R \in \mathrm{Aut}_{\mathrm{Mor}}(E)$ is translation by R. We double-check that $\widetilde{\xi}$ is a 1-cocyle:

$$\begin{aligned}
\widetilde{\xi}_{\sigma\eta} &:= \tau_{\xi_{\sigma\eta}} \\
&= \tau_{\xi_\sigma^\eta + \xi_\eta} \\
&= \tau_{\xi_\sigma^\eta} + \tau_\eta \\
&= \tau_{\xi_\sigma^\eta} + \widetilde{\xi}_\eta \\
&= (\widetilde{\xi}_\sigma)^\eta + \widetilde{\xi}_\eta.
\end{aligned}$$

(To see the last step, note that for any point $P \in E(\overline{k})$, $(\widetilde{\xi}_\sigma)^\eta(P)$ applies η only to the *coefficients* of the morphism, not to P.)

With the above in mind, from $-\xi \in H^1(G_k, E(\overline{k}))$ there exists a twist $(C_{/k}, \phi) \in \mathrm{Twists}(E,k)$ such that for all $\sigma \in G_k$, one has

$$\phi^\sigma \phi^{-1} = \tau_{-\xi_\sigma} \qquad \text{for all } \sigma \in G_k. \tag{26}$$

On the level of points, this says that for all $X \in E(\overline{k})$ we have

$$\phi^\sigma(\phi^{-1}(X)) = X - \xi_\sigma.$$

Let us define a map

$$\mu \colon C \times E \to C, \qquad \mu(p,P) := \phi^{-1}(\phi(p) + P).$$

We claim that this map makes C a homogeneous space for E; intuitively, this map gives an action of E on C by taking points in C to E, adding them in E, and then taking them back to C.

First, we check that μ is simply transitive. Observe that for $p, q \in C$, taking $P := -\phi(p) + \phi(q)$ gives $\mu(p,P) = q$. Furthermore, if $Q \in E$ is another point for which

$\mu(p, Q) = q$, then by definition of μ we have $Q = P$ as above. This proves that μ is simply transitive.

Next, we claim that μ is defined over k. This is equivalent to showing that for all $p \in C$, $P \in E$ and $\sigma \in G_k$, we have

$$\mu(p, P)^\sigma = \mu(p^\sigma, P^\sigma).$$

We first check that

$$\begin{aligned}\mu(p, P)^\sigma :&= [\phi^{-1}(\phi(p) + P)]^\sigma \\ &= (\phi^{-1})^\sigma(\phi^\sigma(p^\sigma) + P^\sigma).\end{aligned}$$

On the other hand, we have

$$\begin{aligned}\mu(p^\sigma, P^\sigma) :&= \phi^{-1}(\phi(p^\sigma) + P^\sigma) \\ &= ((\phi^\sigma)^{-1} \circ \tau_{-\xi_\sigma})(\phi(p^\sigma) + P^\sigma) \qquad \text{(from (26))} \\ &= (\phi^\sigma)^{-1}(\phi(p^\sigma) + P^\sigma - \xi_\sigma) \\ &= (\phi^{-1})^\sigma(\phi(p^\sigma) + P^\sigma - \xi_\sigma) \qquad \text{(since } (\phi^{-1})^\sigma \text{ is the inverse of } \phi^\sigma).\end{aligned}$$

Thus, showing that $\mu(p, P)^\sigma = \mu(p^\sigma, P^\sigma)$ is equivalent to showing that

$$\phi^\sigma(p^\sigma) = \phi(p^\sigma) - \xi_\sigma.$$

This follows from (26): taking $X := \phi(p^\sigma)$, we know that

$$\phi^\sigma(\phi^{-1}(X)) = X - \xi_\sigma,$$

i.e.,

$$\phi^\sigma(\phi^{-1}(\phi(p^\sigma))) = \phi(p^\sigma) - \xi_\sigma,$$

i.e.,

$$\phi^\sigma(p^\sigma) = \phi(p^\sigma) - \xi_\sigma.$$

We conclude that the twist $(C_{/k}, \phi)$ of E whose associated *twist* 1-cocyle is $\phi^\sigma\phi^{-1} = \tau_{-\xi_\sigma}$, is a homogeneous space for E via $\mu(p, P) := p + P := \phi^{-1}(\phi(p) + P)$.

It remains to show that the associated *homogeneous space* 1-cocyle of $(C_{/k}, \phi, \mu)$ under our map $\mathrm{WC}(E, k) \to H^1(G_k, E(\overline{k}))$, which is

$$\sigma \mapsto p_0^\sigma - p_0$$

where $p_0 \in C(\overline{k})$ is any fixed point, is equivalent to ξ modulo 1-coboundaries. As it turns out, these two cocycles are equal if we take $p_0 := \phi^{-1}(O)$: we check that

$$\begin{aligned}p_0^\sigma - p_0 :&= \phi^{-1}(O)^\sigma - \phi^{-1}(O) \\ &= (\phi^{-1})^\sigma(O) - \phi^{-1}(O) && \text{(since } O \in E(k)) \\ &= (\phi^\sigma)^{-1}(O) - \phi^{-1}(O) && \text{(since } (\phi^\sigma)^{-1} = (\phi^{-1})^\sigma) \\ &= ((\phi^\sigma)^{-1} \circ \tau_{-\xi_\sigma})(\xi_\sigma) - \phi^{-1}(O) \\ &= \phi^{-1}(\xi_\sigma) - \phi^{-1}(O) && \text{(from (26)).}\end{aligned}$$

Recall that $\phi^{-1}(\xi_\sigma) - \phi^{-1}(O) := \nu(\phi^{-1}(\xi_\sigma), \phi^{-1}(O)) := Q$ is the unique point in $E(\overline{k})$ which satisfies

$$\phi^{-1}(\xi_\sigma) = \phi^{-1}(O) + Q := \mu(\phi^{-1}(O), Q).$$

Since by definition of μ we have

$$\mu(\phi^{-1}(O), Q) := \phi^{-1}(\phi(\phi^{-1}(O)) + Q) = \phi^{-1}(Q),$$

we deduce that $Q = \xi_\sigma$, and conclude that

$$p_0^\sigma - p_0 = \xi_\sigma.$$

Therefore, the 1-cocyles $\sigma \mapsto p_0^\sigma - p_0$ and ξ are equal, whence we conclude that $\mathrm{WC}(E, k) \to H^1(G_k, E(\overline{k}))$ surjects. (Had we instead used the condition that $\phi^\sigma \phi^{-1} = \tau_{\varphi_\sigma}$, then our space (C, ϕ, μ) would map to $-\xi$.)

Example 10.3.1. In the following example, we will construct homogeneous spaces for an elliptic curve with a rational point of order two. This is a key construction for homogeneous spaces which arise through calculating $E(F)$ via *descent from 2-isogenies,* which will be described in the next section.

Assume that $\mathrm{char}(k) \neq 2$. Let $E_{/k}$ be an elliptic curve. Fix an element $d \in k \smallsetminus k^2$; recall from §10.2 [Sil09] that there exists a quadratic character

$$\chi \colon G_k \to \{\pm 1\}, \qquad \chi(\sigma) := \frac{\sigma(\sqrt{d})}{\sqrt{d}}.$$

Suppose there exists an order two point $T \in E(k)$. Define a map

$$\xi \colon G_k \to E(\overline{k}), \qquad \xi_\sigma := \begin{cases} O & \text{if } \chi(\sigma) = 1 \\ T & \text{if } \chi(\sigma) = -1. \end{cases}$$

This is a homomorphism, and thus induces a 1-cocyle in $H^1(G_k, E(\overline{k}))$. We can construct a homogeneous space for χ through our analysis in Remark 10.3.1.

We need to construct a twist $(C_{/k}, \phi)$ of E for which

$$\phi^\sigma \phi^{-1} = \tau_{-\xi_\sigma};$$

once we have this, we then have our homogeneous space, with an action $\mu \colon C \times E \to C$ given by $\mu(p, P) := \phi^{-1}(\phi(p) + P)$. Pointwise, this cocycle condition says that for $X \in E$, one has

$$\phi^\sigma(\phi^{-1}(X)) = \begin{cases} X & \text{if } \chi_d(\sigma) = 1 \\ X + T & \text{if } \chi_d(\sigma) = -1 \end{cases}$$

(note that $-T = T$). After a change of variables, we can assume that E is given by the equation

$$E : y^2 = x^3 + ax^2 + bx,$$

and that $T = (0, 0)$. We have $\overline{k}(E) = \overline{k}(x, y)$, and the twisted action for elements $f(x, y) \in \overline{k}(E)$ is then

$$f(x, y)^{\sigma, t} := f^\sigma(x^{\sigma,t}, y^{\sigma,t}) = \begin{cases} f^\sigma(x, y) & \text{if } \chi_d(\sigma) = 1 \\ f^\sigma(\tau_T^*(x), \tau_T^*(y)) & \text{if } \chi_d(\sigma) = -1. \end{cases}$$

Let us compute $\tau_T^*(x)$ and $\tau_T^*(y)$; to do this, it is equivalent to describe τ_T on the level of points $(x, y) \in E$. We check using the chord and tangent method that for $(x, y) \neq O, T$, we have

$$\tau_T(x, y) := (x, y) + (0, 0) = \left(\frac{b}{x}, -\frac{by}{x^2}\right).$$

We deduce that $\tau_T^*(x) = \frac{b}{x}$ and $\tau_T^*(y) = \frac{-by}{x^2}$.

Now let us compute ℓ, the fixed field of $\overline{k}(x, y)$ under this twisted action. Through observation, we see that

$$f := \frac{\sqrt{d}x}{y} \in \ell \qquad \text{and} \qquad g := \sqrt{d}\left(x - \frac{b}{x}\right) \in \ell.$$

Consequently, we also have

$$z := f = \frac{\sqrt{d}x}{y} \in \ell \qquad \text{and} \qquad w := \frac{f^2 g}{d} = \sqrt{d}\left(x - \frac{b}{x}\right)\left(\frac{x}{y}\right)^2 \in \ell.$$

These two functions z and w satisfy

$$dw^2 = d^2 - 2adz^2 + (a^2 - 4b)z^4.$$

This equation defines a *hyperelliptic curve,* which we denote by C_d. As it turns out, C_d is an affine piece of a smooth curve in $\mathbb{P}^3$, which is C_d with two points at infinity $\left[0 : 0 : \pm\sqrt{\frac{a^2-4b}{d}} : 1\right]$. By abuse of notation, we also use C_d to denote this smooth curve.

Given our definitions of z and w, there is a rational map $\phi^{-1} \colon E \to C$ given by

$$\phi^{-1}(x, y) := (z, w) = \left(\frac{\sqrt{d}x}{y}, \sqrt{d}\left(x - \frac{b}{x}\right)\left(\frac{x}{y}\right)^2\right)$$

(it will soon be clear why we're using ϕ^{-1} here). Using that $\frac{x}{y} = \frac{xy}{y^2} = \frac{y}{x^2+ax+b}$, we can also define $\phi^{-1}(0, 0) := (0, -\sqrt{d})$ and $\phi^{-1}(O) = (0, \sqrt{d})$. Thus, ϕ^{-1} extends to a morphism (which we already knew by [Sil09, Proposition II.2.1]). We also find its inverse $\phi \colon C \to E$ by expressing z and w in terms of x and y from their definition:

$$\phi(z, w) := \left(\frac{\sqrt{d}w - az^2 + d}{2z^2}, \frac{dw - a\sqrt{dz^2 + d\sqrt{d}}}{2z^3}\right).$$

We conclude that ϕ^{-1} is an isomorphism defined over $k(\sqrt{d})$.

By Remark 10.3.1, we know that the hyperelliptic curve $C_{/k}$ is a homogeneous space for E. We can also double-check directly that its associated 1-cocycle in $H^1(G_k, E(\overline{k}))$, via

$$\sigma \mapsto p_0^\sigma - p_0 \qquad \text{for any fixed } p_0 \in C(\overline{k}),$$

is equivalent to ξ modulo 1-coboundaries. In fact, by our work in Remark 10.3.1, this is an equality if we take $p_0 := \phi^{-1}(O) = (0, \sqrt{d})$. With this p_0, we check that

$$p_0^\sigma - p_0 = (0, \chi_d(\sigma)\sqrt{d}) - (0, \sqrt{d}).$$

Thus, $\chi_d(\sigma) = 1$ if and only if $p_0^\sigma - p_0 = O$. When $\chi_d(\sigma) = -1$, to compute $p_0^\sigma - p_0 = (0, -\sqrt{d}) - (0, \sqrt{d})$, we need to find $Q \in E(\overline{k})$ with $\mu((0, \sqrt{d}), Q) = (0, -\sqrt{d})$. We check directly that such a Q satisfies

$$\begin{aligned}\mu((0, \sqrt{d}), Q) :&= \phi^{-1}(\phi(0, \sqrt{d}) + Q) \\ &= \phi^{-1}(O + Q) \\ &= \phi^{-1}(Q).\end{aligned}$$

Thus, to have $\mu((0, \sqrt{d}), Q) = (0, -\sqrt{d})$, we must have $Q = \phi((0, -\sqrt{d})) = (0, 0)$. We conclude that $p_0^\sigma - p_0 = \xi_\sigma$.

These hyperelliptic curves C_d will be the homogeneous spaces which show up when analyzing the Mordell-Weil group of elliptic curves $E_{/F}$ with an F-rational order two point in the next section.

10.4. **The Selmer and Shafarevich-Tate groups.** As noted in the final remark of Section 10.1, complete 2-descent for an elliptic curve $E_{/F}$ might not work if we find a particular pair $(b_1, b_2) \in F(S, 2) \times F(S, 2)$ for which the associated system of equations (which in fact defines a homogeneous space for E) has solutions over each completion F_v, but no F-rational solution. This is an instance of the failure of the *Hasse principle,* or *local-global principle,* for said homogeneous space. To give this some more context: recall from the introduction of these notes the *Hasse-Minkowski theorem,* which stated that the local-global principle succeeds for quadratic equations:

Theorem 10.4.1 (Hasse-Minkowski)**.** *For a quadratic equation*

$$Q : ax^2 + bxy + cy^2 + dx + ey + f = 0$$

with $a, b, c, d, e, f \in \mathbb{Q}$, there exists a $\mathbb{Q}$-rational solution $(x, y) \in \mathbb{Q}^2$ to Q if and only if there exists a real solution, and for each prime $p \in \mathbb{Z}^+$ a solution over $\mathbb{Q}_p$.

Recall that the homogeneous spaces which show up in complete 2-descent were given by *two* quadratic equations, which means the Hasse principle can fail for them. Thus, in attempting 2-descent on an elliptic curve $E_{/F}$, we might have a pair $(b_1, b_2) \in F(S, 2) \times F(S, 2)$ for which the associated homogeneous space has a local solution over every completion of F, but no F-rational solution. Despite this, there is a way to quantify which of these homogeneous spaces are curves that will satisfy the local-global principle, and that is with the *Shafarevich-Tate group of $E_{/F}$.* We will define this group, along with the ϕ-Selmer group, and describe an alternative method of descent to compute a weak Mordell-Weil group for E which involves a more relaxed rationality condition than $E[2] \subseteq E(F)$.

Let us state what we can for a perfect field k, as some of this will be applied to local fields. As in the number field case, for an elliptic curve $E_{/k}$ and an integer $n \geq 2$ coprime to $\mathrm{char}(k)$, we have a short exact sequence of G_k-modules

$$0 \to E[n] \xrightarrow{\iota} E(k) \xrightarrow{[n]} E(k) \to 0,$$

which induces by cohomology the SES

$$0 \to E(k)/nE(k) \xrightarrow{\delta_n} H^1(G_k, E[n]) \xrightarrow{\iota_\circ} H^1(G_k, E(\overline{\mathbb{Q}}))[n] \to 0.$$

Here, the connecting homomorphism $\delta_n := \delta_{E,n} \colon E(k)/nE(k) \hookrightarrow H^1(G_k, E[n])$ is defined as follows: fixing any point $Q \in E(\overline{k})$ with $nQ = P$, we define

$$\delta_n(\overline{P})(\sigma) := Q^\sigma - Q.$$

When $E[n] \subseteq E(k)$, we get $H^1(G_k, E[n]) = \mathrm{Hom}_{\mathbb{Z}}(G_k, E[n])$, as well as $\delta_n(\overline{P}) = \kappa(P, -)$, the usual elliptic Kummer pairing.

There is a more general version of the short exact sequence above with which we can analyze the Mordell-Weil group, allowing for a weaker requirement than $E[n] \subseteq E(k)$. Suppose that $E_{/k}$ and $E'_{/k}$ are two elliptic curves and $\phi \colon E \to E'$ is a k-rational isogeny of degree $d \in \mathbb{Z}^+$ coprime to $\mathrm{char}(k)$. Then for $E[\phi] := \ker \phi$, we have that $E[\phi]$ is a G_k-module. We thus have a SES of G_k-modules

$$0 \to E[\phi] \to E(\overline{k}) \xrightarrow{\phi} E'(\overline{k}) \to 0,$$

which by cohomology induces the SES

$$0 \to E'(k)/\phi(E(k)) \xrightarrow{\delta_\phi} H^1(G_k, E[\phi]) \xrightarrow{\iota\circ} H^1(G_k, E(\overline{k}))[\phi] \to 0.^{16}$$

The connecting homomorphism is defined as $\delta_\phi(\overline{P'})(\sigma) := Q^\sigma - Q$, for any fixed $Q \in E(\overline{k})$ with $\phi(Q) = P'$. By [Sil09, Theorem X.3.6], we can identify $H^1(G_k, E(\overline{k}))$ with $\mathrm{WC}(E, k)$ via the bijection

$$\mathrm{WC}(E, k) \to H^1(G_k, E(\overline{k})), \qquad [(C, \mu)] \mapsto [\sigma \mapsto p_0^\sigma - p_0] \text{ for any fixed } p_0 \in C(\overline{k}).$$

Thus we have the SES

$$0 \to E'(k)/\phi(E(k)) \xrightarrow{\delta_\phi} H^1(G_k, E[\phi]) \to \mathrm{WC}(E, k)[\phi] \to 0. \tag{27}$$

Taking $E' = E$ and $\phi = [n]$, this generalizes the previous SES.

Remark 10.4.1. Note that understanding δ_ϕ in the short exact sequence above gives information about the weak Mordell-Weil group $E'(k)/\phi(E(k))$ *for* E'*;* however, this and the corresponding SES from the dual isogeny $\hat{\phi} \colon E' \to E$ gives information about the Mordell-Weil group $E(k)$ through the SES

$$0 \to \frac{E'(k)[\hat{\phi}]}{\phi(E(k)[d])} \to \frac{E'(k)}{\phi(E(k))} \xrightarrow{\hat{\phi}} \frac{E(k)}{dE(k)} \to \frac{E(k)}{\hat{\phi}(E'(k))} \to 0.$$

This gives a way to understand $E(k)$ and $E'(k)$ through understanding their homogeneous spaces.

For the rest of this section, we assume that $k =: F$ is a number field. For each place $v \in \Sigma_F$, we have a completion F_v and an inclusion $G_{F_v} \subseteq G_F$ given by extending each $v \in \Sigma_F$ to $\overline{\mathbb{Q}}$ (note that G_{F_v} is the decomposition group of v in G_F). There is an analogous short exact sequence to (27) given by

$$0 \to E'(F_v)/\phi(E(F_v)) \xrightarrow{\delta_\phi} H^1(G_{F_v}, E[\phi]) \to \mathrm{WC}(E, F_v)[\phi] \to 0.$$

[16]Note that we have defined $H^1(G_k, E(\overline{k}))[\phi] := \{\xi \in H^1(G_k, E[\phi]) : \forall \sigma \in G_k,\ \phi(\xi_\sigma) = O\}$. We have $H^1(G_k, E[\phi]) \neq H^1(G_k, E(\overline{k}))[\phi]$ since the coboundary set of the first group is strictly smaller than the coboundary set of the second group.

This implies we have the commutative diagram

$$\begin{array}{ccccccccc} 0 & \longrightarrow & E'(F)/\phi(E(F)) & \xrightarrow{\delta_\phi} & H^1(G_F, E[\phi]) & \longrightarrow & \mathrm{WC}(E,F)[\phi] & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & \prod_{v\in\Sigma_F} E'(F_v)/\phi(E(F_v)) & \xrightarrow{\delta_\phi} & \prod_{v\in\Sigma_F} H^1(G_{F_v}, E[\phi]) & \longrightarrow & \prod_{v\in\Sigma_F} \mathrm{WC}(E,F_v)[\phi] & \longrightarrow & 0 \end{array}$$

where the vertical maps are induced from each inclusion $F \subseteq F_v$. We know by (27) that we can compute $E'(F)/\phi(E(F))$ by analyzing the image of δ_ϕ: it shows that

$$\mathrm{im}\,(\delta_\phi \colon E'(F)/\phi(E(F)) \hookrightarrow H^1(G_F, E[\phi])) = \ker(H^1(G_F, E[\phi]) \to \mathrm{WC}(E,F)[\phi]).$$

However, the diagram shows that this latter kernel is contained in

$$\ker\left(H^1(G_F, E[\phi]) \to \prod_{v\in\Sigma_F} \mathrm{WC}(E,F_v)\right).$$

This leads us to the following definitions.

Definition 10.4.1. Let $E_{/F}, E'_{/F}$ be elliptic curves and $\phi \colon E \to E'$ an F-rational isogeny. Then the **ϕ-Selmer group of** $E_{/F}$ is the subgroup of $H^1(G_F, E[\phi])$ defined by

$$S^{(\phi)}(E,F) := \ker\left\{H^1(G_F, E[\phi]) \to \prod_{v\in\Sigma_F} \mathrm{WC}(E,F_v)\right\}.$$

The **Shafarevich-Tate group of** $E_{/F}$ is the subgroup of $H^1(G_F, E(\overline{\mathbb{Q}}))$ defined by

$$Ш(E,F) := \ker\left\{\mathrm{WC}(E,F) \to \prod_{v\in\Sigma_F} \mathrm{WC}(E,F_v)\right\}.$$

Remark 10.4.2. By Proposition 10.3.3 ([Sil09, Proposition X.3.3]), the Shafarevich-Tate group can be interpreted as the subgroup of $\mathrm{WC}(E,F)$ of homogeneous spaces of E which are locally soluble everywhere, up to equivalence; these are the homogeneous spaces $C_{/F}$ of E such that for each place $v \in \Sigma_F$, one has $C(F_v) \neq \emptyset$. The ϕ-Selmer group $S^{(\phi)}(E,F)$ can be interpreted as the subgroup of $H^1(G_F, E[\phi])$ of *ϕ-coverings* of E defined over F, which are twists of the isogeny $\phi \colon E \to E'$ (in an appropriate sense) which are locally soluble everywhere. For more on ϕ-coverings, see the discussion surrounding Theorem 8 of these notes.

On a less formal level, the commutative diagram above lets us understand the weak Mordell-weil group $E'(F)/\phi(E(F))$ through understanding the ϕ-Selmer group, which is the kernel of the "middle-down-right" map. In fact, this is connected to the ϕ-torsion subgroup of the Tate-Shafarevich group, which is the kernel of the "rightmost-down" map.

Theorem 10.4.2. [Sil09, Theorem X.4.2] *Let $\phi \colon E \to E'$ be an F-rational isogeny.*

a. There is a short exact sequence

$$0 \to E'(F)/\phi(E(F)) \to S^{(\phi)}(E,F) \to Ш(E,F)[\phi] \to 0. \tag{28}$$

b. The Selmer group $S^{(\phi)}(E,F)$ is finite.

Remark 10.4.3. The proof of part a. is a quick consequence of the commutative diagram above. For part b., a key step is to show that all cocyles in $S^{(\phi)}(E,F)$ are *unramified* away from a fixed finite set S of places. For a G_F-module M and a place $v \in \Sigma_F$, we say that a 1-cocyle $\xi \in H^1(G_F, M)$ is *unramified at* v if $\xi = 0$ on an(y) inertia group I_v of v. One shows that elements of $S^{(\phi)}(E,F)$ are unramified away from

$$S := \{\mathfrak{P} \in \Sigma_F^{\mathrm{NA}} : E \text{ has bad reduction at } \mathfrak{P}\} \cup \{\mathfrak{P} \in \Sigma_F^{\mathrm{NA}} : \mathfrak{P} \mid \deg(\phi)\} \cup \Sigma_F^{\mathrm{Arch}}, \tag{29}$$

see [Sil09, Corollary X.4.4]. One then shows that for a G_F-module M, the subset $H^1(G_F, M; S)$ of cocycles unramified away from S is *finite* if S is finite, see [Sil09, Lemma X.4.3]; this is done using the inflation-restriction sequence from Appendix B of [Sil09]. This then proves part b.

Remark 10.4.4. Remark 10.4.3 shows that $S^{(\phi)}(E,F)$ is effectively computable. To see this, first note that $S^{(\phi)}(E,F)$ is contained in $H^1(G_F, E[\phi]; S)$, and $H^1(G_F, E[\phi]; S)$ is finite. Then to check which elements $\xi \in H^1(G_F, E[\phi]; S)$ lie in $S^{(\phi)}(E,F)$, one lifts ξ under the bijection $\mathrm{WC}(E,F) \to H^1(G_F, E(\overline{\mathbb{Q}}))$ to a homogeneous space $(C_{/k}, \psi, \mu)$ as in Remark 10.3.1 ([Sil09, Theorem X.3.6]) and checks for the finitely many $v \in S$ whether $C(F_v) \neq \emptyset$. By Hensel's lemma, this last part is a finite amount of computation.

Example 10.4.1. [Sil09, Example X.4.5.1] Let us rephrase the complete 2-descent example (Example 10.1.1) in terms of the 2-Selmer group and Ш. Recall that we wanted to determine the structure of the Mordell-Weil group $E(\mathbb{Q})$ of the elliptic curve

$$E : y^2 = x^3 - 12x^2 + 20x.$$

We had $E[2] \subseteq E(\mathbb{Q})$, so the theory of Section 10.1 applied. We reduced the problem to checking the following: with $\mathbb{Q}(S,2) := \{\pm 1, \pm 2, \pm 5, \pm 10\}$ (in $\mathbb{Q}^\times/(\mathbb{Q}^\times)^2$), we checked for each pair $(b_1, b_2) \in \mathbb{Q}(S,2) \times \mathbb{Q}(S,2)$ whether the homogeneous space defined by

$$b_1 z_1^2 - b_2 z_2^2 = 2 \qquad \text{and} \qquad b_1 z_1^2 - b_1 b_2 z_3^2 = 10,$$

which defines a curve in $\mathbb{P}^3$, had a rational solution; and if it did, we gave one. We were lucky in our analysis, in that each of these homogeneous spaces either had a solution over $\mathbb{Q}$ that we spotted, or provably had no solution over e.g. $\mathbb{R}$ or $\mathbb{Q}_5$, and thus no solution over $\mathbb{Q}$. This shows that there is no nontrivial order two element of $Ш(E,\mathbb{Q})$, i.e., no homogeneous space with local solutions everywhere but no global solution: $Ш(E,\mathbb{Q})[2] = 0$. By (28), this also shows that $S^{(2)}(E,\mathbb{Q}) \cong E(\mathbb{Q})/2E(\mathbb{Q}) \cong \mathbb{F}_2^3$.

Let us explain how one can "systematize" the example above into our next descent theorem. Let us assume as before that we have an F-rational isogeny $\phi\colon E \to E'$, say of degree n. Assume that ϕ is cyclic. In fact, let us further assume that $E[\phi] \subseteq E(F)$ and $E'[\hat{\phi}] \subseteq E'(F)$, so that $E[\phi]$ and $E'[\hat{\phi}]$ are trivial G_F-modules. Now, (27) tells us we have an embedding

$$\delta_\phi\colon E'(F)/\phi(E(F)) \hookrightarrow \mathrm{Hom}_{\mathbb{Z}}(G_F, E[\phi]).$$

We also have by Hilbert's Theorem 90 an isomorphism $\delta_F\colon F^\times/(F^\times)^n \xrightarrow{\sim} \mathrm{Hom}_{\mathbb{Z}}(G_F, E[\phi])$. In a similar fashion to [Sil09, Proposition VIII.1.5], one can show that this induces an

isomorphism $\delta_F\colon F(S,n) \xrightarrow{\sim} H^1(G_F, \mu_n; S)$. Finally, from $E[\phi] \subseteq E(F)$ one can check that $H^1(G_F, E[\phi]) \subseteq H^1(G_F, \mu_n; S)$, which shows that we can identify $S^{(\phi)}(E,F) \subseteq F(S,n)$ under δ_F^{-1}. We can put these two pieces of information together and attempt to compute $E'(F)/\phi(E(F))$ using (28).

The simplest case is where $n = 2$, which is equivalent to E and E' having an F-rational point of order two; say these points are T and T', respectively. Changing coordinates if necessary, we can assume that we have $E : y^2 = x^3 + ax^2 + bx$ with $T = (0,0)$; we can also assume that $E' : y^2 = x^3 - 2ax^2 + (a^2 - 4b)x$ and $T' = (0,0)$, and

$$\phi(x,y) := \left(\frac{y^2}{x^2}, \frac{y(b-x^2)}{x^2}\right),$$

see Example 3.4.5.

In the situation above, we have $\mu_2 = \{\pm 1\}$, and the isomorphism $\delta_F\colon F(S,2) \xrightarrow{\sim} H^1(G_F, \mu_2; S)$ is given by quadratic characters: that is, we have $\delta_F(d)(\sigma) = \chi_d(\sigma)$, where $\chi_d\colon G_F \to \{\pm 1\}$ is defined by $\sigma(\sqrt{d}) := \chi_d(\sigma) \cdot \sqrt{d}$ (this can be checked directly, noting that δ_F is the usual connecting homomorphism). As we did in Example 10.3.1, we can then define a 1-cocyle in $H^1(G_F, E(\overline{\mathbb{Q}}))$ from χ_d by

$$\xi\colon G_F \to E(\overline{\mathbb{Q}}), \qquad\qquad \xi_\sigma := \begin{cases} O & \text{if } \chi(\sigma) = 1 \\ T & \text{if } \chi(\sigma) = -1. \end{cases}$$

We showed in Example 3.4.5 that the corresponding homogeneous space for ξ_d is

$$C_d : dw^2 = d^2 - 2adz^2 + (a^2 - 4b)z^4.$$

We conclude from the identification $S^{(\phi)}(E,F) \subseteq F(S,2)$ and Remark 10.4.4 that we can effectively compute $S^{(\phi)}(E,F)$ by checking for each $d \in F(S,2)$ and $v \in S$ whether $C_d(F_v) = \emptyset$; those $d \in F(S,2)$ for which $C_d(F_v) \neq \emptyset$ for some $v \in S$ will correspond to a nontrivial element $\delta_F(d) = \chi_d \in S^{(\phi)}(E,F)$.

The example above is referred to as *descent via two-isogeny.* We cast it here as a theorem.

Theorem 10.4.3. [Sil09, Proposition X.4.9] *Let $E_{/F}$ and $E'_{/F}$ be elliptic curves defined by*

$$E : y^2 = x^3 + ax^2 + bx \qquad \text{and} \qquad E' : y^3 = x^3 - 2ax^2 + (a^2 - 4b)x.$$

Let $\phi\colon E \to E'$ be defined by

$$\phi(x,y) := \left(\frac{y^2}{x^2}, \frac{y(b-x^2)}{x^2}\right).$$

Then ϕ is a cyclic 2-isogeny with $\ker\phi = \{O, (0,0)\}$. Let

$$S := \{\mathfrak{P} \in \Sigma_F^{\mathrm{NA}} : \mathfrak{P} \mid 2, \mathfrak{P} \mid b \text{ or } \mathfrak{P} \mid (a^2 - 4b)\} \cup \Sigma_F^{\mathrm{Arch}}.$$

For each $d \in F^\times$, let $C_{d/F}$ be the homogeneous space for $E_{/F}$ defined by

$$C_d : dw^2 = d^2 - 2adz^2 + (a^2 - 4b)z^4.$$

Then there is a short exact sequence

$$0 \to E'(F)/\phi(E(F)) \xrightarrow{\delta} F(S,2) \to \mathrm{WC}(E,F)[\phi].$$

Here, we have

$$\delta(\overline{(x,y)}) := x, \qquad \delta(\overline{O}) := 1, \qquad \delta(\overline{(0,0)}) := a^2 - 4b,$$

and $F(S,2) \to \mathrm{WC}(E,F)[\phi]$ *via* $d \mapsto [C_{d/F}]$.

The ϕ-Selmer group is

$$S^{(\phi)}(E,F) \cong \{d \in F(S,2) : \forall v \in S, C_d(F_v) \neq 0\}.$$

Finally, the map

$$\psi \colon C_d \to E, \qquad \psi(z,w) := \left(\frac{d}{z^2}, -\frac{dw}{z^3}\right)$$

has the property that if $P \in C_d(F)$, then

$$\delta(\psi(P)) \equiv d \pmod{(F^\times)^2}.$$

For a new example of complete 2-descent, see [Sil09, Example X.4.10]. This is already more content than was covered from this section in my class – however, there is one more thing we will discuss. The obstruction to effectively computing the Mordell-Weil group of an elliptic curve with the techniques in this chapter is the potential nontriviality of its Shafarevich-Tate group. However, if $Ш(E,F)$ is *finite,* then one can use "relative Selmer groups" to find generators for $E(F)/nE(F)$ for suitably chosen $n \in \mathbb{Z}^+$. However, it is unknown whether $Ш(E,F)$ is always finite – Theorem 10.4.2 only says that the ϕ-torsion subgroup of $Ш(E,F)$ is finite. This leads us to the following conjecture, which is only known for certain families of elliptic curves.

Conjecture 10.4.4. *Let $E_{/F}$ be an elliptic curve. Then $Ш(E,F)$ is finite.*

Fin.

Appendix A. A Brief Review of Local Fields

In this appendix, we quickly cover a few definitions and results on local fields which will serve as necessary background for Chapter 7. For a more comprehensive set of notes, see e.g. Clark's [ClaANT2].

For a field K, a *valuation on* K is a map $v\colon K \to \mathbb{R} \cup \{\infty\}$ with the following properties:

1. $v(xy) = v(x) + v(y)$ for all $x, y \in K$;
2. $v(x+y) \geq \min\{v(x), v(y)\}$ for all $x, y \in K$;
3. $v(x) = \infty$ if and only if $x = 0$.

For a valuation $v\colon K \to \mathbb{R} \cup \{\infty\}$, the subset

$$R_v := \{x \in K : v(x) \geq 0\}$$

is a local ring in K, with maximal ideal

$$M_v := \{x \in K : v(x) > 0\}.$$

Say v is a *discrete valuation* if its image is $\mathbb{Z} \cup \{\infty\}$. In this case, R_v is a discrete valuation ring.

Given a field K, an *absolute value,* or *norm,* on K, is a map $|\cdot|\colon K \to \mathbb{R}_{\geq 0}$ with the following properties:

1. $|xy| = |x| \cdot |y|$ for all $x, y \in K$;
2. $|x+y| \leq |x| + |y|$ for all $x, y \in K$ (triangle inequality);
3. $|x| = 0$ if and only if $x = 0$.

Say $|\cdot|$ is *non-Archimedean* if for all $x, y \in K$ one has $|x+y| \leq \max\{|x|, |y|\}$. Otherwise, say it is *Archimedean.* In general, we call $(K, |\cdot|)$ a *normed field.*

Given a normed field $(K, |\cdot|)$, the subset

$$R_{|\cdot|} := \{x \in K : |x| \leq 1\}$$

is a local ring in K, with maximal ideal

$$M_{|\cdot|} := \{x \in K : |x| < 1\}.$$

Observe that a normed field $(K, |\cdot|)$ inherits a metric space topology from $|\cdot|$. The completion of K with respect to $|\cdot|$ is denoted by $\widehat{K}$. Let us recall the construction of the completion of a metric space (X, d). A sequence $\{x_n\}_{i=1}^{\infty} \subseteq X$ is called *Cauchy* if for all $\epsilon > 0$, there exists $N \in \mathbb{Z}^+$ such that for any $m, n \geq N$, one has $d(x_m, x_n) < \epsilon$. Two Cauchy sequences $\{x_n\}_{i=1}^{\infty}, \{y_n\}_{i=1}^{\infty} \subseteq X$ are said to be *equivalent* if

$$\lim_{n\to\infty} d(x_n, y_n) = 0.$$

Then the *completion of X with respect to d,* written as $\widehat{X}$, is the quotient space of Cauchy sequences of X under this equivalence. The completion $\widehat{X}$ admits the following metric: for all $A, B \in \widehat{X}$, writing $x = [\{x_n\}_{i=1}^{\infty}]$ and $y = [\{y_n\}_{i=1}^{\infty}]$ one has

$$\widehat{d}(x, y) := \lim_{n\to\infty} d(x_n, y_n).$$

We have a natural embedding $\iota\colon X \hookrightarrow \widehat{X}$, and $\iota(X)$ is dense in $\widehat{X}$ under the metric of the completion; furthermore, $\widehat{d} = d$ on $\iota(X)$. If $(X, d) = (K, |\cdot|)$ is a normed field, then the norm extension of $|\cdot|$ to $\widehat{K}$ can be defined as $|x| := \lim_{n\to\infty} |x_n|$.

For each prime $p \in \mathbb{Z}^+$, we let $\mathbb{Q}_p$ denote the completion of $\mathbb{Q}$ with respect to the *p-adic norm* $|\cdot|_p\colon \mathbb{Q} \to \mathbb{R}_{\geq 0}$. Recall that the *p-adic valuation* $v_p\colon \mathbb{Q} \to \mathbb{Z} \cup \{\infty\}$ is defined on integers $n \in \mathbb{Z}$ by the relation $p^{v_p(n)} \parallel n$; this extends to a map on $\mathbb{Q}$ in a natural way. In turn, this induces a norm map $|\cdot|_p\colon \mathbb{Q} \to \mathbb{R}_{\geq 0}$ via

$$|x|_p := |x|_{v_p} := p^{-v_p(x)}.$$

Since $v_p\colon \mathbb{Q} \to \mathbb{Z} \cup \{\infty\}$ is a discrete valuation which extends to $\mathbb{Q}_p$, there exists a discrete valuation ring $\mathbb{Z}_p \subseteq \mathbb{Q}_p$ for v_p, called the *p-adic integers.* More generally, for a number field F and a nonzero prime ideal $\mathfrak{P} \subseteq F$, we let $F_{\mathfrak{P}}$ denote the $\mathfrak{P}$-adic completion of F with respect to the $\mathfrak{P}$-adic norm $|\cdot|_{\mathfrak{P}}$, and $\mathcal{O}_{F,\mathfrak{P}}$ its discrete valuation ring. The field $\mathbb{Q}_p$, and more generally $F_{\mathfrak{P}}$, is an example of a non-Archimedean local field.

Given a field K and two absolute values $|\cdot|_1, |\cdot|_2$ on K, we say that $|\cdot|_1$ and $|\cdot|_2$ are *equivalent* if there exists $r \in \mathbb{R}_{>0}$ with $|\cdot|_2 = |\cdot|_1^r$. We then write $|\cdot|_1 \sim |\cdot|_2$. There is a classification of absolute values on a number field, due to Ostrowski.

Theorem (Ostrowski's Theorem)**.** *Up to equivalence, the only nontrivial absolute values on $\mathbb{Q}$ are:*

1. *the p-adic norms $|\cdot|_p$ (non-Archimedean);*
2. *the restriction of the usual absolute value $|\cdot|\colon \mathbb{C} \to \mathbb{R}_{\geq 0}$ (Archimedean).*

More generally, for a number field F, up to equivalence any nontrivial absolute absolute value on F is either:

1. *a $\mathfrak{P}$-adic norm $|\cdot|_{\mathfrak{P}}$ for some nonzero prime ideal $\mathfrak{P} \subseteq F$ (non-Archimedean);*
2. *the restriction of the usual absolute value $|\cdot|\colon \mathbb{C} \to \mathbb{R}_{\geq 0}$ to an embedding of F into $\mathbb{C}$. Such a norm has the form $|\sigma(\cdot)|$ where $\sigma\colon F \hookrightarrow \mathbb{C}$ (Archimedean).*

From here on out, any local field (K, v) we consider will be perfect, as well as its residue field $k := R/\pi$. If L/K is a finite extension, then L is also a complete local field, by a unique valuation w extending v (so $w|_K = v$) via

$$w(x) := \frac{1}{n} \cdot v(N_{L/K}(x)),$$

where $n := [L : K]$. In terms of norms, this is equivalent to

$$|x|_w := |N_{L/K}(x)|_v^{1/n};$$

see also [ClaANT2, Theorems 1.43, 1.46]. Note, however, that the valuation w above is *not* necessarily normalized, i.e., we might not have $w(L) = \mathbb{Z} \cup \{\infty\}$.

Let $(L, w)/(K, v)$ be a finite extension of complete local fields, with normalized discrete valuations. Let S be the associated discrete valuation ring of L, with uniformizer Π, and let $\ell := S/\Pi$ be the residue field of L. Then the *ramification index* of L/K is the ramification index of π in S; this is well-defined since S has only one prime up to associates, namely Π. One can show that $e(L/K) = [w(L) : w(K)] = w(\pi)$. From $R \subseteq S$ and $\Pi \mid \pi$, we also have an extension of residue fields ℓ/k; the *inertial degree*

of L/K is then $f(L/K) := [\ell : k]$. We see that an extension L/K is unramified if and only if $[L : K] = [\ell : k]$.

To make things more concrete: if F is a number field, then for each nonzero prime ideal $\mathfrak{P} \subseteq F$, we have a complete local field $F_{\mathfrak{P}}$ with a discrete valuation $v_{\mathfrak{P}} \colon F \to \mathbb{Z} \cup \{\infty\}$ given by ideal divisibility by $\mathfrak{P}$. If $L/F_{\mathfrak{P}}$ is a finite extension, then $L = M_{\mathfrak{Q}}$ where M/F is some finite extension with $[M_{\mathfrak{Q}} : F_{\mathfrak{Q}}] = [M : F]$, and $\mathfrak{Q} \subseteq M$ is some prime ideal which divides $\mathfrak{P}$ in M. One also has $e(M_{\mathfrak{Q}}|F_{\mathfrak{P}}) = e(\mathfrak{Q}|\mathfrak{P})$ and $f(M_{\mathfrak{Q}}|F_{\mathfrak{P}}) = f(\mathfrak{Q}|\mathfrak{P})$.

Finally, we use K^{nr} to denote the *maximal unramified extension of K,* which is the compositum of all unramified extensions of K. By Exercise A.0.5, we have an isomorphism $\mathrm{Gal}(K^{\mathrm{nr}}/K) \cong G_k$ via reduction of automorphisms $\sigma \colon L \xrightarrow{\sim} L$ to $\tilde{\sigma} \colon \ell \xrightarrow{\sim} \ell$, where L/K is unramified (and hence Galois). This fits into a short exact sequence

$$1 \to \mathrm{Gal}(\overline{K}/K^{\mathrm{nr}}) \to G_K \xrightarrow{\mathrm{red}} G_k \to 1.$$

The Galois group $I_v := \mathrm{Gal}(\overline{K}/K^{\mathrm{nr}})$ is called the *inertia group* of K.

Exercise A.0.1. Let K be a field.

a. Show that if $|\cdot| \colon K \to \mathbb{R}_{\geq 0}$ is a non-Archimedean absolute value, then $|\cdot|$ induces a valuation $v_{|\cdot|} \colon K \to \mathbb{R}_{\geq 0}$ via

$$v_{|\cdot|}(x) := \begin{cases} -\ln |x| & \text{if } x \neq 0, \\ \infty & \text{if } x = 0. \end{cases}$$

b. Show that if $v \colon K \to \mathbb{R} \cup \{\infty\}$ is a valuation, then we have an induced absolute value $|\cdot|_v \colon K \to \mathbb{Z} \cup \{\infty\}$ via

$$|x|_v := \begin{cases} 2^{-v(x)} & \text{if } x \neq 0, \\ 0 & \text{if } x = 0. \end{cases}$$

c. Prove that an absolute value $|\cdot| \colon K \to \mathbb{R}$ is non-Archimedean if and only if $|\mathbb{Z} \cdot 1_K|$ is bounded.

d. Deduce that if $v \colon K \to \mathbb{Z} \cup \{\infty\}$ is a discrete valuation, then $|\cdot|_v$ is non-Archimedean.

Exercise A.0.2.

a. Prove directly that $v_p \colon \mathbb{Q} \to \mathbb{Z} \cup \{\infty\}$ is a discrete valuation.

b. More generally, show that every nonzero prime ideal $\mathfrak{P} \subseteq K$ induces a discrete valuation $v_{\mathfrak{P}} \colon K \to \mathbb{Z} \cup \{\infty\}$.

c. Show that $\mathbb{Q}_p \neq \mathbb{Q}$.

Exercise A.0.3.

a. Show that for any real number $c > 1$, the p-adic norm $|\cdot|_p \colon \mathbb{Q} \to \mathbb{R}_{\geq 0}$ satisfies

$$|x|_p \sim c^{-v_p(x)}.$$

b. Let K be a field. Show that two nontrivial absolute values $|\cdot|_1, |\cdot|_2$ on K are equivalent if and only if they induce the same topology on K.

Exercise A.0.4. Prove **Hensel's Lemma** on lifting roots:

Theorem (Hensel's Lemma)**.** *Let K be a complete non-Archimedean field with valuation ring R, maximal ideal M and residue field $k := R/M$. Let $f \in R[t]$ be a polynomial, and let $\overline{f} \in k[t]$ be its reduction modulo M. If $a \in k$ is a simple root of $\overline{f}$ (i.e., $\overline{f}(a) = 0$ and $\overline{f}'(a) \neq 0$), then there exists $\alpha \in R$ with $\alpha \equiv a \pmod{M}$ and $f(\alpha) = 0$.*

Exercise A.0.5. This exercise proves the following result on unramified extensions of local fields.

Theorem. *Given a perfect non-Archimedean local field (K, v) with discrete valuation ring R, uniformizer π and perfect residue field $k := R/\pi$, there is a correspondence between the category of unramified extensions of K and the category of algebraic extensions of k.*

Let L/K be a finite extension; then L is also a non-Archimedean local field, say with discrete valuation w extending v, a discrete valuation ring S for w, a uniformizer Π and residue field $\ell := S/\Pi$.

a. Use Hensel's Lemma to prove there exists an unramified subextension $K \subseteq L' \subseteq L$ with residue field $\ell' = \ell$. Deduce that a finite unramified extension of K is completely determined by its residue field.
b. Show that for each $n \in \mathbb{Z}^+$, there is a unique unramified extension of K with degree n.
c. Conclude that the theorem holds.
d. (Optional) Prove that an unramified extension L/K is always Galois. Then give an explicit isomorphism

$$\mathrm{Gal}(K^{\mathrm{nr}}/K) \xrightarrow{\sim} G_k.$$

References

[ClaAAA] P.L. Clark, *Algebraic curves: an algebraic approach*, course notes, `http://alpha.math.uga.edu/~pete/8320_2020.pdf`.

[ClaANT2] P.L. Clark, *Algebraic Number Theory II: Valuations, Local Fields and Adeles*, course notes, `http://alpha.math.uga.edu/~pete/8410FULL.pdf`.

[Har20] D. Harari, *Galois cohomology and class field theory*, Universitext, Springer, Cham (2020). Translated from the 2017 French original by Andrei Yafaev.

[Har77] R. Hartshorne, *Algebraic geometry*, Graduate Texts in Mathematics, no. 52, Springer-Verlag (1977).

[Lan94] S. Lang, *Algebraic number theory*, 2nd Ed., Graduate Texts in Mathematics, vol. 110, Springer-Verlag, New York (1994).

[Lor96] D. Lorenzini, *An invitation to arithmetic geometry*, Graduate Studies in Mathematics, vol. 9, American Mathematical Society, Providence, RI (1996).

[Maz77] B. Mazur, *Modular curves and the Eisenstein ideal,* Inst. Hautes Études Sci. Publ. Math. No. 47 (1977).

[MilANT] J.S. Milne, *Algebraic Number Theory*, v3.08, course notes, `https://www.jmilne.org/math/CourseNotes/ANT.pdf`.

[Sha13] I.R. Shafarevich, *Basic algebraic geometry 1*, 3rd Ed., Springer, Heidelberg (2013).

[Sil94] J. Silverman, *Advanced topics in the arithmetic of elliptic curves*, Graduate Texts in Mathematics, vol. 151, Springer-Verlag, New York (1994).

[Sil09] J. Silverman, *The arithmetic of elliptic curves*, 2nd Ed., Graduate Texts in Mathematics, vol. 106, Springer (2009).

[ST15] J. Silverman and J. Tate, *Rational points on elliptic curves*, 2nd Ed., Undergraduate Texts in Mathematics, Springer, Cham (2015).

[Tat66] J. Tate, *Endomorphisms of abelian varieties over finite fields*, Invent. Math. 2 (1966), 134–144.

[VoiQA] J. Voight, *Quaternion algebras*, v.1.0.5, course notes, stable post-publication version, `https://jvoight.github.io/quat-book-v1.0.5.pdf`.