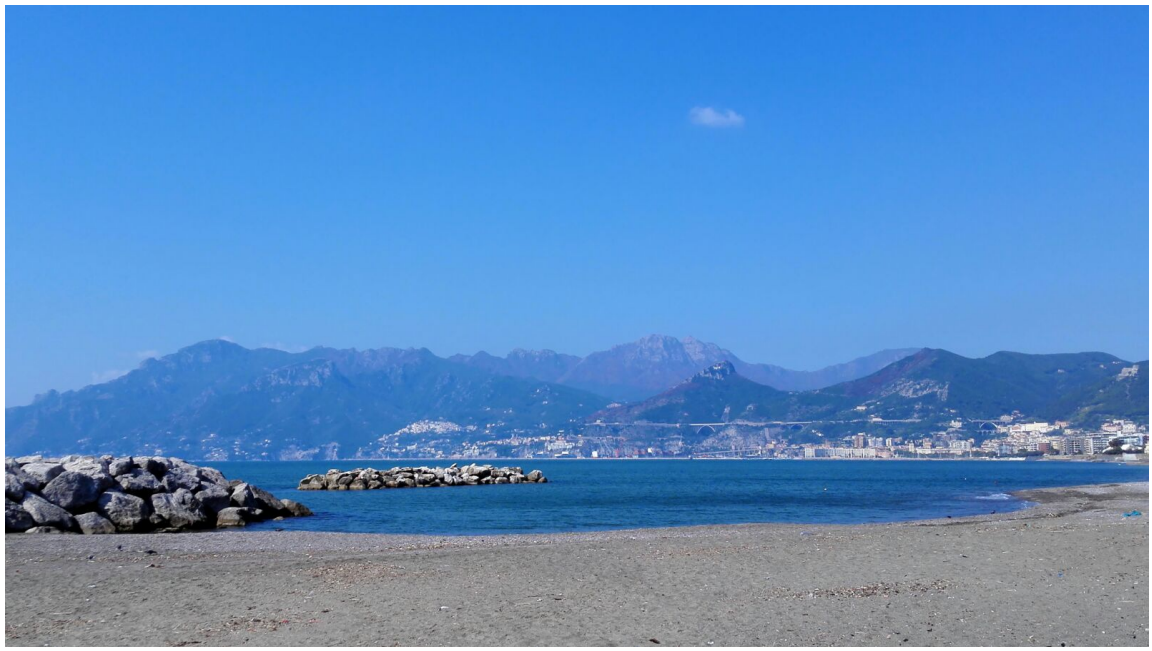
Notes on Elliptic Curves



Dino Festi

April 9, 2026

Contents

Acknowledgments

These notes have originally and gradually been written to serve several courses about elliptic curves that I held at the Nesin Math Village in Şirince, Turkey. The first thanks therefore go to Ali Nesin and all those who contributed to the organization of the village for the amazing atmosphere and hospitality they never fail to provide.

My relationship with the Math Village only started thanks to Pınar Kılıçer, who first brought me there. I will always be grateful to her for showing me such an amazing place.

The courses I held have been often scheduled in combination with other related ones. I am grateful to Pınar Kılıçer, Iuliana Ciocanea Teodorescu, Rachel Newton, Elisa Lorenzo Garcia, Davide Cesare Veniani, Elif Saçıkara, and Matteo Paganini for coordinating our courses.

These notes have been used and adjusted also for a course at the Scuola Superiore di Catania, in 2025, taught together with Peter Stevenhagen. I am grateful to Francesco Russo for inviting me and to all the students for their enthusiastic welcome and participation, in particular to Marco Cottone, Giovanni Giacalone, Vincenzo Scarvaglieri, and Salvatore Bennici.

The last edit was due for a spring school at the National Higher School of Mathematics in Algiers, in 2026, taught together with Valerio Talamanca.

Finally, thanks to all the readers who took the time and made the effort to carefully read these notes (or their previous versions), note several mistakes and report them to me. In particular, thanks to Joachim Jäger and Faris Elmikdad for their remarks.

Chapter 1

Complex tori

Historically, elliptic curves appeared in the mathematical literature because they play a role in computing the length of an arc of an ellipsis. So, the first instance of an elliptic curve comes as a complex surface. In this section we focus on elliptic curves defined over $\mathbb{C}$. In this section, we will briefly go through the historical motivation that led to the definition of elliptic curves, introducing elliptic integrals. Following this path, we will introduce complex lattices and introduce complex tori. Finally, using the Weierstrass $\wp$-function, we will see that every complex torus can be written as a plane cubic curve.

1.1 Ellipses and elliptic curves

If one draws an elliptic curve, he will find that it does not look at all like an ellipse. Then why are they called *elliptic curves*? The reason is that they are related to the computation of the arc length of the ellipses. This theory is classical and vast; we will only briefly sketch it outlining the basic links and leaving some more details as exercises. More can be found in [9, Chapter VI] and [11, Section 1].

Let C be the ellipse defined by the equation $\frac{x^2}{a^2} + \frac{y^2}{b^2} = 1$, then one can inquire about the length L of the perimeter of the ellipse and proceed as in the case of the circle. Namely, from the equation of C we can express y in terms of x:

$$y = \pm b\sqrt{1 - \frac{x^2}{a^2}} \, .$$

Using the symmetry of the ellipse, we can restrict our attention to the upper half and so we obtain

$$y = f(x) := b\sqrt{1 - \frac{x^2}{a^2}} \, .$$

Then using the formula to compute the length of the graph of a function and (again) the symmetry of the ellipse we deduce that

$$L = 2\int_{-a}^{a} \sqrt{1 + f'(x)}\mathrm{d}x = 4\int_{0}^{a} \sqrt{\frac{1 + \frac{b^2 - a^2}{a^2}\frac{x^2}{a^2}}{1 - \frac{x^2}{a^2}}}\mathrm{d}x \, .$$

Assuming $a > b$, we set $k^2 = (a^2 - b^2)/a^2$, and we also perform the change of variables $t := x/a$, obtaining the following equality:

$$L = 4\int_0^1 \sqrt{\frac{1-k^2t^2}{1-t^2}}\mathrm{d}t \ ,$$

called the *Jacobi algebraic form of a complete elliptic integral (of the second type)*. This integral is not path-independent, because the square-root is not single valued. In order to make it well-defined we have to make branch cuts between the zeros and the poles of the integrating function, that is, between the points $z = \pm 1, \pm 1/k$. Then the integral will be path independent in the complement of the branch cuts. As the square-root is double-valued, we have to take two copies of $\mathbb{P}^1_{\mathbb{C}} = \mathbb{C} \cup \{\infty\}$ and glue them identifying the branch cuts. What we get is a torus, that is, as we will see later, an elliptic curve. So studying the arc length of an ellipse leads to the study of integrals on an elliptic curve.

Remark 1.1.1. Using the substitution $t = sin\theta$ one obtains the quality

$$L = 4a\int_0^{\pi/2} \sqrt{1 - k^2\sin^2\theta}\mathrm{d}\theta \ ,$$

which is equal to the integral

$$L = 4\int_0^{\pi/2} \sqrt{x'(\theta)^2 + y'(\theta)^2}\,\mathrm{d}\theta$$

coming from the parametrization of C given by $(x, y) = (a\cos\theta, b\sin\theta)$.

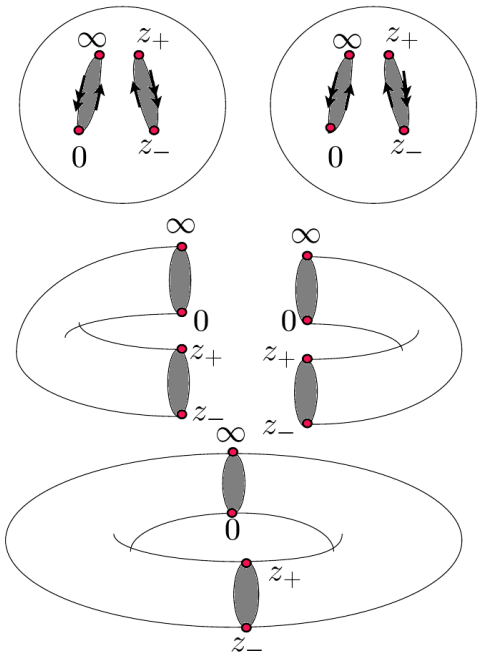


Figure 1.1: Construction of a torus by glueing together two copies of $\mathbb{P}^1_{\mathbb{C}}$ identifying the branch cuts. In the picture the branch cuts are between the points $0, \infty$ and z_+, z_-.

1.2 Lattices and complex tori

Although historically, the above (topological) construction of complex elliptic curve is the original one, it is not the most practical one. Here we will see how to introduce complex tori in a more friendly way.

Definition 1.2.1. We define a *lattice* Λ inside $\mathbb{C}$ to be a discrete subgroup of C containing an $\mathbb{R}$-basis of $\mathbb{C}$, that is, $\Lambda = \{n_1\omega_1 + n_2\omega_2 \mid n_1, n_2 \in \mathbb{Z}\}$ with $\omega_1, \omega_2 \in \mathbb{C}$ such that $\omega_1\mathbb{R} + \omega_2\mathbb{R} = \mathbb{C}$. If $\{\omega_1, \omega_2\}$ is the basis contained inside Λ, we say that Λ is generated by $\{\omega_1, \omega_2\}$, and we write $\Lambda = \langle\omega_1, \omega_2\rangle$.

Example 1.2.2. The ring $\mathbb{Z}[i] \subset \mathbb{C}$ is a lattice. In fact, $\mathbb{Z}[i]$ is the lattice generated by 1 and i, that is, $\mathbb{Z}[i] = \langle 1, i\rangle$.

Example 1.2.3. The ring $\mathbb{Z}[\pi] = \langle 1, \pi\rangle$ is not a lattice, as $1 \cdot \mathbb{R} + \pi \cdot \mathbb{R} = \mathbb{R} \neq \mathbb{C}$.

Definition 1.2.4. A *fundamental parallelogram* for a lattice $\Lambda = \langle\omega_1, \omega_2\rangle$ is a set of the form

$$D = \{a + t_1\omega_1 + t_2\omega_2 \mid 0 \leq t_1, t_2 < 1\}$$

with $a \in \mathbb{C}$. We denote by $\overline{D}$ the closure of D inside $\mathbb{C}$.

Let $\Lambda \subset \mathbb{C}$ be a lattice. Then one can consider the equivalence relation $\sim_\Lambda$ induced by Λ, that is, two points $x, y \in \mathbb{C}$ are in relation $x \sim_\Lambda y$ if and only if $x - y \in \Lambda$.

Definition 1.2.5. Let $\Lambda \subset \mathbb{C}$ be a lattice. We define the *complex torus associated to* Λ the quotient

$$\mathbb{C}/\Lambda := \mathbb{C}/\sim_\Lambda \ .$$

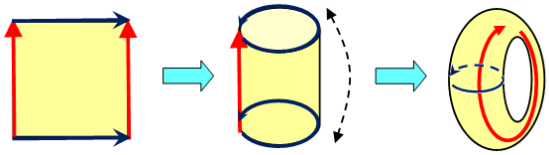


Figure 1.2: A visual explanation of the construction of a torus as a quotient of the complex plane by a lattice.

Remark 1.2.6. Notice that a fundamental domain D of Λ provides a complete set of representative for $\mathbb{C}/\Lambda$.

Definition 1.2.7. Let $\Lambda \subset \mathbb{C}$ be a lattice. The sum over $\mathbb{C}$ induces a commutative group structure onto $\mathbb{C}/\Lambda$: If z_1, z_2 are two elements of $\mathbb{C}/\Lambda$, just consider two representatives for them, say $x_1, x_2 \in \mathbb{C}$ such that $[x_1] = z_1$ and $[x_2] = z_2$, and define

$$z_1 + z_2 = [x_1] + [x_2] := [x_1 + x_2] \ .$$

Then clearly $(\mathbb{C}, +)$ is an abelian group with neutral element $[0]$.

In what follows, with an abuse of notation, we will denote the class of an element $z \in \mathbb{C}$ inside $\mathbb{C}/\Lambda$ simply by z rather then $[z]$.

Definition 1.2.8. Let m be a positive integer. We say that an element $z \in \mathbb{C}/\Lambda$ is an *m-torsion* of $\mathbb{C}/\Lambda$ if $m \cdot z = 0 \in \mathbb{C}/\Lambda$.

Example 1.2.9. The element $[1 + i/2]$ in $\mathbb{C}/\mathbb{Z}[i]$ is a 2-torsion, indeed $2 \cdot [1 + i/2] = [2 + i] = [0]$ as $2 + i \in \mathbb{Z}[i]$.

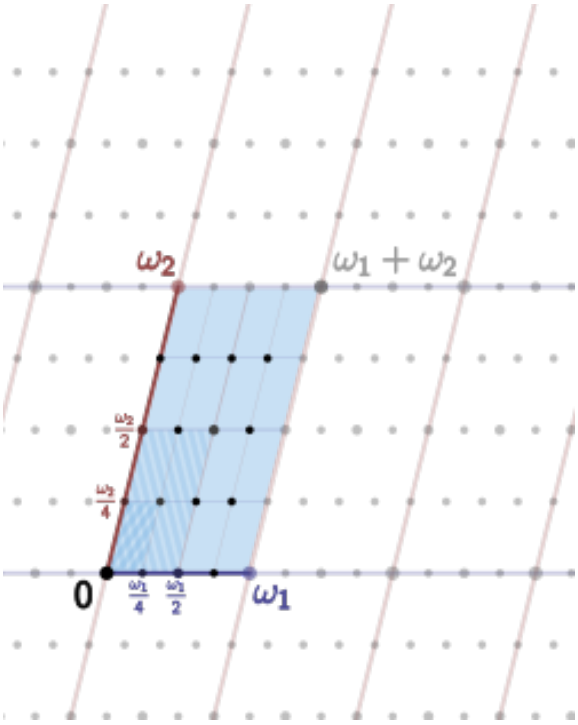


Figure 1.3: A fundamental domain of the lattice generated by ω_1, ω_2. In the picture are also shown the 4-torsion points.

1.3 Elliptic functions

Let $\Lambda \subset \mathbb{C}$ be a lattice. We are now interested in (meromorphic) functions $f \colon \mathbb{C} \to \mathbb{C}$ that 'behave well' with respect to the lattice Λ. Here, 'behaving well' means that the function is invariant by Λ or, equivalently, that a function is Λ-periodic.

Definition 1.3.1. Let $f \colon \mathbb{C} \to \mathbb{C}$ be a meromorphic function. We say that f is an *elliptic function relative to the lattice* Λ if

$$f(z + \omega) = f(z)$$

for every $z \in \mathbb{C}$ and $\omega \in \Lambda$.

Example 1.3.2. Any constant function trivially is an elliptic function. We will see later non-trivial examples of elliptic functions.

Definition 1.3.3. Let $f\colon \mathbb{C} \to \mathbb{C}$ be a meromorphic function and $w \in \mathbb{C}$. We denote the *order of vanishing* and the *residue* of f at w by $\operatorname{ord}_w(f)$ and $\operatorname{res}_w(f)$, respectively.

If f admits a Laurent expansion $\sum_{k\geq n} a_k(z-w)^k$ at w, then

$$\operatorname{ord}_w(f) := n \ ,$$
$$\operatorname{res}_w(f) := a_{-1} \ .$$

We say that z is a *pole* for f if $n < 0$; we say it is a *zero* if $n > 0$.

Definition 1.3.4. Let f be an elliptic function relative to the lattice Λ, and let D be a fundamental domain for Λ. The *order* of f, denoted by $\operatorname{ord}(f)$, is the number of poles of f inside D, counted with multiplicity. In other words, $\operatorname{ord} f := \sum_{\text{poles } w\in D} \operatorname{ord}_w(f)$.

Proposition 1.3.5. *Let $\Lambda \subset \mathbb{C}$ be a lattice and f an elliptic function relative to Λ. The following statements hold:*

(a) if f has no poles then it is constant;

(b) $\sum_{w\in\mathbb{C}/\Lambda} \operatorname{res}_w(f) = 0$;

(c) $\sum_{w\in\mathbb{C}/\Lambda} \operatorname{ord}_w(f) = 0$;

(d) $\sum_{w\in\mathbb{C}/\Lambda} \operatorname{ord}_w(f) w \in \Lambda$;

(e) if f has no zeros then it is constant;

(f) a non-constant elliptic function has order at least 2.

Proof. The prove the first statement it is enough to notice that a meromorphic function with no poles is holomorphic. A holomorphic function is bounded over a compact domain, hence f is bounded over $\overline{D}$, where D is a fundamental domain of Λ. As f is Λ-periodic, it follows that f is bounded over $\mathbb{C}$, hence it is constant.

The statements (b), (c), (d) are applications of the residue theorem, see [9, Theorem 2.2].

Statement (e) follows from (a) and (c). Indeed, if f has no zeros, then, by (c), it has no poles either and hence, by (a), it is constant.

Statement (f) follows from (b) and (a). Indeed, if $\operatorname{ord} f = 0$, then the statement follows from (a). If $\operatorname{ord} f = 1$, it means that f has a single simple pole (that is, a pole of order -1, then by (b) its residue must be 0 implying that f is holomorphic and hence constant by (a). □

Remark 1.3.6. Let f be an elliptic function relative to a lattice Λ. From Proposition 1.3.5.(c) it follows that the order of f is also equal to the numbers of zeros of f, counted with multiplicity. In other words, $\operatorname{ord} f := \sum_{\text{zeros } w\in D} \operatorname{ord}_w(f)$.

Definition 1.3.7. Let $\Lambda \subset \mathbb{C}$ be a lattice. We define $\mathbb{C}(\Lambda)$ to be the set of all the elliptic functions for Λ. The pointwise sum and multiplication give $\mathbb{C}(\Lambda)$ the structure of field and we call $\mathbb{C}(\Lambda)$ the *function field* of Λ.

1.4 The divisor group of a complex torus

Let $\Lambda \subset \mathbb{C}$ be a lattice. We have seen that, given an elliptic function f with respect to Λ, we can consider the zeros and the poles of f inside a fundamental domain of Λ. Moreover, these zeros and poles come with a multiplicity. In order to keep track of the zeros and the poles of a function, together with their multiplicity, we give the following definition.

Definition 1.4.1. We define the *divisor group* of the complex torus $\mathbb{C}/\Lambda$ to be the group of formal linear combinations of elements of $\mathbb{C}/\Lambda$, that is,

$$\mathrm{Div}(\mathbb{C}/\Lambda) := \bigoplus_{w \in \mathbb{C}/\Lambda} \mathbb{Z} \cdot (w) = \left\{ \sum_{w \in \mathbb{C}/\Lambda} n_w(w) \mid n_w \in \mathbb{Z} \ \forall w \text{ and } \ n_w = 0 \ \forall\forall w \right\} .$$

Example 1.4.2. Consider $\Lambda = \mathbb{Z}[i]$. Then the formal sum $(1) - 3(i) + 2(2)$ is a divisor; the formal sum $\sum_{w \in \Lambda}(w)$ is not, because there are infinitely many non-zero coefficients.

Definition 1.4.3. Let $D = \sum n_w(w)$ be a divisor of $\mathbb{C}/\Lambda$. Then we define the *degree* of D as

$$\deg D := \sum n_w \ .$$

Example 1.4.4. $\deg\left((1) - 3(i) + 2(2)\right) = 1 - 3 + 2 = 0$.

Keeping in mind Proposition 1.3.5, we are mostly interested in divisors of degree 0.

Definition 1.4.5. We define the following subgroup of $\mathrm{Div}(\mathbb{C}/\Lambda)$:

$$\mathrm{Div}^0(\mathbb{C}/\Lambda) = \{D \in \mathrm{Div}(\mathbb{C}/\Lambda) \ : \ \deg D = 0\} \ .$$

The following definition makes the connection between zero and poles of an elliptic function and divisors finally clear.

Definition 1.4.6. Let $f \in \mathbb{C}(\Lambda)^*$ be a non-zero elliptic functin with respect to Λ. We define *the divisor of* f as

$$\mathrm{div}(f) := \sum_{w \in \mathbb{C}/\Lambda} \mathrm{ord}_w(f)(w) \ .$$

Lemma 1.4.7. *The map*

$$\mathrm{div}\colon \mathbb{C}(\Lambda)^* \to \mathrm{Div}^0(\mathbb{C}/\Lambda) \ , f \mapsto \mathrm{div}\, f$$

is a group homomorphism.

Proof. Exercise. □

Definition 1.4.8. We also define a map in the other direction, namely, *the summation map*

$$\mathrm{sum}\colon \ \mathrm{Div}^0(\mathbb{C}/\Lambda) \to \mathbb{C}/\Lambda \ , \ \sum n_w(w) \to \sum n_w w \mod \Lambda \ .$$

Example 1.4.9. Again, if we consider $D = (1) - 3(i) + 2(2) \in \mathbb{Z}[i]$, then $\mathrm{sum}\, D = 1 - 3i + 2 \cdot 4 = 5 - 3i = 0 \mod \mathbb{Z}[i]$.

Lemma 1.4.10. *The summation map is a well defined group homomorphism.*

Proof. Exercise. □

Using these definitions, we can summarize the results about zeros and poles of elliptic functions as follows.

Theorem 1.4.11. *The sequence is exact.*

$$1 \longrightarrow \mathbb{C}^* \longrightarrow \mathbb{C}(\Lambda)^* \xrightarrow{\text{div}} \text{Div}^0(\mathbb{C}/\Lambda) \xrightarrow{\text{sum}} \mathbb{C}/\Lambda \longrightarrow 0 \tag{1.1}$$

Proof. Exercise. □

1.5 The Weierstrass $\wp$-function

In this section we give the most important example of non-constant elliptic function for a lattice Λ, the Weierstrass $\wp$-function.

Definition 1.5.1. Let $\Lambda \subset \mathbb{C}$ be a lattice. The *Weierstrass $\wp$-function (relative to Λ)* is defined by the series

$$\wp(z;\Lambda) := \frac{1}{z^2} + \sum_{\substack{w\in\Lambda \\ w\neq 0}} \frac{1}{(z-w)^2} - \frac{1}{w^2}.$$

Lemma 1.5.2. *The first derivative of $\wp$ is given by*

$$\wp'(z) = -2\sum_{w\in\Lambda} \frac{1}{(z-w)^3}.$$

Proof. By explicit computation using the definition of $\wp$. □

We then provide some basic properties of $\wp$.

Proposition 1.5.3. *Let $\Lambda \subset \mathbb{C}$ be a lattice and let $\wp = \wp(z;\Lambda)$ the Weierstrass $\wp$-function associated to it. Then $\wp$:*

(a) converges uniformly on every compact subset of $\mathbb{C} \setminus \Lambda$,

(b) is an even elliptic function having a double pole with residue 0 at $z = 0$ (and so at every lattice point) and no other poles,

(c) has derivative $\wp'$, which is an odd elliptic function.

Proof. We report Silverman's proof of [9, Theorem VI.3.1]. For the first two statements we just refer to to [9, Theorem VI.3.1.(b)].

To prove the last statement, just notice that

$$\wp'(z) := -2\sum_{w\in\Lambda} \frac{1}{(z-w)^3} = -2\sum_{w\in\Lambda} \frac{1}{(z+w)^3}$$

as Λ is a group inside $\mathbb{C}$. Hence

$$\wp'(-z) := -2\sum_{w\in\Lambda}\frac{1}{(-z+w)^3} = 2\sum_{w\in\Lambda}\frac{1}{(z-w)^3} = -\wp'(z)\ .$$

□

The following theorem shows why $\wp$ is the most important elliptic function for a lattice Λ.

Theorem 1.5.4. *Let Λ be a lattice and let $\wp = \wp(z;\Lambda)$ the Weierstrass $\wp$-function associated to it. Then*

$$\mathbb{C}(\Lambda) = \mathbb{C}(\wp, \wp')\ .$$

Proof. For a proof, see [9, Theorem VI.3.2]. □

In order to state the next results, we need a family of auxiliary functions.

Definition 1.5.5. Let $\Lambda \subset \mathbb{C}$ be a lattice. The *Eisenstein series of weight $2k$ related to Λ* is the series

$$G_{2k}(\Lambda) := \sum_{\substack{w\in\Lambda\\ w\neq 0}} w^{-2k}.$$

We will simply write G_{2k} if the lattice is fixed or clear from the context.

Lemma 1.5.6. *The series $G_{2k}(\Lambda)$ is absolutely convergent for $k > 1$.*

Proof. See [9, Theorem VI.3.1.(a)]. □

Lemma 1.5.7. *For every $k \geq 4$, the series G_{2k} can be computed recursively from G_4 and G_6.*

Proof. [11, Exercise 2.20]. □

Theorem 1.5.8. *The following statements hold:*

(a) the Laurent series for $\wp(z)$ at $z = 0$ is given by

$$\wp(z) = z^{-2} + \sum_{n=1}^{\infty}(2n+1)G_{2n+2}z^{2n};$$

(b) for all $z \in \mathbb{C}$ with $z \notin \Delta$, we have that

$$\wp'(z)^2 = 4\wp(z)^3 - 60G_4\wp(z) - 140G_6.$$

Proof. (a) Recall that the Laurent expansion of $\frac{1}{1-z}$ at 1 for $|z| < 1$ is $\sum_{k=0}^{\infty} z^n$. By derivation, it follows that

$$\frac{1}{(1-z)^2} = \sum_{k=1}^{\infty} kz^{k-1}$$

and hence

$$\frac{1}{(1-z)^2} - 1 = \sum_{k=1}^{\infty}(k+1)z^k.$$

Write $\wp(z)$ as

$$z^{-2} + \sum_{\substack{w\in\Lambda\\ w\neq 0}} \frac{1}{(z-w)^2} - \frac{1}{w^2} = z^{-2} + \sum_{\substack{w\in\Lambda\\ w\neq 0}} w^{-2}[(1-z/w)^{-2} - 1].$$

As we are computing the Laurent series of $\wp$ at $z = 0$ we may assume that $|z| < |w|$ for every $w \in \Lambda$, and hence we can apply the Laurent expansion computed before, getting

$$\begin{aligned}\wp(z) &= z^{-2} + \sum_{\substack{w\in\Lambda\\ w\neq 0}} \sum_{k=1}^{\infty} (k+1)\frac{z^k}{w^{k+2}} = \\ &= z^{-2} + \sum_{k=1}^{\infty} (k+1) z^k \sum_{\substack{w\in\Lambda\\ w\neq 0}} w^{-(k+2)} = \\ &= z^{-2} + \sum_{n=1}^{\infty} (2n+1) z^{2n} G_{2n+2},\end{aligned}$$

where $k = 2n$; notice that $\sum_{\substack{w\in\Lambda\\ w\neq 0}} w^{-(k+2)} = 0$ for k odd. This proves the statement.

(b) Consider the first terms of the following Laurent expansions:

$$\begin{aligned}\wp(z) &= z^{-2} + 3G_4 z^2 + \cdots \\ \wp(z)^3 &= z^{-6} + 9G_4 z^{-2} + 15G_6 + \cdots \\ \wp'(z)^2 &= 4z^{-6} - 24G_4 z^{-2} - 80G_6 + \cdots .\end{aligned}$$

It follows that the function

$$f(z) = \wp'(z)^2 - 4\wp(z)^3 + 60G_4\wp(z) + 140G_6$$

is holomorphic around $z = 0$ and it vanishes at $z = 0$. As f is a combination of functions that are elliptic for Λ, it is also elliptic for Λ. Then, by Proposition 1.5.3.i), it follows that $f(z)$ is the constantly 0, proving the statement.

□

Corollary 1.5.9. *Let Λ be the lattice $\langle \omega_1, \omega_2\rangle$ and set $\omega_3 := \omega_1 + \omega_2$.*
The divisor of $\wp(\Lambda)$ is

$$\operatorname{div}(\wp) = -2(0) + (\omega) + (-\omega)$$

for some ω in the fundamental domain of Λ.
The divisor of $\wp'(\Lambda)$ is

$$\operatorname{div}(\wp') = -3(0) + (\omega_1/2) + (\omega_2/2) + (\omega_3/2) .$$

Proof. Exercise. □

Definition 1.5.10. It is customary to set

$$\begin{aligned} g_2 = g_2(\Lambda) &:= 60G_4, \\ g_3 = g_3(\Lambda) &:= 140G_6.\end{aligned}$$

Remark 1.5.11. Using (1.5.10), the relation in Theorem 1.5.8 reads

$$\wp'(z)^2 = 4\wp(z)^3 - g_2\wp(z) - g_3.$$

In other words, $\wp$ and $\wp'$ satisfy the equation

$$y^2 = 4x^3 - g_2x - g_3 \ ,$$

which is *almost* in very short Weierstrass form. To reduce it in very short Weierstrass form, we multiply both sides by 16, obtaining

$$4^2y^2 = 4^3x^3 - 4^2g_2x - 4^2g_3 \ ,$$

and then we apply the following change of variables:

$$\begin{cases} x' = 4x \\ y' = 4y \end{cases} \ ,$$

obtaining the equation

$$y^2 = x^3 - 4g_2x - 16g_3 \ ,$$

which is indeed in very short Weierstrass form.

Definition 1.5.12. Let $\Lambda \subset \mathbb{C}$ be a lattice and g_2, g_3 the quantities associated to it defined in Definition 1.5.10. We define the curve $E = E(\Lambda) \subset \mathbb{A}^2$ as the curve given by

$$E(\Lambda)\colon y^2 = x^3 - 4g_2x - 16g_3 \subset \mathbb{A}^2(x, y).$$

With an abuse of notation, we will use $E(\Lambda)$ also to denote its projective closure inside $\mathbb{P}^2$.

Remark 1.5.13. The projective closure of $E(\Lambda)$ inside $\mathbb{P}^2$ is given by

$$y^2z = x^3 - 4g_2xz^2 - 16g_3z^3 \subset \mathbb{P}^2(x, y, z) \ .$$

Lemma 1.5.14. *The curve $E(\Lambda)$ is smooth.*

Proof. To show that E is an elliptic curve it is enough to show that $\Delta(E) \neq 0$ or, equivalently, that the equation

$$x^3 - 4g_2x - 16g_3 = 0 \tag{1.2}$$

has no repeated roots. Notice that the equation (1.2) has the same roots of the equation

$$f(x) := 4x^3 - g_2x - g_3 = 0.$$

So we have to show that $f(x)$ has no repeated roots.

In order to do so, let $\{w_1, w_2\}$ a basis for Λ, and define $w_3 := w_1 + w_2 \in \Lambda$ As $\wp'(z)$ is an odd elliptic function,

$$-\wp'(-w_i/2) = \wp'(w_i/2) = \wp'(w_i/2 - w_i) = \wp'(-w_i/2),$$

from which it follows that $\wp'(w_i/2) = 0$ for $i = 1, 2, 3$. By Theorem 1.5.8 it follows that $\wp(w_i/2), i = 1, 2, 3$ are the three roots of f. We are left to show that they are distinct.

As $\wp$ is an even elliptic function, so is the function $\psi_i(z) := \wp(z) - \wp(w_i/2)$, for every $i = 1, 2, 3$. As $\wp'(w_i/2)$ is zero, then $w_i/2$ is a zero of order at least 2. Notice that $\psi_i(z)$ has exactly one pole of order 2 (inside a fundamental domain) at $z = 0$ (as $\wp$ does) and so $w_i/2$ has order exactly 2 and it is the only zero. This shows that $\wp(w_i/2) \neq \wp(w_j/2)$ for $i \neq j$, proving the statement. □

Theorem 1.5.15. *Let $\Lambda = \langle \omega_1, \omega_2 \rangle \subset \mathbb{C}$ be a lattice of $\mathbb{C}$ with generators ω_1, ω_2, and let $E(\Lambda)$ be the curve associated to Λ. Then the map*

$$\begin{aligned} \phi\colon \mathbb{C}/\Lambda &\to E(\Lambda) \\ z &\mapsto (\wp(z) : \wp'(z)/2 : 1) \\ 0 &\mapsto (0:1:0) = O \end{aligned}$$

is an isomorphism of Riemann surfaces.

The inverse is given by

$$\begin{aligned} \psi\colon E(\Lambda) &\to \mathbb{C}/\Lambda \\ P &\mapsto \int_O^P \frac{dx}{y} \mod \Lambda\,. \end{aligned}$$

Proof. See [9, Propositions VI.3.6(b), VI.5.2]. □

Remark 1.5.16. The isomorphism in Theorem 1.5.15 can be used to endow the set of points of $E(\Lambda)$ with a group structure. In fact, later we will see that the $E(\Lambda)$ admits a geometric construction of this group structure.

Chapter 2

Isogenies of complex tori

In the previous chapter we have seen that, given a complex lattice $\Lambda \subset \mathbb{C}$, we can construct the complex torus $\mathbb{C}/\Lambda$, which is Riemann surface also endowed with a group structure (see §1.2). Then, the next natural step is to study maps between complex tori that also preserve the group structure.

2.1 Isogenies

Let $\Lambda_1, \Lambda_2 \subset \mathbb{C}$ be two lattices and consider the associated complex tori $T_1 := \mathbb{C}/\Lambda_1$ and $T_2 := \mathbb{C}/\Lambda_2$.

Definition 2.1.1. An *isogeny* between T_1 and T_2 is a morphism of Riemann surfaces $T_1 \to T_2$ that preserves the group structure.

We denote by $\mathrm{Hom}(T_1, T_2)$ the group of isogenies between T_1 and T_2.

We denote by $\mathrm{End}(T_1) := \mathrm{Hom}(T_1, T_1)$ the endomorphism ring of T_1.

Remark 2.1.2. Let $\phi\colon T_1 \to T_2$ be an isogeny. If ϕ is constant, then the requirement to be a group homomorphism forces $\phi = 0$. Hence, 0 is the only constant isogeny.

Later we will see that a non-constant isogeny is surjective (Corollary 2.1.6).

The first thing to notice is that, every isogeny $\psi\colon T_1 \to T_2$ comes from a map $\phi\colon \mathbb{C} \to \mathbb{C}$ sending Λ_1 into Λ_2, as shown by the following lemma.

Lemma 2.1.3. *Let T_1, T_2 be defined as above and, for $i = 1, 2$, let $\pi\colon \mathbb{C} \to T_i$ denote the canonical projection. Let $\psi\colon T_1 \to T_2$ be an isogeny. Then there exists a continuous map $\phi\colon \mathbb{C} \to \mathbb{C}$ such that the following diagram commute. The map ϕ is unique up to an additive constant $c \in \Lambda_2$.*

$$\begin{array}{ccc} \mathbb{C} & \xrightarrow{\phi} & \mathbb{C} \\ \downarrow{\scriptstyle \pi_1} & & \downarrow{\scriptstyle \pi_2} \\ T_1 & \xrightarrow{\psi} & T_2 \end{array} \tag{2.1}$$

Proof. As ψ is an isogeny, it is a group homomorphism and therefore $\psi(0) = 0$. Define $\phi(0) := 0$ and notice that the diagram commutes in 0.

Take an arbitrary $x \in \mathbb{C}$ and let $z \in T_1$ be its image in T_1. To define $\phi(x)$, consider a path γ in $\mathbb{C}$ starting from 0 and ending in x. The path γ induces the path $\overline{\gamma} := \psi \circ \pi_1 \circ \gamma$ inside T_2. As

$\pi_1 \colon \mathbb{C} \to T_1$ is a covering map, we can lift $\overline{\gamma}$ to a path γ_2 inside $\mathbb{C}$. We define $\phi(z)$ as the end point of γ_2.

As $\mathbb{C}$ is simply connected, the definition of $\phi(z)$ is independent of the choice of γ. The continuity of γ_2 follows from the construction.

Finally, to see that ϕ is unique up to a constant $c \in \Lambda_2$ assume that ϕ' is another continuous map making the diagram commute. It means that, for every $x \in \mathbb{C}$ one has

$$\pi_2 \circ \phi'(x) = \psi \circ \pi_1(x) = \pi_2 \circ \phi(x) \ ,$$

from which it follows that $\pi_2 \circ \phi' - \pi_2 \circ \phi = \pi_2 \circ (\phi' - \phi) = 0 \colon \mathbb{C} \to \Lambda_2$. As $\Lambda_2 \subset \mathbb{C}$ is discrete, it follows that $\phi' - \phi$ is a constant c and therefore, in order to have the zero map from $\mathbb{C}$ to $T_2 = \mathbb{C}/\Lambda_2$ it must be $c \in \Lambda_2$. □

The above lemma shows that every isogeny comes from a continuous map $\mathbb{C} \to \mathbb{C}$, but even more can be said about these lifts.

Proposition 2.1.4. *Let T_1, T_2 be defined as above and, for $i = 1, 2$, let $\pi \colon \mathbb{C} \to T_i$ denote the canonical projection. Let $\psi \colon T_1 \to T_2$ be an isogeny. Then there exists an $\alpha \in \mathbb{C}$ such that the multiplication by α*

$$\phi_\alpha \colon \mathbb{C} \to \mathbb{C} \ , x \mapsto \alpha x$$

makes diagram (2.1) commute. In other words, ϕ_α is the lift of ψ to $\mathbb{C}$.

Proof. Recalling Lemma 2.1.3, let $\phi \colon \mathbb{C} \to \mathbb{C}$ be the lift of ψ satisfying $\phi(0) = 0$. For every $\lambda_1 \in \Lambda_1$, using the commutativity of the diagram (2.1), one can see that $\phi(x) \equiv \phi(x + \lambda_1) \mod \Lambda_2$ for every $x \in \mathbb{C}$. This means that, for every $\lambda_1 \in \Lambda_1$ and $x \in \mathbb{C}$ we have that $\phi(x) - \phi(x + \lambda_1) \in \Lambda_2$. As Λ_2 is discrete and $\phi(x) - \phi(x + \lambda_1)$ is continuous in x, it follows that it for every $\lambda_1 \in \Lambda_1$ the function $\phi(x) - \phi(x + \lambda_1)$ is a constant $\lambda_2 \in \Lambda_2$. Hence, the derivative $\phi'(x)$ is continuous elliptic function with respect to Λ_1, and therefore it is also constant, say $\phi'(x) =: \alpha \in \mathbb{C}$. We deduce then that $\phi(x) = \alpha x + \beta$, for some $\beta \in \mathbb{C}$. As $\phi(0) = 0$, it follows that $\beta = 0$, concluding the proof. □

Corollary 2.1.5. *Let T_1, T_2 be defined as above and, for $i = 1, 2$, let $\pi \colon \mathbb{C} \to T_i$ denote the canonical projection. Let $\psi \colon T_1 \to T_2$ be an isogeny. Let $\phi_\alpha \colon \mathbb{C} \to \mathbb{C} \ , x \mapsto \alpha x$ be a lift of ψ. Then $\alpha\Lambda_1 \subseteq \Lambda_2$.*

Proof. Indeed, if $\lambda_1 \in \Lambda_1$, then

$$\psi_2(\alpha\lambda_1) = \psi_2 \circ \phi_\alpha(\lambda_1) = \phi \circ \pi_1(\lambda_1) = \phi(0) = 0 \ ,$$

that is, $\alpha\lambda_1 \in \Lambda_2$, concluding the proof. □

Corollary 2.1.6. *Let $\phi \colon T_1 \to T_2$ be a non-constant isogeny. Then ϕ is a surjective group homomorphism.*

Proof. By definition, ϕ is a group homomorphism. By Proposition 2.1.4, there exists an $\alpha \in \mathbb{C}^*$ such that $\phi(z) = \alpha z$. Therefore, any element $w \in T_2$ is the image of w/α. □

We have seen that every isogeny of complex tori comes from a multiplication by an element α such that $\alpha\Lambda_1 \subseteq \Lambda_2$. The converse is also true.

Proposition 2.1.7. *Let $\Lambda_1, \Lambda_2 \subset \mathbb{C}$ be two complex lattices and let T_1, T_2 the associated complex tori. If $\alpha \in \mathbb{C}$ is such that $\alpha\Lambda_1 \subset \Lambda_2$, then the multiplication by α induces the isogeny*

$$\psi_\alpha \colon T_1 \to T_2, z \mapsto \alpha z \ .$$

Proof. Just notice that ψ_α is well defined, continuous, and respects the group structures of T_1 and T_2. □

Remark 2.1.8. The above results show that $\mathrm{Hom}(T_1, T_2)$ is in bijection with the set $\{\alpha \in \mathbb{C} \ : \alpha\Lambda_1 \subset \Lambda_2\}$.

Definition 2.1.9. We say that two tori $T_1 = \mathbb{C}/\Lambda_1, T_2 = \mathbb{C}/\Lambda_2$ are are *isogenous* if there exists a non-zero isogeny between them. Equivalently, if there exists an $\alpha \in \mathbb{C}^*$ such that $\alpha\Lambda_1 \subseteq \Lambda_2$ (or viceversa).

If $\psi \colon T_1 \to T_2$ is an isogeny induced by $\alpha \in \mathbb{C}^*$, we define the *degree* of ψ as the index $[\Lambda_2 : \alpha\Lambda_1]$.

Lemma 2.1.10. *Let $\phi_\alpha \colon T_1 \to T_2$ be an isogeny of degree k. Then the following statements hold:*

1. $k\Lambda_2 \subset \alpha\Lambda_1 \subset \Lambda_2$,
2. $\frac{k}{\alpha}\Lambda_2 \subset \Lambda_1$.

Proof. By definition of an isogeny we know that $\alpha\Lambda_1 \subset \Lambda_2$; by definition of the degree of an isogeny we know that $k = [\Lambda_2 : \alpha\Lambda_1]$ and hence $k\Lambda_2 \subseteq \alpha\Lambda_1$, proving the first statement.

The second statement follows directly from dividing $k\Lambda_2 \subseteq \alpha\Lambda_1$ by α. □

Definition 2.1.11. If $\phi \colon T_1 \to T_2$ is an isogeny of degree k, induced by the multiplication by $\alpha \in \mathbb{C}^*$, we define its *dual* isogeny, denoted by $\hat{\phi}$, as the isogeny

$$\hat{\phi} \colon T_2 \to T_1 \ , \quad [z] \mapsto \left[\frac{k}{\alpha} z\right] .$$

Lemma 2.1.12. *If $\phi \colon \Lambda_1 \to \Lambda_2$ is an isogeny of degree k and $\hat{\phi}$ is its dual, then their composition (in any order) is the multiplication by k.*

Proof. It is clear as the isogenies are just multiplication by the elements α and $\hat{\alpha} = k/\alpha$. □

Corollary 2.1.13. *Being isogenous is an equivalence relation.*

Proof. Reflexivity is clear: $\Lambda_1 \subseteq 1\Lambda_1$. Transitivity is also elementary: if $\alpha\Lambda_1 \subset \Lambda_2$ and $\beta\Lambda_2 \subset \Lambda_3$, then $\beta\alpha\Lambda_1 \subset \Lambda_3$. Reflexivity comes from Lemma 2.1.10: if $\alpha\Lambda_1 \subset \Lambda_2$, then $\hat{\alpha}\Lambda_2 \subset \Lambda_1$. □

Definition 2.1.14. Two lattices $\Lambda_1, \Lambda_2 \subset \mathbb{C}$ are called *isomorphic* or, equivalently, *homotetic*, if there exists an $\alpha \in \mathbb{C}$ such that $\alpha\Lambda_1 = \Lambda_2$.

We say that two complex tori are *isomorphic* if there is an isogeny of degree 1 between them.

Remark 2.1.15. Notice that two lattices Λ_1, Λ_2 are isomorphic if and only if $\mathbb{C}/\Lambda_1$ and $\mathbb{C}/\Lambda_2$ are isomorphic.

At this point, there are three natural questions that may catch our interest.

Question 2.1.16. Given a complex torus T, describe its endomorphism ring $\mathrm{End}(T)$.

Question 2.1.17. Given the tori T_1, T_2, determine whether T_1 and T_2 are isomorphic.

Question 2.1.18. Given the tori T_1, T_2, determine whether T_1 and T_2 are isogenous.

2.2 The endomorphism ring

Let $T = \mathbb{C}/\Lambda$ be a complex torus, with $\Lambda = \langle \omega_1, \omega_2 \rangle$.

Definition 2.2.1. Given $m \in \mathbb{Z}$, one can always consider the endomorphism induced by the multiplication by m, denoted by

$$[m] \colon T \to T,\ z \mapsto mz\ .$$

Definition 2.2.2. For $m \in \mathbb{Z}$, we define the *m-torsion points* of T as

$$T[m] := \ker[m]\ .$$

Lemma 2.2.3. *For $0 \neq m \in \mathbb{Z}$ one has*

$$T[m] = \left\{ \frac{a_1}{m}\omega_1 + \frac{a_2}{m}\omega_2 \mid a_1, a_2 \in \{0, \dots, m-1\} \right\} \cong \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}\ .$$

Proof. Exercise. □

Remark 2.2.4. Notice that the degree of $[m]$ is $[\Lambda : m\Lambda] = m^2$ which is also equal to the cardinality of $\ker[m]$.

Proposition 2.2.5. *The map $\mathbb{Z} \to \mathrm{End}(T), m \mapsto [m]$ is a ring embedding.*

Proof. Just notice that for $m \neq 0$, one has $\ker[m] \cong \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$ (by Lemma 2.2.3) and hence $\ker[m] \neq T$, meaning that $[m] \neq 0$. □

In fact, for most tori the endomorphism ring is isomoprhic to $\mathbb{Z}$. Cases of tori with a bigger endomorphism ring are special. The most notable examples are below.

Example 2.2.6. Let T_i be the torus $\mathbb{C}/\mathbb{Z}[i]$, where i is the imaginary unit. Then the multiplication by i gives the endomorphism

$$[i] \colon T_i \to T_i\ ,\ z \mapsto iz\ .$$

It turns out that $\mathrm{End}(T_i) \cong \mathbb{Z}[i]$.

Example 2.2.7. Analogously, let T_ζ be the torus $\mathbb{C}/\mathbb{Z}[\zeta]$, where ζ denotes a primitive third root of unity. Then the multiplication by ζ gives the endomorphism

$$[\zeta] \colon T_\zeta \to T_\zeta\ ,\ z \mapsto \zeta z$$

and it turns out that $\mathrm{End}(T_\zeta) \cong \mathbb{Z}[\zeta]$.

These examples motivate the following definition.

Definition 2.2.8 (Complex multiplication)**.** We say that a torus has *complex multiplication* if its endomorphism ring strictly contains $\mathbb{Z}$.

Among the endomorphisms of T, the invertible ones are worth mentioning.

Definition 2.2.9. An *automorphism* of T is an invertible endomorphism of T. The set of automprhisms of T is denoted by $\mathrm{Aut}(T)$.

Lemma 2.2.10. *The set $\mathrm{Aut}(T)$ endowed with the composition is a group.*

Proof. Exercise. □

Example 2.2.11. If $\mathrm{End}(T) \cong \mathbb{Z}$ then, clearly, $\mathrm{Aut}(T) = \{[\pm 1]\}$.
If $\mathrm{End}(T) \cong \mathbb{Z}[i]$ (see Example 2.2.6) then, $\mathrm{Aut}(T) = \{[\pm 1], [\pm i]\}$.
If $\mathrm{End}(T) \cong \mathbb{Z}[\zeta]$ (see Example 2.2.7) then, $\mathrm{Aut}(T) = \{[(1+\zeta)^k] \ : \ k \in \{0, 1, \ldots, 5\}\}$.

In fact, more can be said about about the endomorphisms and automorphisms of complex tori.

Theorem 2.2.12. *The endomorphism ring of T is isomorphic to either $\mathbb{Z}$ or to an order of an imaginary quadratic extension of $\mathbb{Q}$.*
The automorphism group of T is isomorphic to the group of units of that order.

Proof. See [9, Corollary III.9.4]. □

Remark 2.2.13. Recall that an *imaginary quadratic extension* of $\mathbb{Q}$ is an extension K of $\mathbb{Q}$ of the form $K = \mathbb{Q}(\sqrt{-d})$ with $d \in \mathbb{N}$. An *order* $\mathcal{O}$ in K is a subring of K that is finitely generated as $\mathbb{Z}$-module and such that $\mathcal{O} \otimes \mathbb{Q} = K$.

2.3 The special linear group

In order to give a full answer to questions 2.1.16 and 2.1.17 we need to introduce an action on the upper half of the complex plane.

Definition 2.3.1. We define the *upper-half plane* to be the region $\mathbb{H}$ of $\mathbb{C}$ defined by

$$\mathbb{H} := \{z \in \mathbb{C} \mid \Im(z) > 0\}.$$

Definition 2.3.2. We define the *general linear group of* $\mathbb{C}$ to be the group

$$\mathrm{GL}_2(\mathbb{Z}) := \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \;\middle|\; a, b, c, d \in \mathbb{Z},\ ad - bc = \pm 1 \right\}.$$

We define the *special linear group* of $\mathbb{C}$ to be the normal subgroup of $\mathrm{GL}_2(\mathbb{Z})$ defined by

$$\mathrm{SL}_2(\mathbb{Z}) := \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \;\middle|\; a, b, c, d \in \mathbb{Z},\ ad - bc = 1 \right\}.$$

Sometimes, we might denote $\mathrm{SL}_2(\mathbb{Z})$ by simply Γ.

Define $T := \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, S := \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})$.

Lemma 2.3.3. *The group Γ is generated by S and T.*

Proof. Just notice that $S^2 = -\mathrm{Id}$ and then follow the proof of [5, Proposition III.1.4]. □

We define an action of the group $\mathrm{SL}_2(\mathbb{Z})$ on $\mathbb{P}^1_{\mathbb{C}}$ in the following way. For every $z \in \mathbb{H}$ and $g = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})$ we define:

$$gz := \frac{az + b}{cz + d},$$

$$g\infty := \frac{a}{c},$$

where $z := (z : 1)$ and $\infty := (1 : 0)$.

Lemma 2.3.4. *The action of* $\mathrm{SL}_2(\mathbb{Z})$ *on* $\mathbb{P}^1_{\mathbb{C}}$ *is well defined. Furthermore, it preserves* $\mathbb{H}$.

Proof. Exercise. □

As $\mathbb{H}$ is preserved by the action of $\Gamma = \mathrm{SL}_2(\mathbb{Z})$, we can consider the action induced on it, and hence consider the quotient $\mathbb{H}/\Gamma$. Let $\mathcal{F}$ be the region of the upper-half plane defined as

$$\mathcal{F} := \{z \in \mathbb{H} \ : \ |z| \geq 1 \text{ and } -\frac{1}{2} \leq \Re(z) < \frac{1}{2}\}.$$

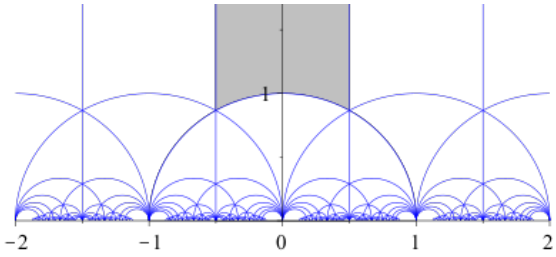


Figure 2.1: A visual rendition of the region $\mathcal{F}$ (the one in grey). The boundaries of other fundamental domains are also shown (the blue curves).

Lemma 2.3.5. *The region* $\mathcal{F}$ *is a fundamental domain of* $\mathbb{H}/\Gamma$.

Proof. Let z be any point in $\mathbb{H}$. Use a power T^j of T to move z to a point z' inside the strip $-\frac{1}{2} \leq \Re(z) < \frac{1}{2}$. If it is outside the unit circle, then it is in $\mathcal{F}$; otherwise use S to move the point outside the unit circle, and the again a power T^k to move it inside the strip. Go on like this until you get a point in $\mathcal{F}$. We leave the details of the proof as an exercise. (Note that they can be found in [5, Proposition 1]) □

2.4 The j-function

Let $\Lambda \subset \mathbb{C}$ be a lattice and let $T = \mathbb{C}/\Lambda$ be the associated torus, and recall the Eisenstein series associated to Λ, (Definition 1.5.5) and the quantities $g_2(\Lambda), g_3(\Lambda)$ (Definition 1.5.10).

Definition 2.4.1. We define the *discriminant* of Λ as the quantity

$$\Delta(\Lambda) := g_2(\Lambda)^3 - 27g_3(\Lambda)^2$$

and the *j-invariant* of Λ as the quantity

$$j(\Lambda) := 1728\frac{g_2(\Lambda)^3}{\Delta(\Lambda)}\ .$$

Remark 2.4.2. Notice that $\Delta(\Lambda) := g_2(\Lambda)^3 - 27g_3(\Lambda)^2$ is the discriminant of the equation $4x^3 - g_2x - g_3 = 0$, cf. Theorem 1.5.8(b).

Noting that two complex tori are isomorphic if and only if the associated lattices are homothetic, we are now ready to answer Question 2.1.17 using the j-invariant.

Lemma 2.4.3. *Two complex lattices are homothetic if and only if they have the same j-invariant.*

Proof. Let Λ_1 and Λ_2 two complex lattices, and assume they are homothetic, that is, there is a $\alpha \in \mathbb{C}$ such that $\alpha\Lambda_1 = \Lambda_2$. Then $G_{2k}(\Lambda_2) = \alpha^{-2k} G_{2k}(\Lambda_1)$. From this it immediately follows that $j(\Lambda_2) = j(\Lambda_1)$.

On the other hand, if two lattices Λ_1, Λ_2 have the same j-invariant, it follows that

$$\frac{g_2(\Lambda_1)^3}{g_2(\Lambda_1)^3 - 27g_3(\Lambda_1)^2} = \frac{g_2(\Lambda_2)^3}{g_2(\Lambda_2)^3 - 27g_3(\Lambda_2)^2}$$

and hence there exists $\alpha \in \mathbb{C}^*$ such that

$$\begin{cases} g_2(\Lambda_1)^3 = \alpha g_2(\Lambda_2)^3 \,, \\ g_2(\Lambda_1)^3 - 27g_3(\Lambda_1)^2 = \alpha(g_2(\Lambda_2)^3 - 27g_3(\Lambda_2)^2) \,. \end{cases}$$

Substituting the first equality in the second we find that

$$\alpha g_2(\Lambda_2)^3 - 27g_3(\Lambda_1)^2 = \alpha(g_2(\Lambda_2)^3 - 27g_3(\Lambda_2)^2)$$

and hence

$$g_3(\Lambda_1)^2 = \alpha g_3(\Lambda_2)^2 \,.$$

Let $\beta \in \mathbb{C}$ denote a 12-th root of α, that is, $\beta^{12} = \alpha$, then it follows that

$$\begin{cases} g_2(\Lambda_1) = \beta^4 g_2(\Lambda_2) \,, \\ g_3(\Lambda_1) = \beta^6 g_3(\Lambda_2). \end{cases}$$

We then claim that $\Lambda_2 = \beta\Lambda_1$. To see that, notice that for $k = 2, 3$

$$g_k(\beta\Lambda_1) = \beta^{-2k} g_k(\Lambda_1) = g_k(\Lambda_2)$$

Then, from Lemma 1.5.7 it follows that all the Eisenstein series of Λ_2 and $\beta\Lambda_1$ coincide and, therefore, also their Weierstrass functions (Theorem 1.5.8(a)). In particular $\wp(\beta\Lambda_1)$ and $\wp(\Lambda_2)$ will have the same poles, but the poles of the $\wp$-function of a lattice are exactly in the lattice points, hence we conclude that $\Lambda_2 = \beta\Lambda_1$, showing that Λ_1 and Λ_2 are indeed homothetic. □

We have then seen that the j-invariant classifies all the complex tori. In particular, it can be used to show that the family of all complex tori forms a line. To see it, we will first show that the j-invariant defines a function on $\mathbb{H}$ that is invariant under the action of $\mathrm{GL}_2(\mathbb{Z})$.

Lemma 2.4.4. *Every lattice is homothetic to a lattice $\langle 1, \tau\rangle$ with $\tau \in \mathbb{H}$.*

Proof. Let $\{w_1, w_2\}$ be any basis of Λ, and assume $\tau := w_2/w_1 \in \mathbb{H}$ (if this is not the case, take $\tau := -w_2/w_1$). Then $\langle 1, \tau\rangle$ is homothetic to Λ, via the multiplication by $1/w_1$. □

Lemma 2.4.5. *Let Λ_1, Λ_2 be the lattices generated by $\{1, w_1\}$ and $\{1, w_2\}$, respectively, with $w_1, w_2 \in \mathbb{C}$. Then the two lattices are homothetic if and only if $w_2 = \frac{aw_1+b}{cw_1+d}$, for some $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{GL}_2(\mathbb{Z})$.*

Proof. By definition, two lattices are homothetic if and only if there is a $\alpha \in \mathbb{C}$ such that $\alpha\Lambda_2 = \Lambda_1$. Then there exist $a, b, c, d \in \mathbb{Z}$ such that

$$\begin{aligned} \alpha &= a + bw_1 \ , \\ \alpha w_2 &= c + dw_1 \ . \end{aligned}$$

As $\{1, w_2\}$ is a basis of Λ_2 and $\alpha\Lambda_2 = \Lambda_1$, it follows that $a + bw_1, c + dw_1$ is a basis of Λ_1, and hence $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{GL}_2(\mathbb{Z})$. The statement then follows by noticing that $w_2 = \alpha w_2/\alpha$.

For the reverse statement, assume Λ_2 is generated by 1 and $w_2 = \frac{aw_1+b}{cw_1+d}$ with $M := \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{GL}_2(\mathbb{Z})$. Set $\alpha := cw_1 + d$. Then $\alpha\Lambda_2 = \langle aw_1 + b, cw_1 + d\rangle$. By multiplying by the inverse of M, we obtain that $\alpha\Lambda_1 = \langle 1, w_1\rangle = \Lambda_1$, concluding the proof. □

Corollary 2.4.6. *Let Λ_1, Λ_2 be the lattices generated by $\{1, w_1\}$ and $\{1, w_2\}$, respectively, with $w_1, w_2 \in \mathbb{H}$. Then the two lattices are homothetic if and only if $w_2 = \frac{aw_1+b}{cw_1+d}$, for some $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})$.*

Proof. It follows from Lemma 2.4.5 by noticing that the condition of preserving $\mathbb{H}$ implies that $ad - bc = 1$. □

Let τ be a complex number in $\mathbb{H}$. We define the complex lattice associated to τ as the lattice $\Lambda_\tau = \langle 1, \tau\rangle$.

Definition 2.4.7. We define the j-function as the function of $\mathbb{H}$ defined by

$$\begin{aligned} j \colon \mathbb{H} &\to \mathbb{C} \\ \tau &\mapsto j(\tau) := 1728 \frac{g_2(\Lambda_\tau)^3}{g_2(\Lambda_\tau)^3 + 27 g_3(\Lambda_\tau)^2}. \end{aligned}$$

Remark 2.4.8. For computational purposes, it might be useful to state the Laurent series in terms of $q = \exp(2\pi i\tau)$ associated to the j-function:

$$j(\tau) = \frac{1}{q} + 744 + 196884q + 21493760q^2 + 864299970q^3 + \dots \ .$$

Lemma 2.4.9. *Let γ be an element of $\mathrm{SL}_2(\mathbb{Z})$ and $\tau \in \mathbb{H}$. Then $j(\gamma\tau) = j(\tau)$.*

Proof. It immediately follows from Lemma 2.4.3 and Corollary 2.4.6. □

Lemma 2.4.9 tells us that the j-function induces a function on the quotient $\mathbb{H}/\Gamma$.

Proposition 2.4.10. *The function $\mathbb{H}/\mathrm{SL}_2(\mathbb{Z}) \to \mathbb{C}$ induced by j is a bijection.*

Proof. Here we follow [11, Proof of Theorem 3.6]. The injectivity comes from Corollary 2.4.6. We are left to prove the surjectivity. We will show it by proving that the image $j(\mathbb{H})$ is both open and closed in $\mathbb{C}$. Then, by the connectedness of $\mathbb{C}$, the result will follow.

As j is a non-constant holomorphic function on $\mathbb{H}$, its image is open in $\mathbb{C}$.

Let $j = \lim_{n\to\infty} j(z_n)$ be a limit point of $j(\mathbb{H})$ in $\mathbb{C}$. Without loss of generality, we may and do assume that all the z_n lie in $\mathcal{F}$. If the values $\Im(z)$ are bounded, the sequence $\{z_n\}$ lie in a bounded subset of $\mathcal{F}$, that is compact. Hence they converge to a limit point $z \in \mathbb{H}$ and so $j = j(z) \in j(\mathbb{H})$. So assume that the values $\Im(z_n)$ are not bounded. Then we can pass to a subsequence and assume $\lim_{n\to\infty} \Im(z_n) = +\infty$. Then

$$\lim_{n\to\infty} g_2(z_n) = \frac{4\pi^4}{3}$$
$$\lim_{n\to\infty} g_3(z_n) = \frac{8\pi^6}{27},$$

and so

$$\lim_{n\to\infty} \Delta(z_n) = \lim_{n\to\infty} (g_2(z_n)^3 - 27g_3(z_n)^3) = 0,$$

from which it follows that $j = \lim_{n\to\infty} |j(z_n)| = \infty$, contradicting the assumption that the $j(z_n)$ converge. □

Chapter 3

A very old challenge: solving equations

Solving equations or, more precisely, finding the zeros of a given equation has been one of the first reasons to study mathematics, since the ancient times. The branch of mathematics devoted to solving equations is called *algebra*. We are going to see how elliptic curves represent a very natural and important step in the study of solutions of equations.

Since 19^{th} century, *geometry* has become is a very powerful tool in order to study the zeros of one or more polynomials. In this chapter, we will see a geometric approach to study the zeros of some easy equations. Elliptic curves lie exactly at the next step.

3.1 Equation of degree one in one variable

Let R be any ring of characteristic 0, and let $R[x_1, ..., x_n]$ denote the polynomial ring with n variables over R. Let $f(x_1, ..., x_n)$ be an element of $R[x_1, ..., x_n]$ and let K be a field containing R.

Solving $f = 0$ over K or, more precisely, finding the roots of f in K means finding the n-tuples $(a_1, ..., a_n) \in K^n$ such that

$$f(a_1, ..., a_n) = 0.$$

The easiest, and best known, case of an equation is given by

$$ax + b = 0, \tag{3.1}$$

with $a, b \in R$, $a \neq 0$ and x the variable; that is, an *equation of degree one in one variable*. We all know the following result.

Proposition 3.1.1. *Let K be a field containing R. The equation (3.1) has always exactly one solution in K, namely $x = -b/a$.*

There are two natural ways to generalise (3.1): considering equations of higher degree, or considering equations with more coefficients.

3.2 Equations of higher degree in one variable

3.2.1 Degree two

If we look at equation in one variable and higher degree, the next step is to consider equations of degree 2. Let R be any ring, K a field containing R and $\overline{K}$ an algebraic closure of K.

Example 3.2.1. For example, one can consider $R = \mathbb{Z}$, $K = \mathbb{Q}$ and $\overline{K} = \overline{\mathbb{Q}}$.
Another standard example is given by $R = \mathbb{Q}$, $K = \mathbb{R}$ and $\overline{K} = \mathbb{C}$.

$$ax^2 + bx + c = 0, \tag{3.2}$$

with $a, b, c \in R$ and $a \neq 0$. We have seen that the quantities

$$x_{1,2} = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}$$

are (the) two solutions, counted with multiplicity, of (3.2) over $\overline{K}$. It is important to note that $x_{1,2}$ do not need to be defined over R or even over K.

Example 3.2.2. Consider the equatio $x^2 + 1 = 0$. It is defined over $\mathbb{Z}$, but its roots, $\pm i$, are defined only in $\mathbb{C}$, and not in $\mathbb{Q}$ or $\mathbb{R}$.

Proposition 3.2.3. *The following statements hold.*

(a) The equation (3.2) has two solutions, counted with multiplicity, over $\overline{K}$.

(b) The equation (3.2) has two solutions, counted with multiplicity, in K if and only if $b^2 - 4ac$ is a square in K.

Remark 3.2.4. Notice that when (3.2) has solutions over K, then they are x_1 and x_2.

3.2.2 Degree three

For the case of equations of degree $d \geq 3$ over R we have similar statements. For these notes it will be enough to explicitly state only the case $d = 3$:

$$ax^3 + bx^2 + cx + d = 0. \tag{3.3}$$

with $a, b, c, d \in R$ and $a \neq 0$.

Lemma 3.2.5. *The solutions of (3.3) in $\overline{K}$ are*

$$x_k = -\frac{1}{3a}\left(b + \zeta^k C + \frac{\Delta_0}{\zeta^k C}\right)$$

where

$$\begin{aligned}
\zeta &= \frac{-1 + \sqrt{-3}}{2}\,, \\
\Delta_0 &= b^2 - 3ac\,, \\
\Delta_1 &= 2b^3 - 9abc + 27a^2 d\,, \\
C &= \sqrt[3]{\frac{\Delta_1 + \sqrt{\Delta_1^2 - 4\Delta_0^3}}{2}}
\end{aligned}$$

Proof. Reduce (3.3) to the form

$$t^3 + pt + q = 0$$

with $p, k \in K$ by applying the transformation

$$t = x + \frac{b}{3a} ,$$

then use Cardano's formula. □

Proposition 3.2.6. *The following statements hold.*

(a) The equation (3.3) has three solutions, counted with multiplicity, in $\overline{K}$.

(b) The equation (3.3) has either three, one, or no solutions, counted with multiplicity, in K.

Definition 3.2.7. We define the *discriminant* of (3.3) to be the quantity

$$\Delta := \frac{4\Delta_0^3 - \Delta_1^2}{27a^2} \in K ,$$

where Δ_0 and Δ_1 are the quantities defined in Lemma 3.2.5.

The discriminant comes in handy in particular when working over $\mathbb{R}$.

Proposition 3.2.8. *Assume $R \subseteq \mathbb{R}$. Then equation (3.3) has at least one solution over $\mathbb{R}$. If $\Delta < 0$, it has exactly one solution over $\mathbb{R}$ and two more distinct roots in $\mathbb{C}$; if $\Delta = 0$, then it has three roots over $\mathbb{R}$, not all distinct; if $\Delta > 0$, then it has three distinct roots over $\mathbb{R}$.*

3.2.3 Higher degrees

For $d = 4$, the situation is analogous to the case $d = 3$, but the formulas involved are (even) longer.

For $d \geq 5$ the situations dramatically change, and we do not have explicit conditions on the coefficients to determine the number of solutions on K.

What we can say is that if d is odd, then there is at least one real solution. Moreover, there is an algorithm to find all the solutions over $\mathbb{Q}$.

We can sum up what we know in general in the following result.

is quite clear.

Proposition 3.2.9. *Consider the equation*

$$\sum_{i=0}^{d} a_i x^i = 0, \tag{3.4}$$

with $a_i \in \mathbb{Q}$ and $a_d \neq 0$. Let $K = \mathbb{Q}, \mathbb{R}$, or $\mathbb{C}$. The equation (3.4) has finitely many solutions in K. If $K = \mathbb{C}$, then it has exactly d solutions, if counted with multiplicity. If $K = \mathbb{Q}$, there is an algorithm to determine whether (3.4) has solutions in K and, in case it does, to find all of them.

3.3 Equations of degree one in more variables

In the previous subsection we have seen what happen if consider equations over $\mathbb{Q}$ of higher degree but in only one variable. In this section we are going to study the solutions of equations of degree one but allowing more variables. We start with an example.

Example 3.3.1. Consider the equation

$$ax + by + c = 0, \tag{3.5}$$

with $a, b, c \in \mathbb{Q}$ and $a, b \neq 0$. Take $K \in \{\mathbb{Q}, \mathbb{R}, \mathbb{C}\}$ and let $x = x_0 \in K$ be fixed. Then the pair $(x_0, \frac{-c-ax_0}{b}) \in K \times K$ is a solution over K of (3.5). So for every fixed value of x we have a value of y that gives us a solution of the equation. We say that the solutions are parametrised by $K = \mathbb{A}^1_K$.

Example 3.3.1 can be easily extended to the general case:

$$a_0 + \sum_{i=1}^{n} a_i x_i = 0, \tag{3.6}$$

with $a_i \in \mathbb{Q}$ for $i = 0, 1, ..., n$ and $a_i \neq 0$ for $i = 1, ..., n$. In this case, if we fix the value of the first $n-1$ variables we always get exactly one value of the last variable satisfying the equation.

Theorem 3.3.2. *The solutions of (3.6) over K are parametrised by $K^{\times n-1} = \mathbb{A}^{n-1}_K$.*

Proof. All the solutions are of the form

$$\left(x_1, ..., x_{n-1}, \frac{-a_0 - a_1x_1 - ... - a_{n-1}x_{n-1}}{a_n}\right) \in \mathbb{A}^n_K,$$

with $(x_1, ..., x_{n-1}) \in \mathbb{A}^{n-1}_K$. □

Remark 3.3.3. Notice that in this case the number of solutions does not depend on the field K.

3.4 Equations of degree two in two variables: plane conics

So far we have kept either the degree or the number of variables equal to one. What happens if we let both grow? The first case is then given by equations of degree two in two variables:

$$ax^2 + bxy + cy^2 + dx + ey + f = 0, \tag{3.7}$$

with $a, ..., f \in \mathbb{Q}$ and $(a, b, c) \neq (0, 0, 0)$. We will see in the next example how this problem, that looks purely algebraic, can be solved by using geometric tools. The theory of the conics it is very beautiful and rich. Here we will only give a quick survey about the rational points of conics.

Example 3.4.1. Consider the following equation over $\mathbb{Q}$:

$$f(x, y) := x^2 + y^2 - 1 = 0. \tag{3.8}$$

Our goal is to determine how many solutions does (3.8) have and, possibly, write them all.

Notice that equation $f(x,y)=0$ define the unit circle C in $\mathbb{A}^2$, and that $P=(-1,0)$ is a point on it, that is, $f(-1,0)=0$. Yet in other words, $(-1,0)$ is a solution for (3.8). We call the solution of f *the K-rational points of C*; we denote the set of solutions of (3.8) in K by $C(K)$, *the set of K-rational points* of C.

Let ℓ be a curve *defined* over K passing through the point P, that is, ℓ is defined by the equation $y=m(x+1)$, with $m\in K$. Finding the intersection $C\cap\ell$ implies solving an equation of degree two in one variable, by substituting y in the equation of C:

$$\begin{aligned} 0 &= x^2+(m(x+1))^2-1 = \\ &= (1+m^2)x^2+2m^2x+x^2-1. \end{aligned}$$

The solutions to the above equations are -1 (which we already knew) and $x=\frac{1-m^2}{1+m^2}$. This implies $\ell\cap C=\{P,(\frac{1-m^2}{1+m^2},\frac{2m}{1+m^2})\}$. Notice that as $m\in K$, then $(\frac{1-m^2}{1+m^2},\frac{2m}{1+m^2})\in K\times K$. Since this construction holds for any $m\in K$, we have

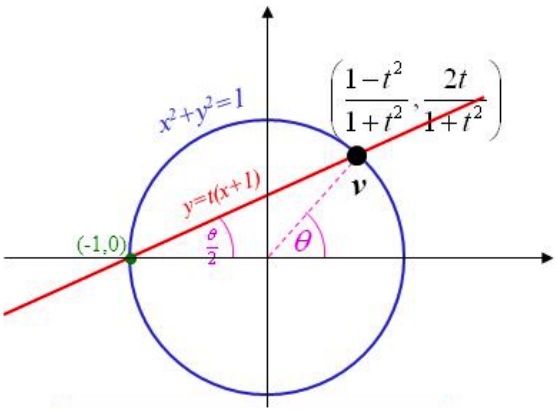
$$\{(-1,0)\}\cup\{(\frac{1-m^2}{1+m^2},\frac{2m}{1+m^2})\mid m\in K\,\}\subseteq C(K).$$

Does the equality hold? Assume $Q=(x_0,y_0)\in C(K)$ and consider the line ℓ passing through Q and P, that is,

$$\ell\colon y=m(x+1),$$

with $m=\frac{y_0}{x_0+1}\in K$. Hence it follows that $Q\in\{(-1,0)\}\cup\{(\frac{1-m^2}{1+m^2},\frac{2m}{1+m^2})\mid m\in K\,\}$, proving the equality.

So we have seen that (3.8) has infinitely many solutions over K, and that they are parametrised by $\mathbb{A}^1$ plus a point.



The argument used in Example 3.4.1 can be generalised to any equation $f(x,y)=0$ defining a *smooth conic* (cf. Definition 3.4.2).

Definition 3.4.2. Let C be the curve in $\mathbb{A}^2$ defined by the equation $f(x, y) = 0$. The curve C is called a *conic* if f has degree two. Let $P = (u, v)$ be a K-point of C, that is, $u, v \in K$ and $f(u, v) = 0$. We say that P is a *singular point* of C if

$$\frac{\partial f}{\partial x}(u, v) = \frac{\partial f}{\partial y}(u, v) = 0.$$

We say that C is *singular* if it admits singular points. We say that C is *smooth* if it is not singular.

Theorem 3.4.3. *Let $f(x, y) = 0$ be an equation of degree two in two variable defining a smooth conic C in $\mathbb{A}^2_K$. One of the two following statements holds:*

(a) f admits no solutions;

(b) the solutions of f are parametrised by $\mathbb{A}^1_K$ plus a point.

Proof. If f admits no solution then we are done. If it does admit one solution, it means that $C(K)$ contains at least one point, say P. Consider the lines defined over K passing through P. By Proposition 3.2.3 we know that each such line intersects in two points, one of them being P and as P is defined over K, so is also the other one. □

Corollary 3.4.4. *The points of any smooth conic over $\mathbb{C}$ are parametrised by $\mathbb{A}^1_{\mathbb{C}}$ plus a point.*

3.5 Exercises

The exercises marked with * are harder; those marked with ! are important.

Exercise 3.5.1. ! A triple (A, B, C) of positive integer numbers is called *pythagorean* if $A^2+B^2 = C^2$. A pythagorean triple is called *primitive* if $\gcd(A, B, C) = 1$. Describe all the primitive pythagorean triples. [Hint: use Example 3.4.1.]

Exercise 3.5.2. Describe all the $\mathbb{Q}$-rational points of the hyperbole $x^2 - y^2 = 1$.

Exercise 3.5.3. Give an example of a smooth conic over K not admitting rational points, for $K = \mathbb{Q}$ and $K = \mathbb{R}$.

Exercise 3.5.4. For $K = \mathbb{Q}, \mathbb{R}, \mathbb{C}$, is it possible to find a conic (possibly singular) with only finitely many K-rational points? If yes, give an example.

Chapter 4

Basic algebraic geometry on curves

In this section we review the basic theory of algebraic curves, following [9, 4].

4.1 Affine curves

Let K be any field and fix an algebraic closure $\overline{K}$ of K. With $G_K := G_{\overline{K}/K}$ we denote the Galois group $\mathrm{Gal}(\overline{K}/K)$

Example 4.1.1. In the following we might think of K as $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ or $\mathbb{F}_p$, usually with $p \geq 5$.

Definition 4.1.2. The *n-dimensional affine space over* K, denoted by $\mathbb{A}^n_K$, is the set

$$\mathbb{A}^n_K := \mathbb{A}^n(\overline{K}) := \{(x_1, \ldots, x_n) \ : \ x_i \in \overline{K}\}.$$

The set of *K-rational points* of $\mathbb{A}^n_K$ is

$$\mathbb{A}_n(K) := \{(x_1, \ldots, x_n) \ : \ x_i \in K\}.$$

Remark 4.1.3. Notice the following equiality

$$\mathbb{A}^n(K) = \{P \in \mathbb{A}^n_K \ : \ P^\sigma = P \text{ for every } \sigma \in G_K \ \}.$$

Set $\overline{K}[x] := \overline{K}[x_1, \ldots, x_n]$ the ring of polynomials over $\overline{K}$ in n variables and let $I \subseteq \overline{K}[x]$ be an ideal.

Definition 4.1.4. *The algebraic variety* associated to I is the set

$$V_I := \{P \in \mathbb{A}^n_K \ : \ f(P) = 0 \text{ for every } f \in I\}.$$

An *algebraic variety* is any set of the form V_I, for some ideal $I \subseteq \overline{K}[x]$.

If V is an algebraic variety, then we denote I_V the ideal associated to it, i.e., the ideal such that $V = V_{I_V}$.

Definition 4.1.5. An algebraic variety V *can be defined over* K if I_V can be generated by polynomials in $K[x] \subset \overline{K}[x]$.

Example 4.1.6. The variety of $\mathbb{A}^2_K$ defined by $x_1^2 - x_2^2 - 1 = 0$ can be defined over K.

Remark 4.1.7. Let V be an algebraic variety that can be defined over K. Then G_K induces an action on the points of V.

Definition 4.1.8. An affine variety $V \subset \mathbb{A}^n$ is called *irreducible* if the associated ideal $I_V \subseteq K[x]$ is prime. The affine variety V is called *geometrically irreducible* if the associated ideal is prime in $\overline{K}[x]$.

Definition 4.1.9. Let V be an irreducible variety of $\mathbb{A}^n$. The *coordinate ring* of V is the quotient

$$K[V] := \frac{K[x]}{I_V} .$$

Remark 4.1.10. As V is irreducible, $K[V]$ is a domain.

Definition 4.1.11. We define the *function field* of V, denoted by $K(V)$, the fraction field of $K[V]$.

If V is geometrically irreducible, then we can define the function field $\overline{K}(V)$ as the fraction field of $\overline{K}[x]/I_V$.

Definition 4.1.12. Let V be a geometrically irreducible variety. The dimension of V, denoted by $\dim V$, is the transcendental degree of $\overline{K}(V)$ over $\overline{K}$.

Example 4.1.13. Unsurprisingly, $\mathbb{A}^n_K$ has dimension n.

Definition 4.1.14. An *affine curve* is a geometrically irreducible variety of dimension 1.

Definition 4.1.15. Let $V \subseteq \mathbb{A}^n$ be a variety, $P \in V$, and $f_1, \ldots, f_m \in \overline{K}[x]$ a set of generators of I_V. We say that V is *smooth* at P if the $m \times n$ matrix

$$\left(\tfrac{\partial f_i}{\partial x_j}(P)\right)$$

has rank equal to $n - \dim V$.

Otherwise the variety is called *singular at* P, and P is called a *singular point* of V.

If V is smooth at every point, then it is called *smooth*.

4.2 Projective curves

Consider the affine space $\mathbb{A}^{n+1}$ and the equivalence relation $\sim$ on it given by

$$(x_0, x_1, \ldots, x_n) \sim (y_0, y_1, \ldots, y_n) \iff \exists \lambda \in \overline{K}^\times \text{ such that } (x_0, x_1, \ldots, x_n) = (\lambda y_0, \lambda y_1, \ldots, \lambda y_n) .$$

The equivalence class of $(x_0, \ldots, x_n)$ is denoted by $(x_0 : \ldots : x_n)$.

Definition 4.2.1. We define the *n-dimensional projective space* over K to be the quotient

$$\mathbb{P}^n_K := \frac{\mathbb{A}^{n+1}_K \setminus \{(0, \ldots, 0)\}}{\sim} .$$

Definition 4.2.2. *The set of K-rational points* of $\mathbb{P}^n_K$ is the set

$$\mathbb{P}^n(K) := \{(x_0 : \ldots : x_n) \mid \text{all } x_i \in K \}.$$

Remark 4.2.3. As before, one has that $\mathbb{P}^n(K) = \{P \in \mathbb{P}^n \ : \ P^\sigma = P \text{ for every } \sigma \in G_K \}$.

Definition 4.2.4. A polynomial $f \in \overline{K}[x_0, \dots, x_n]$ is *homogeneous of degree* d if $\deg f = d$ and $f(\lambda x) = \lambda^d f(x)$ for every $\lambda \in \overline{K}$.

An ideal $I \subseteq \overline{K}[x]$ is *homogeneous* if it can be generated by homogeneous polynomials.

If $I \subseteq \overline{K}[x]$ is a homogeneous ideal then the following definition makes sense:

$$V_I = \{P \in \mathbb{P}^n \mid f(P) = 0 \text{ for every } f \in I \}.$$

Definition 4.2.5. A *projective variety* is a subset V of the form $V = V_I$ for some homogeneous ideal $I \subseteq \overline{K}[x]$.

A projective variety $V = V_I$ *can be defined* over K if I can be generated by homogeneous polynomials in $K[x]$.

As for the the affine case, we can introduce the notion of K-rational points also for projective varieties. Let V be a projective variety defined over K, then we define its set of K-rational points to be

$$V(K) := V \cap \mathbb{P}^n(K) = \{P \in V \ : \ P^\sigma = P \text{ for any } \sigma \in G_K \}.$$

Definition 4.2.6. A projective variety is defined to be *(geometrically) irreducible* analogously to 4.1.12.

A projective space *contains* many affine spaces. For every $i = 0, \dots, n$, consider the following map:

$$\phi_i \colon \mathbb{A}^n \to \mathbb{P}^n, \ (x_1, \dots, x_n) \mapsto (x_1, \dots, x_{i-1}, 1, x_i, \dots, x_n).$$

Lemma 4.2.7. *The following statements hold.*

1. *For every i, the map ϕ_i is injective.*
2. *the image of ϕ_i is the projective variety H_i defined by $x_i = 0$.*

Proof. Exercise. □

Let U_i be the complement of $H_i = \{x_i = 0\}$, that is, $U_i = \{(x_0, \dots, x_n) \ : \ x_i \neq 0\}$. Then we can define the maps

$$\psi_i \colon U_i \to \mathbb{A}^n \ , \ (x_0 : \dots : x_n) \mapsto (x_0/x_i, \dots, x_{i-1}/x_i, x_{i+1}/x_i, \dots, x_n/x_i).$$

Clearly, $\psi_i \circ \phi_i = \mathrm{id}_{\mathbb{A}^n}$. The maps ϕ_i and ψ_i also determine a relation between affine and projective varieties. Let V be a projective algebraic variety with ideal I, then $V_i := \psi_i(U_i \cap V)$ is the affine algebraic variety defined by the ideal

$$\{f(y_1, \dots, y_{i-1}, 1, y_i, \dots y_n) \ : \ f(x_0, \dots, x_n) \in I\}$$

As $U_0, \dots, U_n$ cover $\mathbb{P}^n$, the $V_i's$ cover V and are called the *affine patches* of V.

This process can be reversed: if $V \subset \mathbb{A}^n$ is an affine algebraic variety defined by the ideal $I \subset K[x]$, then one can define the *projective closure* $\overline{V}$ of V in $\mathbb{P}^n$ as the projective variety associated to the ideal

$$\{x_0^{\deg f} f(x_1/x_0, \dots, x_n/x_0) \ : \ f(x_1, \dots, x_n) \in I\}.$$

Proposition 4.2.8. *(a) If V is an affine variety, then $\overline{V}$ is an algebraic variety and $\psi_0(V \cap U_0) = V$.*

(b) If V is a projective variety, then $\psi_i(V \cap U_i)$ is either empty or an affine variety V_i such that $\overline{V_i} = V$.

(c) If an affine variety is defined over K, then so is its projective closure. Conversely, if a projective map is defined over K, then so is any of its affine patches.

Proof. Exercise. □

Remark 4.2.9. It turns out that if V is a projecive variety, then all its non-empty affine patches have the same dimension and isomorphic function fields.

Definition 4.2.10. Let V be a projective variety. The *dimension* of V is defined to be as the dimension of any of its non-empty affine patches. The *function field* of V is defined to be the function field of any of its non-empty affine patches.

4.3 Maps between varieties

After defining objects, we define maps between them. Let V be a projective variety and consider its function field $K(V)$. An element $f \in K(V)$ is called a *rational function*.

Definition 4.3.1. Let $V_1 \subset \mathbb{P}^n, V_2 \subset \mathbb{P}^m$ be two projective varieties, then a *rational map* is a map

$$\begin{aligned} f \colon V_1 &\to V_2 \\ P &\mapsto (f_0(P) : \ldots : f_m(P)) \end{aligned}$$

with $f_0, \ldots, f_m \in K(V_1)$.

Remark 4.3.2. It might happen that a rational map $f \colon V_1 \to V_2$ is not defined everywhere, indeed there might exist points $P \in V_1$ such that $f_0(P) = \ldots = f_m(P) = 0$. It might also happen that $f_i(P)$ is not defined for some i, that is, P is a pole for f_i. Sometimes these issues can be solved by multiplying all the functions f_i for a certain rational function $g \in K(V)$. If this is not possible, then we say that f *is not defined* at P.

Definition 4.3.3. A rational map that is defined everywhere is called *a morphism*.

Example 4.3.4. Let C be the affine line $\mathbb{A}^1_K$ with coordinate x. Then a function of C is given by a ratio f_1/f_2, with f_1, f_2 polynomials in x. For example,

$$f \colon x \mapsto \frac{x-2}{x^2-1}.$$

Notice that f is not defined at 1 and -1, that is, it has poles (of multiplicity one) at 1 and -1; it has a zero at 2

If we embed $\mathbb{A}^1$ into $\mathbb{P}^1$ via

$$x \mapsto (X : Y) = (x : 1),$$

then f extends to the regular map of $\mathbb{P}^1$ given by

$$(X : Y) \mapsto \frac{(X-2Y)Y}{X^2-Y^2}.$$

Then notice that it has poles at $(1:1), (-1:1)$ and zeros at $(2:1), (1:0)$.

4.4 Algebraic curves and maps between them

An affine (respectively, projective) algebraic curve is an affine (resp. projective) algebraic variety of dimension 1. Let C be a curve over a field K and P a point on it and consider the function field $\overline{K}(C)$.

We can define the following valuation on $\overline{K}(C)$ by using the order of a function $f \in \overline{K}(C)$ at P.

$$\begin{aligned} \mathrm{ord}_P \colon \overline{K}(C) &\to \mathbb{Z} \cup \{\infty\} \\ f &\mapsto \mathrm{ord}_P(f) \end{aligned}$$

Proposition 4.4.1. *Let C be a smooth curve, $f \in \overline{K}(C)$. Then there exists only finitely many points $P \in C$ such that $\mathrm{ord}_P(f) \neq 0$. If $\mathrm{ord}_P(f) \geq 0$ for every point $P \in C$ then $f \in \overline{K}$.*

Proof. [9, Proposition II.1.2]. □

Example 4.4.2. Consider the curve $C = \mathbb{P}^1$, the variety $V = \mathbb{P}^2$ and the map $\mathbb{P}^1 \to \mathbb{P}^2$ defined by

$$(X : Y) \to \left(X^2(X^2 - Y^2) : Y^2(X - Y)^2 : (X^2 - Y^2)(X - Y)^2\right).$$

Notice that the map is not defined at $(1 : 1)$.

Lemma 4.4.3. *Let C be a curve, $V \subset \mathbb{P}^n$ a variety, $\phi \colon C \to V$ a rational map. The following statements hold.*

(a) If $P \in C$ is a smooth point for C, then ϕ is defined at P. In particular, if C is smooth, ϕ is a morphism.

(b) If ϕ is a morphism and V is also a curve, then ϕ is either surjective or constant.

(c) If V is a curve and ϕ is a non-constant morphism, then ϕ is a finite map.

Proof. (a) [9, Proposition II.2.1].

(b) [9, Theorem II.2.3].

(c) [9, Theorem II.2.4(a)].

□

If $\phi \colon C_1 \to C_2$ is a map of curves and $f \in K(C_2)$ is a rational function on C_2, then one can use ϕ to define a rational map on C_1

$$\phi^* f := f \circ \phi \colon C_1 \to K \ , \ P \to f(\phi(P)) \ .$$

This defines a map between the two function fields:

$$\phi^* \colon K(C_2) \to K(C_1) \ , \ f \mapsto \phi^* f \ .$$

Notice that the above a map is a morphism of fields hence it is injective; moreover, ϕ^* fixes K.

Lemma 4.4.4. *Let C_1, C_2 be curves over K.*

(a) If $\phi \colon C_1 \to C_2$ is a non-constant map over K, then $K(C_1)$ is a finite extension of $\phi^* K(C_2)$.

(b) If $\iota\colon K(C_2) \to K(C_1)$ is an injection of fields fixing K, then there exists a unique non constant morphism $\phi\colon C_1 \to C_2$ defined over K such that $\phi^* = \iota$.

Proof. [9, Theorem 2.4]. □

Definition 4.4.5. Let $\phi\colon C_1 \to C_2$ be a morphism of curves over K. Then by Lemma 4.4.4 $K(C_1)$ is a finite extension of $\phi^*K(C_2)$. We define the *degree* of the map ϕ to be

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

If ϕ is constant then $\deg \phi = 0$; if ϕ is non-constant then $\deg \phi$ is finite and ϕ is called a *finite* map.

Remark 4.4.6. Let $\phi\colon C_1 \to C_2$ be a rational map of curves, and let $Q \in C_2$ be a point of C_2. The degree of ϕ equals the number of points in the pre-image $\phi^{-1}(Q)$ of Q, *counted with multiplicity.*

Remark 4.4.7. By multiplicity here we mean what in [9] is called ramification index. See [9, Section II.2] for more details about this notion.

Example 4.4.8. Let $E\colon Y^2Z = X^3 + aXZ^2 + bZ^3$ and let $\pi\colon E \to \mathbb{P}^1$ be the projection on the X-axis, i.e.,

$$\pi\colon (X : Y : Z) \to (X : Z).$$

Notice that π is not defined at $(0 : 1 : 0)$, it is not surjective as $(1 : 0)$ is not in the image, and it has degree 2. Indeed, if $Q = (x : 1) \in \mathbb{P}^1$, then $\pi^{-1}(Q) = \{(x : \pm\sqrt{x^3 + ax + b} : 1)\}$.

The rational map π can be extended to a morphism defining $\pi((0 : 1 : 0)) = (1 : 0)$.

4.5 The Frobenius map

When working in characteristic 0, Remark 4.4.6 gives a good intuition about how the degree of a map works. This is not true anymore when we work in positive characteristic, as we are going to see in this subsection.

Assume K is a *perfect* field with $\operatorname{Char} K = p > 0$, e.g. $K = \mathbb{F}_p, \mathbb{F}_{p^n}, \overline{\mathbb{F}_p}$. Then we can consider the *Frobenius map*

$$F\colon K \to K \ , \ a \mapsto a^p.$$

Of course we can consider also powers of this function, $F^r\colon a \mapsto a^{p^r}$.

The Frobenius map induces an action also on the ring of polynomials $K[X]$ by acting on the coefficients of the polynomial. In this way we can define a map on a curve over K.

Let C/K be a curve and $I \subset K[X]$ its associated ideal. Then we can consider the ideal

$$I^F = \{F(f) \ : \ f \in I\}$$

and the curve associated to it, C^F.

Definition 4.5.1. The *Frobenius map* of C is the map

$$\begin{aligned} F \ &: \ C \to C^F \\ (x_0 : \ldots : x_n) &\mapsto (F(x_0) : \ldots : F(x_n)) \end{aligned}$$

Remark 4.5.2. Notice that if C can be defined over $\mathbb{F}_p \subseteq K$, then $C^F = C$ and the Frobenius is an automorphism. More in general, if C can only be defined over $\mathbb{F}_{p^r} \subseteq K$ with $r > 1$, then $C^F \neq F$ but $C^{F^r} = C$.

Proposition 4.5.3. *In the previous setting, the following statements hold.*

(a) $F^*K(C^F) = F(K(C)) = \{f^F \ : \ f \in K(C)\}$.

(b) $K(C)/F^*K(C^F)$ *is a purely inseparable extension.*

(c) $\deg F = p$.

(d) Any map $\phi\colon C_1 \to C_2$ *factors as* $\lambda \circ F^r$ *for some* $r > 0$ *and some separable map* λ.

Proof. [9, Proposition II.2.11 and Corollary II.2.12]. □

4.6 The divisor group

Definition 4.6.1. Let C be a curve, we define the *divisor group of* C, denoted by $\operatorname{Div} C$ to be the free abelian group generated by the points of C.

A *divisor* of C is an element of $\operatorname{Div} C$, that is, formal sum of the form

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

where n_P is an integer and it is equal to zero for almost all P.

Definition 4.6.2. Let $D = \sum n_P P$ be a divisor of C. We define the *degree* of D as

$$\sum_{P \in C} n_P \in \mathbb{Z}.$$

This defines a map (in fact a group homomorphism)

$$\deg\colon \operatorname{Div} C \to \mathbb{Z}\ .$$

We define $\operatorname{Div}^0 C$ to be the kernel of deg.

If C is defined over a field k, then $\operatorname{Gal}(\overline{k}/k)$ acts on $\operatorname{Div} C$ (and $\operatorname{Div}^0 X$) in the obvious way: if $\sigma \in \operatorname{Gal}(\overline{k}/k)$ and $D = \sum n_P P$, then

$$D^\sigma = \sum n_P P^\sigma.$$

Definition 4.6.3. Let $D \in \operatorname{Div} C$ a divisor on C. We say that D *can be defined over* k if $D^\sigma = D$ for any $\sigma \in \operatorname{Gal}(\overline{k}/k)$.

Remark 4.6.4. We recall the notion of a regular function for a curve. Let $C \subset \mathbb{A}^n$ be an affine curve. A regular function of C, that is an element of $K(C)$, is a function that can be expressed as

$$P = (x_1, ..., x_n) \mapsto \frac{f_1(x_1, ..., x_n)}{f_2(x_1, ..., x_n)},$$

where f_1, f_2 are polynomials in n variables. Notice that a regular function of C does not need to be defined on the whole C.

If C is a projective curve, that is, $C \subset \mathbb{P}^n$, then a regular function of C is a function that can be expressed as

$$P = (x_0 : ... : x_n) \mapsto \frac{f_1(x_0, ..., x_n)}{f_2(x_0, ..., x_n)},$$

where f_1, f_2 are polynomials of the same degree in $n+1$ variables. Also in this case, a regular function of C does not need to be defined on the whole C.

Definition 4.6.5. Let f be a function of C defined over $\overline{k}$, that is an element of $\overline{k}(C)$, then we defined the divisor associated to f to be the divisor

$$(f) = \operatorname{div} f = \sum \operatorname{ord}(P)P.$$

Divisors of the form $D = \operatorname{div} f$ for $f \in \overline{k}(C)$ are called *principal*.

Two divisors D_1, D_2 are called *linearly equivalent*, denoted $D_1 \sim_{\text{lin}} D_2$ if their difference is a principal divisor.

Example 4.6.6. Continuing Example 4.3.4, the divisor associated to the map of $\mathbb{P}^1$ defined by

$$(X : Y) \mapsto \frac{(X - 2Y)Y}{X^2 - Y^2}.$$

is

$$(2 : 1) + (1 : 0) - (1 : 1) - (-1 : 1).$$

Example 4.6.7. Let E be the elliptic curve over $\mathbb{Q}$ given by the equation

$$E\colon y^2 = x^3 - x\ .$$

Consider the points $P_1 = (-1, 0), P_2 = (0, 0), P_3 = (0, 0) \in E(\mathbb{Q})$, and the points $Q_1 = (2, \sqrt{6}), Q_2 - (2, -\sqrt{6})$.

Then $D = 2(-1, 0) - 3(0, 0) + (2, \sqrt{6})$ is a divisor of E. The degree of D is 0, and hence $D \in \operatorname{Div}^0 E$.

Let $\sigma \in \operatorname{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ be the map defined by

$$\sigma\colon \sqrt{6} \to -\sqrt{6}.$$

Then $D^\sigma = 2(-1, 0) - 3(0, 0) + (2, -\sqrt{6}) \neq D$, hence D cannot be defined over $\mathbb{Q}$.

Consider instead the divisor $D_1 = (2, -\sqrt{6}) + (2, \sqrt{6})$. Notice that $D_1^\sigma = (2, \sqrt{6}) + (2, -\sqrt{6}) = D_1$ and hence D_1 can be defined over $\mathbb{Q}$, even though Q_1 and Q_2 cannot, if taken singularly!

Consider the function of E defined by

$$f := y = \frac{Y}{Z}.$$

Then f has three zeros of multiplicity one at P_1, P_2, P_3 and one pole of multiplicity three at $\mathcal{O} = (0 : 1 : 0)$. It follows that $P_1 + P_2 + P_3 \sim_{\text{lin}} 3\mathcal{O}$.

Proposition 4.6.8. *Let C be a smooth curve and $f \in \overline{K}(C)$. let $\phi\colon C_1 \to C_2$ be a noncostant map of curves. Then the following statements hold.*

(a) $\operatorname{div} f = 0$ *if and only if* $f \in \overline{k}^*$.

(b) $\deg \operatorname{div} f = 0$.

Proof. [9, Proposition II.3.1]. □

Definition 4.6.9. Let $f\colon C_1 \to C_2$ be a map of curves. Then f induces *two* maps at the level of divisors:

$$\begin{aligned} \phi^*\colon \operatorname{Div} C_2 &\to \operatorname{Div} C_1 \\ Q &\mapsto \sum_{P \in f^{-1}(Q)} e_\phi(P) P \end{aligned}$$

where $e_\phi(P)$ is the multiplicity of P inside $f^{-1}(Q)$;

$$\begin{aligned} \phi_*\colon \operatorname{Div} C_1 &\to \operatorname{Div} C_2 \\ P &\mapsto \phi(P)\ . \end{aligned}$$

Remark 4.6.10. One can rephrase Definition 4.6.9 for $\operatorname{Div}^0 C$, $\operatorname{Pic} C$, and/or $\operatorname{Pic}^0 C$.

Facts 4.6.11. *Let* $\phi\colon C_1 \to C_2$ *be a noncostant map of curves. Then the following statements hold.*

(a) For all $D \in \operatorname{Div} C_2$, $\deg \phi^* D = \deg \phi \cdot \deg D$.

(b) For all $f \in \overline{k}(C_1)$, $\phi^*(\operatorname{div} f) = \operatorname{div}(\phi^* f)$.

(c) For all $D \in \operatorname{Div} C_1$, $\deg(\phi_* D) = \deg D$.

(d) For all $f \in \overline{k}(C_1)$, $\phi_*(\operatorname{div} f) = \operatorname{div}(\phi_* f)$.

(e) $\phi_* \circ \phi^*$ *acts as multiplication by* $\deg \phi$ *on* $\operatorname{Div} C_2$.

(f) If $\psi\colon C_2 \to C_3$ *is another nonconstant morphism of curves, then*

$$\begin{aligned} (\psi \circ \phi)^* &= \phi^* \circ \psi^* \text{ and} \\ (\psi \circ \phi)_* &= \psi_* \circ \phi_*\ . \end{aligned}$$

4.7 The Picard group

Definition 4.7.1. The *Picard group* of C, denoted by $\operatorname{Pic} C := \operatorname{Div} C / \sim_{\text{lin}}$, is the quotient of $\operatorname{Div} C$ by linear equivalence.

We define $\operatorname{Pic}^0 C$ to be $\operatorname{Div}^0 / \sim_{\text{lin}}$.

Example 4.7.2 (Picard group of $\mathbb{P}^1$)**.** It is easy to see, that if $C = \mathbb{P}^1$, then a divisor $D \in \operatorname{Div} \mathbb{P}^1$ is principal if and only if $\deg D = 0$. It follows that the map deg induces an isomorphism between $\operatorname{Pic} \mathbb{P}^1$ and $\mathbb{Z}$

Example 4.7.3. As in Example 4.6.7, consider the function of E defined by

$$f := y = \frac{Y}{Z}.$$

Then f has three zeros of multiplicity one at P_1, P_2, P_3 and one pole of multiplicity three at $\mathcal{O} = (0 : 1 : 0)$. It follows that $P_1 + P_2 + P_3 \sim_{\text{lin}} 3\mathcal{O}$ or, equivalently, that $P_1 + P_2 + P_3 = 3\mathcal{O}$ in $\operatorname{Pic} E$.

Definition 4.7.4. Let $D = \sum n_P P$ be a divisor of C. We say that D is *effective*, denoted by

$$D \geq 0,$$

if $n_P \geq 0$ for every P.

We say that $D_1 \geq D_2$ if $D_1 - D_2$ is effective.

Definition 4.7.5. Let D be a divisor of C. We associate to D the set of function

$$\mathcal{L}(D) := \{f \in \overline{k}(C)^* : \operatorname{div} f \geq -D\} \cup \{0\}.$$

We denote the dimension of $\mathcal{L}(D)$ by $\ell(D) := \dim_{\overline{k}} \mathcal{L}(D)$.

Example 4.7.6. We continue with Example 4.6.7. The divisor $D_2 = P_1 + P_2 + P_3$ is effective, and $f \in \mathcal{L}(D_2)$.

Facts 4.7.7. *Let $D \in \operatorname{Div} C$. Then the following statements hold.*

(a) If $\deg D < 0$, then $\mathcal{L}(D) = \{0\}$.

(b) $\mathcal{L}(D)$ is a finitely dimensional $\overline{k}$-vector space.

(c) If D' is linearly equivalent to D, then $\mathcal{L}(D) \cong \mathcal{L}(D')$.

Chapter 5

Cubic curves

After giving a complete answer for the solution of quadratic equations in two variables, we proceed by studying equations of degree three in two variables. First we will show that, provided there exists a point, the equation can be brought in a more convenient form.

5.1 Weierstrass form

Let K be any field, and fix an algebraic closure $\overline{K}$ of K. Let $f = f(x, y) \in K[x, y]$ be a polynomial in two variables. of degree 3 over K. Then f can be written as

$$f(x, y) = \sum a_{ij} x^i y^j, \tag{5.1}$$

where the sum ranges over all the $0 \leq i, j \leq 3$ such that $i + j \leq 3$, $a_{ij} \in K$ for every i, j and the polynomial has actual degree 3. We define a *cubic* (curve) a curve $C \subset \mathbb{A}^2(x, y)$ whose defining equation is of degree three.

Remark 5.1.1. The curve C is a curve inside the affine plane $\mathbb{A}^2_K$. Let $\mathbb{P}^2$ be the projective plane with coordinates X, Y, Z such that $X/Z = x$ and $Y/Z = y$. The projective closure of C inside $\mathbb{P}^2_K$ is the projective curve $\bar{C}$ defined by the equation

$$\sum a_{ijk} X^i Y^j Z^k,$$

where the sum ranges over all the non-negative integers i, j, k such that $i + j + k = 3$.

Definition 5.1.2. Let $P \in C(\overline{K})$. We say that P is a singular point for C if

$$\frac{\partial f}{\partial x}(P) = 0 = \frac{\partial f}{\partial y}(P) \, .$$

Definition 5.1.3. We say that a cubic C over K is in *Weierstrass form* if its defining equation is of the form

$$y^2 + a_1 xy + a_3 y = x^3 + a_2 x^2 + a_4 x + a_6 \tag{5.2}$$

with $a_1, a_2, a_3, a_4, a_6 \in K$.

We say that it is in *short* Weierstrass form if its defining equation is of the form

$$y^2 = x^3 + b_2x^2 + b_4x + b_6 \tag{5.3}$$

with $b_2, b_4, b_6 \in K$.

We say that it is in *very* short Weierstrass form if its defining equation is of the form

$$y^2 = x^3 + ax + b \tag{5.4}$$

with $a, b \in K$.

Proposition 5.1.4. *Let C be a smooth projective cubic over K with a K-rational point.*
Then C can be put into a Weierstrass form using K-rational maps.
If $\operatorname{Char} K \neq 2$, then C can be put into a short Weierstrass form.
If $\operatorname{Char} K \neq 2, 3$, then C can be put into a very short Weierstrass form.

Proof. This proof follows [10, I.3]. Let $\bar{C}$ denote the projective closure of C inside $\mathbb{P}^2(X, Y, Z)$. Then $\bar{C}$ is defined by the homogeneous degree three polynomial

$$f_0 := a_0X^3 + a_1X^2Y + a_2X^2Z + a_3XY^2 + a_4XYZ + a_5XZ^2 + a_6Y^3 + a_7Y^2Z + a_8YZ^2 + a_9Z^3.$$

By assumption $\bar{C}$ has a rational point, say $(x_0 : y_0 : z_0)$; without loss of generality we assume $x_0 \neq 0$. Applying the transformation

$$t_1 : \begin{cases} X' &= X \\ Y' &= x_0Y - y_0X \\ Z' &= x_0Z - z_0X \end{cases}$$

we move the point $(x_0 : y_0 : z_0)$ to $\mathcal{O} := (1 : 0 : 0)$ and $\bar{C}$ transforms into the curve C_1 defined by

$$f_1 := b_1X^2Y + b_2X^2Z + b_3XY^2 + b_4XYZ + b_5XZ^2 + b_6Y^3 + b_7Y^2Z + b_8YZ^2 + b_9Z^3.$$

Notice that the coefficient of X^3 is zero as $(1 : 0 : 0)$ is on C_1.

Let $L_{\mathcal{O}}$ be the tangent curve of C_1 at $\mathcal{O}$: it is defined by the equation $b_2Z + b_1Y = 0$. By applying the transformation

$$t_2 : \begin{cases} X' &= X \\ Y' &= Y \\ Z' &= b_2Z + b_1Y \end{cases}$$

we fix the point $\mathcal{O}$ and move $L_{\mathcal{O}}$ to the line $Z = 0$. The curve C_1 gets mapped to the curve C_2 defined by

$$f_2 := c_2X^2Z + c_3XY^2 + c_4XYZ + c_5XZ^2 + c_6Y^3 + c_7Y^2Z + c_8YZ^2 + c_9Z^3.$$

Notice that the coefficient of X^2Y is zero since $Z = 0$ is the tangent line of C_2 at $\mathcal{O} := (1 : 0 : 0)$.

Let P be the third point of intersection of $L_{\mathcal{O}} = \{Z = 0\}$ and C_2, that is, $P = (-c_6 : c_3 : 0)$. Then the transformation

$$t_3 : \begin{cases} X' &= c_3X + c_6Y \\ Y' &= Y \\ Z' &= Z \end{cases}$$

moves P to the point $(0:1:0)$ and keeps the point $\mathcal{O} = (1:0:0)$ and the line $\{Z=0\}$ fixed; it sends C_2 to the curve C_3 defined by

$$f_3 := d_2X^2Z + d_3XY^2 + d_4XYZ + d_5XZ^2 + d_7Y^2Z + d_8YZ^2 + d_9Z^3.$$

Notice that the coefficient of Y^3 is zero since $(0:1:0)$ is a point on the curve.

As before, we consider the tangent line L_P to C_3 at $(0:1:0)$: it is defined by the equation $d_3X + d_7Z = 0$. Then the transformation

$$t_4 : \begin{cases} X' &= d_3X + d_7Z \\ Y' &= Y \\ Z' &= Z \end{cases}$$

fixes $\mathcal{O} = (1:0:0), P = (0:1:0)$ and the line $\{Z=0\}$; it sends the line L_P to $\{X=0\}$ and the curve C_3 to the curve C_4 defined by

$$f_4 := e_2X^2Z + e_3XY^2 + e_4XYZ + e_5XZ^2 + e_8YZ^2 + e_9Z^3\,.$$

Notice that the coefficient of Y^2Z is zero since $X=0$ is the tangent line to C_4 at $(0:1:0)$.

Consider the affine part of C_4 given by $C_4 \cap \{Z \neq 0\}$; for sake of simplicity we will denote it again by C_4. If we take $x = X/Z, y = Y/Z$ to be the affine coordinates of $\mathbb{A}^2 = \{Z \neq 0\}$, we can write C_4 as the curve defined by the equation

$$xy^2 + (\alpha_0 x + \alpha_1)y = \alpha_2 x^2 + \alpha_3 x + \alpha_4\,.$$

Notice that we can divide by e_3 otherwise C_4 would be a conic, hence C would be rational, contradicting the assumption that C is a smooth cubic. We can multiply both sides by x obtaining the curve

$$C_5 \colon (xy)^2 + (\alpha_0 x + \alpha_1)xy = \alpha_2 x^3 + \alpha_3 x^2 + \alpha_4 x\,.$$

By applying the transformation

$$t_5 : \begin{cases} x' &= x \\ y' &= xy \end{cases}$$

we send C_5 to the curve

$$C_5 \colon y^2 + \alpha_1 xy + \alpha_3 y = \alpha_0 x^3 + \alpha_2 x^2 + \alpha_4 x\,.$$

Multiplying both sides by α_0^2 and using the substitution $y' = \alpha_0 y, x' = \alpha_0 x$ we reduce it to the Weierstrass form.

Now assume $\operatorname{Char} K \neq 2$. Using the transformation

$$t_6 : \begin{cases} x' &= x \\ y' &= y + (\alpha_0 x + \alpha_1)/2 \end{cases}$$

we transform C_5 into the curve

$$C_6 \colon y^2 = \beta_0 x^3 + \beta_1 x^2 + \beta_2 x + \beta_3$$

which again, after multiplying both sides by β_0^2 and using substituting x and y with $\beta_0 x$ and $\beta_0 y$, respectively, reduces to a short Wierstrass form.

Finally, if we further assume that $\operatorname{Char} K \neq 3$, we can use the transformation

$$t_7 : \begin{cases} x' &= x + \beta_1/(3\beta_0) \\ y' &= y \end{cases}$$

to send C_6 to the curve

$$C_7 \colon y^2 = x^3 + ax + b\,,$$

which is in very short Weierstrass form, completing the proof. □

Remark 5.1.5. When we say that the curve C 'can be put into Weierstrass form' we more precisely mean that there is a rational map over K from C to a curve defined by an equation in Weierstrass form. One can easily see that all the transformations $t_i, i = 1, ..., 7$, are rational transformations of $\mathbb{P}^2$ defined over K. In fact, all of them except t_5 are automorphisms of $\mathbb{P}^2$.

The map t_5 is a *rational* map, i.e., it is not defined on the whole $\mathbb{P}^2$, but on an open subset of it. Indeed, t_5 is defined everywhere except at $(1 : 0 : 0)$ and $(0 : 1 : 0)$. This is not too much of a problem as the point $(0 : 1 : 0)$ is on the curve C_6 but not in the image of t_5. This means that passing from the original cubic to the one in Weierstrass form we only lose one solution, the one we already knew from the beginning and started with.

Remark 5.1.6. In the proof of Proposition 5.1.4 we tacitly assumed some coefficients to be nonzero. If this were not the case, i.e., if some coefficients were to be zero, putting the cubic in the desired form would actually be easier, even though the transformations used would be slightly different. Analogously, we assumed $\mathcal{O}$ not to be a flex point. If it were, we could have assumed that $\mathcal{O} = (0 : 1 : 0)$ with tangent line $Z = 0$. This implies that we can write the equation of C as

$$\alpha_0 y^2 + (\alpha_1 x + \alpha_2) y = \alpha_3 x^3 + \alpha_4 x^2 + \alpha_5 x + \alpha_6.$$

From here, assuming to work in characteristic at least 5, one can use transformations t_6 and t_7 as in the proof of Proposition 5.1.4 to obtain the short Weierstrass form.

5.2 Elliptic curves as cubic curves with a point

In this section we finally give the definition of an elliptic curve. The idea is to take a cubic curve with a point and endow it with a group structure.

Definition 5.2.1. An *elliptic curve* over a field K is a couple $E = (C, O)$ where C is a smooth projective cubic over K and $O \in \overline{C}(K)$ is a K-rational point on the projective closure of C.

Corollary 5.2.2. *Every elliptic curve can be put in Weierstrass form. If* $\operatorname{Char} K \neq 2$*, then it can be put into short Weierstrass form. If* $\operatorname{Char} K \neq 2, 3$*, then it can be put into very short Weierstrass form.*

Proof. Immediate from Proposition 5.1.4. □

Example 5.2.3. Let K be any field, and consider a smooth cubic C defined by an equation in very short Weierstrass form:

$$C\colon y^2 = x^3 + ax + b\ .$$

It is immediate to see that the point $O = (0 : 1 : 0)$ belongs to the projective closure of C, defined by

$$\overline{C}\colon Y^2Z = X^3 + aXZ^3 + bZ^3\ .$$

Then (C, O) is an elliptic curve over K. This is the most important example of elliptic curve and most elliptic curves used in practice appear in this form.

In what follows, when will talk about an elliptic curve given by $y^2 = x^3 + ax + b$, we will always mean the cubic curve together with the point O.

Remark 5.2.4. The ((very) short) Weierstrass form is not the only useful and classical form to write the equation of an elliptic curve. Other classical forms to write an elliptic curve E are the following:

$$E\colon y^2 = x(x-1)(x-\lambda) \quad \text{(Legendre form)}, \tag{5.5}$$

for some $\lambda \in \mathbb{R} - \{0, 1\}$;

$$E\colon y^2 = (1-x^2)(1-k^2x^2) \quad \text{(Jacobi form)}, \tag{5.6}$$

for some $k \in \mathbb{C} - \{0, \pm 1\}$.

In particular, from an historical point of view, the first elliptic curves indeed appeared in Jacobi form, see §1.1.

Definition 5.2.5. Let C be the curve in Weierstrass form

$$y^2 = x^3 + ax + b\ .$$

We define the *discriminant* of C to be

$$\Delta := \Delta(C) := 4a^3 + 27b^2.$$

Lemma 5.2.6. *Let C be a cubic curve in very short Weierstrass form (5.3) and let $\overline{C}$ be its projective closure. Then $(\overline{C}, (0 : 1 : 0))$ is an elliptic curve if and only if $\Delta(C) \neq 0$.*

Proof. Notice that if C is defined as in the hypothesis, then $\overline{C}$ always contains the point $(0 : 1 : 0)$, as seen in Example 5.2.3. So to prove the statement it is enough to prove that C is smooth if and only if $\Delta \neq 0$.

Let $f := f(x)$ be the polynomial $x^3 + ax + b$, and notice that the discriminant of f is exactly Δ, Definition 3.2.7.

By studying the partial derivatives of the equation defining C, one can see that C has a singular point if and only if f admits a double root, that is, if and only $\Delta = 0$. □

5.3 The j-invariant

For sake of semplicity, in this section we will always assume to work on a field K of characteristic $\operatorname{Char} K \neq 2, 3$, although the results can be extended also to the case of characteristic 2 and 3. Let $\overline{K}$ denote a fixed algebraic closure of K.

In §5.2 we have defined the an elliptic curve to be a cubic curve together with a point. As seen in Proposition 5.1.4, such a curve always admits a Weierstrass form. In fact, there is no result assuring that such form is unique. One might then ask: can the same cubic admit two different Weierstrass forms? This question can be phrased in a different way: what are the isomorphism of affine curves that preserve the Weierstrass form?

Proposition 5.3.1. *Let K be a field with characteristic different from 2 and 3, and let C be a cubic curve given in very short Weierstrass form. The only change of variables preserving the very short Weierstrass form is*

$$t_u : \begin{cases} x &= u^2 x' \\ y &= u^3 y' \end{cases} \tag{5.7}$$

for some $u \in \overline{K}^*$.

Proof. The generic change of variables can be written as

$$t : \begin{cases} x &= \alpha_1 x' + \alpha_2 y' + \alpha_3 \\ y &= \beta_1 x' + \beta_2 y' + \beta_3 \end{cases}$$

Substituting these expression x and y into the short Weierstrass form and imposing the conditions on the coefficient in order to obtain again a short Weierstrass form, we get that t must be of the form

$$t : \begin{cases} x &= \alpha_1 x' \\ y &= \beta_2 y' \end{cases}$$

with $\alpha_1^3 = \beta_2^2$. From this it follows that $(\alpha_1, \beta_2) = (u^2, u^3)$ for some $u \in \overline{K}^*$. □

Corollary 5.3.2. *Let C and C' be two elliptic curves. Then C and C' are isomorphic if and only if there is a $u \in \overline{K}^*$ such that the change of variable t_u sends the very short Weierstrass form of C to the very short Weierstrass form of C'.*

Proof. Let E and E' denote the very short Weierstrass form of C and C', respectively, and note that E and E' are then isomorphic to C and C', respectively.

If there exists a $u \in \overline{K}^*$ such that t_u sends E to E', it means that E and E' are isomorphic, yealding that C and C' are also isomorphic.

Now assume C and C' to be isomorphic. This implies that E and E' are also isomorphic. But then, by Proposition 5.3.1, the isomorphism between E and E' must be of the form t_u for some $u \in \overline{K}^*$, completing the proof. □

The above result shows that we might have different two elliptic curves in different very short Weierstrass form that are nevertheless isomorphic. Is there an easy to determine whether two elliptic curves (in very short Weierstrass form) are isomorphic? In order to answer, we need the following quantity.

Consider $u \in \overline{K}^*$ and apply the transformation t_u to the curve C with equation $y^2 = x^3 + ax + b$. We get the curve C' with equation $y^2 = x^3 + a'x + b'$ with $a' = a/u^4$ and $b' = b/u^6$. From this it also follows that $\Delta(C') = \Delta(C)/u^{12}$. Can we define a quantity associated to C that is invariant under this kind of transformation?

Definition 5.3.3. Let E be the elliptic curve defined by $y^2 = x^3 + ax + b$. We define the j-invariant of E to the quantity

$$j(E) := 1728\frac{4a^3}{4a^3 + 27b^2} = 2^8 3^3 \frac{a^3}{\Delta}. \tag{5.8}$$

Proposition 5.3.4. *Two elliptic curves over K are isomorphic (over $\overline{K}$) if and only if they have the same j-invariant.*

Moreover, for any $j_0 \in K^*$., there exists an elliptic curve E defined over K, such that $j(E) = j_0$.

Proof. Without loss of generality, we may and do assume that the two elliptic curves are given in very short Weierstrass form, say

$$E\colon y^2 = x^3 + ax + b \quad \text{and} \quad E'\colon y^2 = x^3 + a'x + b' \ .$$

By Lemma 5.3.1, if E and E' are isomorphic, then there exists a $u \in \overline{K}^*$ such that the change of variable t_u as in (5.7) sends E to E'. This means that $a' = a/u^4$ and $b' = b/u^6$, from which it follows that

$$j(E') = 1728\frac{4(a/u^4)^3}{4(a/u^4)^3 + 27(b/u^6)^2} = 1728\frac{4a^3}{4a^3 + 27b^2} = j(E) \ .$$

Conversely, assume that

$$j(E) = 1728\frac{4a^3}{4a^3 + 27b^2} = 1728\frac{4a'^3}{4a'^3 + 27b'^2} = j(E') \ .$$

The equality above yields $a^3 b'^2 = a'^3 b^2$. Then we have three cases.

- If $a = 0$, then $b \neq 0$, as otherwise $\Delta(E) = 0$ and hence $a' = 0$. Then the transformation t_u with $u = (b/b')^{1/6} \in \overline{K}^*$ gives an automorphism between E and E'.
- If $b = 0$ then it follows that $a \neq 0$, as otherwise $\Delta(E) = 0$, and hence $b' = 0$. Then the transformation t_u with $u = (a/a')^{1/4} \in \overline{K}$ gives an automorphism between E and E'.
- If $ab \neq 0$ then $a'b' \neq 0$ and he transformation t_u with $u = (b/b')^{1/6} = (a/a')^{1/4} \in \overline{K}^*$ gives an automorphism between E and E'.

The second statement is left as an exercise for the reader. [Hint: consider an elliptic curve in very short Weierstrass form with $a = b$.] □

5.4 The group law

Let K be any field and fix an algebraic closure $\overline{K}$. Fix an elliptic curve $E = (C, O)$ over K, where C is a smooth cubic over K and $O \in \overline{C}(K)$. We want to define an operation on the set $\overline{C}(K)$ of K-rational points of the projective closure of C.

Lemma 5.4.1. *Let P, Q be two points in $\overline{C}(K)$, and let L be the line passing through P and Q. Then L intersects $\overline{C}$ in a third point R defined over K.*

Proof. By Bezout theorem, a line and a cubic meet in three points, counted with multiplicity. Hence, the intersection between C and L contains another point R, possibly equal to P or Q. All we need to prove is that R is defined over K. To see that, notice that as P and Q are defined over K, so is the line L. Then intersecting L and C consists in solving a cubic equation over K, having already two roots over K. Therefore, by (3.2.6), also the third root is defined over K, from which we conclude that R is a K-rational point of $\overline{C}$. □

We can then define the following operation on the K-rational points of an elliptic curve.

Definition 5.4.2. Let P, Q be two points in $\overline{C}(K)$, and L be the line passing through P and Q. Let $R \in \overline{C}(K)$ be the third point of intersection of L and C (cf. Lemma 5.4.1). Let L' be the line passing through R and O. We define $P + Q$ to be the third point of intersection of L' and C.

Remark 5.4.3. Lemma 5.4.1 ensures that $P + Q$ is well defined and belongs to $\overline{C}(K)$.

Remark 5.4.4. If $P = Q$, then L is the tangent curve to C at $P = Q$. It follows that $2P := P + P$ is obtained by considering the tangent line to C at P.

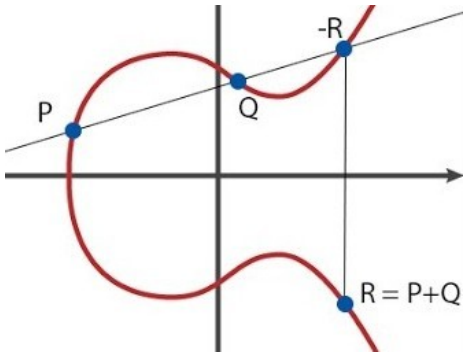


Figure 5.1: Geometric construction of the sum of two points.

Proposition 5.4.5. *The following statements hold:*

(a) the addition $+$ on $\bar{C}(K)$ is well defined;

(b) the addition $+$ is associative and commutative;

(c) O is the neutral element for $+$;

(d) for every $P \in \overline{C}(K)$, there exists the element $-P \in \overline{C}(K)$.

(e) $P + Q + R = \mathcal{O}$ if and only if P, Q, R lie on a line.

Proof. (a) It follows immediately from Lemma 5.4.1.

(b) Exercise. Note that commutativity is almost trivial; associativity is the hard part.

(c) Let L the line passing through P and O. Then $L \cap \bar{C} = \{P, O, Q\}$, from which it follows that $P + O = P$.

(d) Exercise.

(e) Exercise.

□

Corollary 5.4.6. *$(\overline{C}(K), +)$ is an abelian group.*

Proof. Immediate from Proposition 5.4.5. □

Although the sum of point on an elliptic curve is defined in general, if the elliptic curve is given in Weierstrass form, then it is much easier to explicitly write the coordinates of $P+Q$ in terms of the coordinates of P and Q.

Proposition 5.4.7. *Let E be the elliptic curve in Weierstrass form $y^2 = x^3+ax+b$; let $P = (x_1, y_1)$ and $Q = (x_2, y_2)$ be two elements of $E(K)$. Then*

$$P + Q := (x_3, y_3) = (\lambda^2 - x_1 - x_2, -\lambda(x_2 - x_1) - y_1), \tag{5.9}$$

where $\lambda = \frac{y_2-y_1}{x_2-x_1}$;

$$-P = (x_1, -y_1). \tag{5.10}$$

Proof. The line L passing through P and Q has equation $y - y_1 = \lambda(x - x_1)$. We can then substitute y in the equation of E, getting a cubic monic polynomial $f(x)$. Doing the computations, one can check that the coefficient of x^2 is $-\lambda^2$. Since the coefficient of x^2 equals minus the sum of the roots of a cubic monic polynomial, and we already know that x_1 and x_2 are roots of f, we have that the third root, x_3 is $\lambda^2 - x_1 - x_2$. The value of y_3 follows by simply plugging the value x_3 in the equation of L. □

Remark 5.4.8. One can use Proposition 5.4.7 to prove 5.4.5.

Corollary 5.4.9 (Duplication formula)**.** *Let E be the elliptic curve in Weierstrass form $y^2 = x^3 + ax + b$ and let $P = (x_0, y_0)$ be an element of $C(K)$. If $y_0 = 0$, then $2P = O$. If $y_0 \neq 0$, then $2P$ has first coordinate equal to*

$$x_{2P} = \frac{x_0^4 - 2ax_0^2 - 8bx_0 + a^2}{4(x_0^3 + ax_0 + b)} = \frac{x_0^4 - 2ax_0^2 - 8bx_0 + a^2}{4y^2}.$$

Proof. Let L be the tangent line to E at P. Set $F := x^3+ax+b-y^2$. and let $F_x := 3x^2+a, F_y := -2y$ denote the partial derivatives of F with respect to x and y respectively. Then $L\colon F_y(P)(y - y_0) = F_x(P)(x - x_0)$ and $2P$ is the third point of intersection of L and E. If $y_0 = 0$, then $L\colon y = y_0$ and hence the third point is the point at infinity O. If $y_0 \neq 0$, the statement follows from direct computations. □

5.5 Singular cubics

In the previous sections, we focused on *smooth* cubics. In particular, we always considered cubics over K in very short Weierstrass form given by $y^2 = x^3 + ax + b$ with $\Delta := 4a^3 + 27b^2 \neq 0$. One might then wonder: what happens if $\Delta = 0$.

Lemma 5.5.1. *Let C be the curve with equation $y^2 = x^3 + ax + b$. Assume $\Delta(C) = 0$. Then C has exactly one singular point, which is either a node or a cusp.*

Proof. As $\Delta(C) = 0$, we know that the equation $x^3 + ax + b = 0$ has at least a root of multiplicity 2, i.e., $x^3 + ax + b = (x - \alpha)^2(x - \beta)$. This means that $(\alpha, 0)$ is a singular point for C.

Assume $\alpha \neq \beta$. Then, shifting x by α we see that C is isomorphic to the curve $y^2 = x^2(x - \beta')$, hence it has a node.

If $\alpha = \beta$, then by shifting x by α we see that C is isomorphic to the curve $y^2 = x^3$, hence it has a cusp. □

Remark 5.5.2. First notice that a cubic curve C can have at most one singular point. If it had two, then the line passing through these two singular points would intersect C with multiplicity at least 4, contradicting Bezout's theorem.

Moreover, if C is singular, then its rational points can be studied by projecting from the singular point, using the same argument as in the case for conics. (cf. Exercises 5.6).

Let E/K be a cubic with a node $P \in E(K)$, with K a field of characteristic different from 2 and 3. Then we can write E as $y^2 = x^3 + ax + b$ with $\Delta(E) = 0$. As we assumed P to be a node defined over K, the polynomial $x^3 + ax + b$ completely factors over K as

$$x^3 + ax + b = (x - \alpha)(x - \beta)^2$$

with $P = (\beta, 0)$. The slopes of the tangent lines to E in P are $\pm\sqrt{\beta - \alpha}$.

Definition 5.5.3. A cubic curve $E\colon y^2 = (x-\alpha)(x-\beta)^2$ over K is defined to be *split* if $\sqrt{\beta - \alpha} \in K$, i.e., if the tangent lines to the curve in the node $(\beta, 0)$ are defined over K; *non-split* otherwise.

This definition will play an important role in chapter 9.

5.6 Exercises

The exercises marked with * are harder; those marked with ! are important.

Exercise 5.6.1. ! Find all the $\mathbb{Q}$-rational points of the singular cubic $y^2 = x^3$.

Exercise 5.6.2. Put the Fermat cubic $u^3 + v^3 = 1$ in Weierstrass form.

Exercise 5.6.3. * Find a rational solution of the following equation: $\frac{x}{y+z} + \frac{y}{x+z} + \frac{z}{x+y} = 4$.

Exercise 5.6.4. In Lemma 5.5.1 we have seen that, in general, a cubic curve can only have two kinds of singular points: either a node or a cusp. Nevertheless, over $\mathbb{R}$, we can have *three* different looking singular cubic curves, as shown in (5.2).

(a) For each type of singularity in the picture, find a cubic over $\mathbb{R}$ realizing it.

(b) Determine whether an isolated point is a cusp or a node.

Exercise 5.6.5. Prove Proposition 5.3.4.ii) . [Extra*: For every fixed j_0, how many different, yet isomorphic, elliptic curves in Weierstrass form with j invariant equal to j_0 are there?]

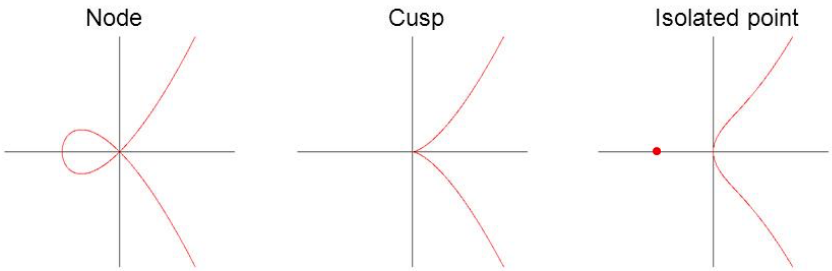


Figure 5.2: The three possible types of singular cubics over $\mathbb{R}$.

Chapter 6

Isogenies of elliptic curves

After giving an elliptic curve a group structure, it is very natural to look for morphisms that preserve this structure analogously to chapter 2. In doing so, we will use the theory recalled in chapter 4.

6.1 Divisors on elliptic curves

Let K be any field and $\overline{K}$ a fixed algebraic closure of K. Let E be an elliptic curve over K and let D be a divisor on E, Definition 4.6.1. Also, recall Definition 4.7.5 for $\mathcal{L}(D)$.

Theorem 6.1.1 (Riemann–Roch for elliptic curves)**.** *Let E be an elliptic curve and D any divisor on E. Then*

$$\ell(D) - \ell(-D) = \deg D \, .$$

Example 6.1.2. We again use Example 4.6.7 and Example 4.7.6. As $D_2 \sim_{\text{lim}} 3\mathcal{O}$, we have that $\mathcal{L}(D_2) \cong \mathcal{L}(3\mathcal{O})$. As $\deg -3\mathcal{O} = -3 < 0$, from Facts 4.7.7a it follows that $\ell(-3\mathcal{O}) = 0$ and hence, by Theorem 6.1.1, it follows that $\ell(D_2) = \ell(3\mathcal{O}) = 3$.

Lemma 6.1.3. *Let E be an elliptic curve over K and consider $P, Q \in E$. Then $(P) \sim_{lin} (Q)$ if and only if $P = Q$.*

Proof. The implication from right to left is trivial, so we only have to show the one from left to right. Assume then $(P) \sim_{\text{lin}} (Q)$, that is, there exists a function $f \in K(C)^*$ such that $\text{div}(f) = (P) - (Q)$. Then $f \in \mathcal{L}(Q)$. As $\deg(Q) = 1$, by Facts 4.7.7 we have that $\ell(-(Q)) = 0$ and so, using Theorem 6.1.1, it follows that $\ell(Q) = 1$ and it contains the constant functions, yielding $\mathcal{L}(Q) \cong K$. Hence f is a constant and its divisor is then $0 = (P) - (Q)$, that is, $(P) = (Q)$ and so $P = Q$. □

Lemma 6.1.4. *Let E be an elliptic curve over a field K. For any $D \in \text{Div}^0(E)$ there exists a unique point $P \in E$ such that $D \sim_{lin} (P) - (O)$.*

Proof. Notice that $\deg D + (O) = 1$ ane hence, from Facts 4.7.7 and Theorem 6.1.1, it follows that $\ell(D + (O)) = 1$. Let f be a generator of $\mathcal{L}(D + (O))$. This means that

$$\text{div}\, f \geq D + (O) \quad \text{and} \quad \deg \text{div}\, f = 0 \, ,$$

therefore $\text{div}\, f = (P) - (O) - D$ for some point $P \in E$, from which it follows that $D \sim_{\text{lin}} (P) - (O)$. □

Theorem 6.1.5. *Let E be an elliptic curve with fixed point O. Then the map*

$$\begin{aligned}\kappa\colon E &\to \operatorname{Pic}^0 E\\ P &\mapsto [(P)-(O)]\end{aligned}$$

is a group isomorphism.

Proof. Without loss of generality, we assume E to be a smooth projective cubic in $\mathbb{P}^2(X,Y,Z)$ having a flex point in O with tangent line $Z=0$. For example, this is always the case for elliptic curves in very short Weierstrass form.

First notice that $\kappa(O) = [(O)-(O)] = [(0)]$, which is the class of the divisor of a constant function, hence it is the zero element of $\operatorname{Pic}^0 E$. Then we prove that κ is a group homomorphism, that is, $\kappa(P+Q) = \kappa(P)+\kappa(Q)$. Let f be the equation of the line passing through P and Q and let R be its third point of intersection with E. Let g be the equation of the line passing through O and R and notice that its third point of intersection with E is exactly $P+Q$, by definition of the sum on E, Definition 5.4.2. Consider the functions f/Z and g/Z on E. As Z intersects E in O with multiplicity 3, we have

$$\begin{aligned}\operatorname{div} f/Z &= (P)+(Q)+(R)-3(O),\\ \operatorname{div} g/Z &= (R)+(P+Q)-2(O).\end{aligned}$$

It follows that

$$\operatorname{div} f/g = (P)+(Q)-(O)-(P+Q) \sim_{\text{lin}} 0,$$

that is,

$$[(P)+(Q)-(O)-(P+Q)] = 0\,.$$

But then

$$\begin{aligned}0 = [(P)+(Q)-(O)-(P+Q)] &= [(P)-(O)+(Q)-(O)-(O)+(O)-(P+Q)+(O)]\\ &= [(P)-(O)]+[(Q)-(O)]-[(O)-(O)]-[(P+Q)-(O)]\\ &= \kappa(P)+\kappa(Q)-0-\kappa(P+Q)\end{aligned}$$

and therefore

$$\kappa(P)+\kappa(Q) = \kappa(P+Q)\,,$$

proving that κ is a group homomorphism.

Next we show that the map is injective. Take $P,Q\in E$ such that $[(P)-(O)] = [(Q)-(O)]$. This means that $(P)-(O) \sim_{\text{lin}} (Q)-(O)$ and hence $(P)\sim_{\text{lin}}(Q)$. Then $P=Q$ from Lemma 6.1.3.

Finally, notice that the surjectivity of κ directly follows from Lemma 6.1.4. □

Corollary 6.1.6. *Let E be an elliptic curve and $D=\sum n_P(P)$ a divisor on E. Then D is principal if and only if $\deg D = 0$ and $\sum[n_P]P = O\in E$.*

Proof. First assume that D is principal. Then by Facts 4.6.8b it follows that $\deg D = 0$. So $[D]\in\operatorname{Pic}^0 E$; as D is principal, $[D]=0\in\operatorname{Pic}^0 E$. By Theorem 6.1.5 we have that the sums in $\operatorname{Pic}^0 E$ and E coincide, and hence $D=O$.

Conversely, assume that $\deg D=0$ and $\sum[n_P]P=O$. Then, as κ is an isomorphism, $[D]=0\in\operatorname{Pic}^0 E$ and hence it is a principal divisor. □

Remark 6.1.7. Corollary 6.1.6 proves Proposition 5.4.5(e).

6.2 Isogenies of elliptic curves

As done with complex tori, we are interested in maps between elliptic curves that preserve the group structure. Let K fe any field and $\overline{K}$ an algebraic closure of K. Let $E_1 = (C_1, O_1)$ and $E_2 = (C_2, O_2)$ be two elliptic curves over K.

Definition 6.2.1. We define an *isogeny* from E_1 to E_2 over K to be a morphism $\phi\colon C_1 \to C_2$ defined over K such that $\phi(O_1) = O_2$.

Remark 6.2.2. From Lemma 4.4.3 it follows immediately that non-constant isogenies are surjective. In particular, $\phi(E_1)$ is either $\{\mathcal{O}_2\}$ or E_2.

Lemma 6.2.3. *Let $\phi\colon E_1 \to E_2$, $\psi\colon E_2 \to E_3$ be two isogenies of elliptic curves. Then*

(a) $\psi \circ \phi\colon E_1 \to E_3$ is an isogeny.

(b) $\deg(\psi \circ \phi) = \deg \psi \cdot \deg \phi$.

Proof. (a) Clearly $\psi \circ \phi(O_1) = O_3$.

(b) Set $m := \deg \phi$ and $n := \deg \psi$ and let R be a point of E_3. Then $\#\psi^{-1}(R) = n$, counting points with multiplicity. Write $\psi^{-1}(R) = \{Q_1, \dots, Q_n\}$. Then for every $i = 1, \dots, n$ we have that $\#\phi^{-1}(Q_i) = m$, again counting with multiplicity. We can then conclude that $\#(\psi \circ \phi)^{-1}(R) = mn$, counting with multiplicity.

□

Definition 6.2.4. Given two elliptic curves E_1, E_2, we denote the set of isogenies from E_1 to E_2 defined over K by

$$\mathrm{Hom}_K(E_1, E_2) := \{\phi\colon E_1 \to E_2 \mid \phi \text{ isogeny over } K\ \}.$$

Given an elliptic curve E, we define the set of *endomorphisms* of E as

$$\mathrm{End}_K(E) := \mathrm{Hom}_K(E, E).$$

The set of invertible elements of $\mathrm{End}_K(E)$ is denoted by $\mathrm{Aut}_K(E)$.

Remark 6.2.5. The set $\mathrm{Hom}_K(E_1, E_2)$ can be endowed with an abelian group structure (and hence of $\mathbb{Z}$-module) by defining the sum $\phi + \psi\colon P \mapsto \phi(P) + \psi(P)$.

This structure is inherited by $\mathrm{End}_K(E)$, that can also be endowed with the composition: $(\mathrm{End}_K(E), +, \circ)$ is called *the endormorphism ring of* E.

As $\mathrm{Aut}_K(E)$ is set of invertible elements of $\mathrm{End}_K(E)$ and so $(\mathrm{Aut}_K(E), \circ)$ has the structure of group; it is called the *automorphism group* of E.

Example 6.2.6. The first and easiest example of an isogeny comes from the multiplication by an integer. Let E be an elliptic curve and let $m \in \mathbb{Z}$ be an integer. We define the map $[m]\colon E \to E$ by sending a point P to

$$[m](P) := \begin{cases} \underbrace{P + \ldots + P}_{m \text{ times}} & \text{if } m > 0 \\ \underbrace{(-P) + \ldots + (-P)}_{-m \text{ times}} & \text{if } m < 0\ . \\ \mathcal{O} & \text{if } m = 0 \end{cases}$$

One can immediately check that $[m]$ is indeed an isogeny.

Proposition 6.2.7. *Let E be an elliptic curve over a field K of characteristic 0. The map $[\ ]\colon \mathbb{Z} \to \mathrm{End}(E)$ is an injective ring homomorphism.*

Proof. Checking that $[\ ]$ is a ring homomorphism is immediate: in fact, $[m+n] = [m] + [n]$ and $[mn] = [m] \circ [n]$.

First notice that the duplication formula (cf. 7.4) shows that $[2] \neq 0$. Then, over $\overline{K}$, there are three non-trivial 2-torsion points (use the duplication formula). Let P_0 be one of them. Then $[m](P_0) = P_0 \neq 0$ for every odd m, in particular for every odd prime. This shows that the kernel of $[\ ]$ is trivial. □

Remark 6.2.8. When K has characteristic zero, the map $[\ ]$ is usually also surjective, that is, $\mathrm{End}_K(E) \cong \mathbb{Z}$.

When this is not the case, we say that E has *complex multiplication*.

Example 6.2.9. Let E be the elliptic curve $y^2 = x^3 - x$ over $K = \mathbb{C}$ (but any field containing $\mathbb{Q}(i)$ is also fine). Beside $\mathbb{Z}$, in $\mathrm{End}_K(E)$ there is also the element

$$[i]\colon (x, y) \to (-x, iy).$$

Indeed it turns out that $\mathrm{End}_K(E) \cong \mathbb{Z}[i]$.

Definition 6.2.10. Let E be an elliptic curve over K and m an integer. We define the m-torsion points of E over K, denoted by $E(K)[m]$, as the elements in the kernel of $[m]$, that is:

$$E(K)[m] := \{P \in E(K) \mid [m]P = \mathcal{O}\}.$$

Remark 6.2.11. Trivially

$$E(K)_{\mathrm{tors}} = \bigcup_{m=1}^{\infty} E(K)[m].$$

Moreover, by looking at the degree of the multiplication polynomials, one can see that $\#E(\overline{K})[m] = m^2$. Hence, in general, $\#E(K)[m] \leq m^2$.

Using the group structure, one can consider another important family of self-maps of an elliptic curve, the translations, defined as follow. Together the isogenies, they are the building blocks of all the morphisms between elliptic curves, as shown by Proposition 6.2.14.

Definition 6.2.12. Let $E = (C, O)$ be an elliptic curve over a field K and take $T \in E(K)$. We define *the translation by T* as the morphism

$$\tau_P\colon C \to C\ ,\ P \mapsto P + T\ .$$

Remark 6.2.13. Notice that, although τ_T is defined using the group structure of E, it does not respect it as it sends O to T. Indeed, for $T \neq O$, the morphism τ_T is not an isogeny, but only a morphism of curves.

Proposition 6.2.14. *Let $E_1 = (C_1, O_1), E_2 = (C_2, O_2)$ be two elliptic curves and let $F\colon C_1 \to C_2$ be a morphism of curves. Then there exists a point $T \in E_2$ and an isogeny $\phi\colon E_1 \to E_2$ such that*

$$F = \tau_T \circ \phi\ .$$

Proof. Set $T := F(O_1)$ and consider the translation $\tau_{-T}\colon E_2 \to E_2$ defined by $P \mapsto P - T$. Then the composition $\tau_{-T} \circ F = \phi$ is an isogeny, as it sends O_1 to O_2. As translations are obviosuly invertible, we conclude that

$$F = \tau_T \circ \phi\,,$$

proving the statement. □

Isogenies are particularly interesting in the theory of elliptic curves because they preserve the group structure of the curves. The following is the main result of the section.

Theorem 6.2.15. *Let $\phi\colon E_1 \to E_2$ be an isogeny. Then for every $P, Q \in E_1$ it holds that*

$$\phi(P+Q) = \phi(P) + \phi(Q).$$

Proof. If $\phi = O_2$ then the statement is trivially true. So assume ϕ is not constant and consider the induced homomorphism

$$\phi_*\colon \operatorname{Pic}^0 E_1 \to \operatorname{Pic}^0 E_2$$

sending $[\sum n_i P_i]$ to $[\sum n_i \phi(P_i)]$. For $i = 1, 2$ we also have the group isomorphisms

$$\kappa_i\colon E_i \to \operatorname{Pic}^0 E_i$$

defined by $P \mapsto [P - O_i]$. As $\phi(O_1) = O_2$, we have the following commutative diagram.

$$\begin{array}{ccc} E_1 & \xrightarrow{\kappa_1} & \operatorname{Pic}^0 E_1 \\ \downarrow{\scriptstyle \phi} & & \downarrow{\scriptstyle \phi_*} \\ E_2 & \xrightarrow[\kappa_2]{} & \operatorname{Pic}^0 E_2 \end{array}$$

As ϕ_* and κ_1 are group homomorphisms and κ_2 is injective, the statement follows. □

6.3 The dual isogeny

In this subsection we are going to prove that being isogenous induces an equivalence relation on the set of elliptic curves over a given field K. In these notes we will only prove it in characteristic 0, but Corollary 6.3.6 holds in any characteristic: see [9, §III.6] for a more general proof. As in the previous section, let K be any field and let K be a fixed algebraic closure of K, assume $\operatorname{Char} K = 0$; let $E_1 = (C_1, O_1), E_2 = (C_2, O_2)$ be two elliptic curves.

Proposition 6.3.1. *Let $\phi\colon E_1 \to E_2$ be a non-zero isogeny over K.*

(a) For every $Q \in E_2$, the pre-image $\phi^{-1}(Q)$ contains exactly $\deg\phi$ distinct points. In particular, $\#\ker\phi = \deg\phi$.

(b) The map $\ker\phi \to \operatorname{Aut}(\overline{K}(E_1)/\phi^*\overline{K}(E_2))$, $T \mapsto \tau_T^*$ is a group isomorphism.

(c) $\overline{K}(E_1)$ is a Galois extension of $\phi^*\overline{K}(E_2)$.

Proof. (a) As we are in characteristic 0, every extension is separable. As elliptic curves are smooth, we can then use the final part of the proof of [4, II.6.9] to prove our statement. The second statement is just a special case, as $\ker\phi = \phi^{-1}(O)$.

(b) Take $T \in \ker \phi$ and $f \in \overline{K}(E_2)$, then $\phi \circ \tau_T = \phi$ and hence

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

In other words, τ_T^* fixes $\phi^*\overline{K}(E_2)$ as automorphism of $\overline{K}(E_1)$. Moreover, as $\tau_{T+S} = \tau_T \circ \tau_S$, the map is a group homomorphism. From (a) we know that $\#\ker\phi = \deg\phi$ and from Galois theory, again because we are working in characteristic 0, we know that

$$\#\operatorname{Aut}(\overline{K}(E_1)/\phi^*\overline{K}(E_2)) \leq \deg\phi\ .$$

To prove that the map is an isomorphism then we are only left to prove that the map is injective. Assume that τ_T^* fixes the whole $\overline{K}(E_1)$, then for every $f \in \overline{K}(E_1)$ we have $f = \tau_T^* f$ and hence, in particular,

$$f(\mathcal{O}) = \tau_T^* f(\mathcal{O}) = f(T).$$

As this is true for all functions of E_1, including the projections on the coordinates, this implies that $T = O$, proving the statement.

(c) From (a) and (b) it follows that

$$\#\operatorname{Aut}(\overline{K}(E_1)/\phi^*\overline{K}(E_2)) = \deg\phi =: [\overline{K}(E_1) : \phi^*\overline{K}(E_2)]\ ,$$

i.e., $\overline{K}(E_1)/\phi^*\overline{K}(E_2)$ is a Galois extension.

□

Corollary 6.3.2. *Let K be a field with characteristic 0. Let E_1, E_2, E_3 be three elliptic curves over a field K and $\phi\colon E_1 \to E_2$ and $\psi\colon E_1 \to E_3$ be isogenies defined over K. If $\ker\phi \subseteq \ker\psi$, then there exists an isogeny $\lambda\colon E_2 \to E_3$ such that $\psi = \lambda \circ \phi$.*

Proof. By Proposition 6.3.1(c) we know that $\overline{K}(E_1)/\phi^*\overline{K}(E_2)$ is a Galois extension; by Proposition 6.3.1(b) we know that

$$\ker\phi \cong \operatorname{Aut}(\overline{K}(E_1)/\phi^*\overline{K}(E_2)) \text{ and}$$
$$\ker\psi \cong \operatorname{Aut}(\overline{K}(E_1)/\psi^*\overline{K}(E_3))\ .$$

As $\ker\phi \subseteq \ker\psi$, we have that every element of $\operatorname{Aut}(\overline{K}(E_1)/\phi^*\overline{K}(E_2))$ fixes $\psi^*\overline{K}(E_3)$ too, hence

$$\psi^*\overline{K}(E_3) \subset \phi^*\overline{K}(E_2) \subset \overline{K}(E_1).$$

Hence we have an injection $\iota\colon \psi^*\overline{K}(E_3) \to \phi^*\overline{K}(E_2)$ and so, by Lemma 4.4.4(b) we know that there exists a non-constant map $\lambda\colon E_2 \to E_3$ such that $\lambda^* = \iota$. This means that $\phi^*\lambda^*\overline{K}(E_3) = \psi^*\overline{K}(E_3)$ and hence $\psi^* = \phi^*\lambda^* = (\lambda\circ\phi)^*$. From this we conclude that $\psi = \lambda \circ \phi$, as desired. We are left to show that λ is an isogeny. This is easy as ϕ and ψ are isogenies and hence $\lambda(\mathcal{O}) = \lambda(\phi(\mathcal{O})) = \psi(\mathcal{O}) = \mathcal{O}$. □

Let $\phi\colon E_1 \to E_2$ be a non-constant isogeny over K and consider the induced map $\phi^*\colon \operatorname{Pic}^0 E_2 \to \operatorname{Pic}^0 E_1$. For $i = 1, 2$ recall that we have the isomorphisms

$$\kappa_i\colon E_i \to \operatorname{Pic}^0 E_2\ .$$

We then have the following diagram.

$$\begin{array}{ccc} E_2 & \xrightarrow{\kappa_2} & \operatorname{Pic}^0 E_2 \\ & & \downarrow{\scriptstyle \phi^*} \\ E_1 & \xleftarrow{\kappa_1^{-1}} & \operatorname{Pic}^0 E_1 \end{array}$$

Our goal is to construct an isogeny from E_2 to E_1. Notice that if $P \in E_1$ and $Q := \phi(P) \in E_2$, then $\kappa_1^{-1} \circ \phi^* \circ \kappa_2(Q) = [\deg \phi](P)$ by 4.6.11(a). This gives us a hint to follow. Unfortunately, a priori it is not clear that $\kappa_1^{-1} \circ \phi^* \circ \kappa_2$ is an isogeny. In fact, it is not even clear that it is a rational map, as if we start with $Q \in E_2$, finding a point $P \in E_1$ such that $\phi(P) = Q$ involves taking roots of polynomials. Indeed, the situation is a bit more subtle.

Lemma 6.3.3. *Let K be a field with $\operatorname{Char} K = 0$, E_1, E_2 two elliptic curves over K and $\phi\colon E_1 \to E_2$ an isogeny of degree m. Fix a $Q \in E_2$. Then the following equality holds:*

$$\sum_{P \in \phi^{-1}(Q)} P - \sum_{T \in \ker \phi} T = mP \,,$$

for any $P \in \phi^{-1}(Q)$.

Proof. From 6.3.1(a) we know that $\ker \phi$ and $\phi^{-1}(Q)$ both contain exactly m points, say

$$\begin{aligned} \ker \phi &= \{T_1 = O, T_2, \dots, T_m\} \,, \\ \phi^{-1}(Q) &= \{P_1, \dots, P_m\} = \\ &= \{P_1 + T_1, \dots, P_1 + T_m\} \,. \end{aligned}$$

First we prove that for every $P, P' \in \phi^{-1}(Q)$ one has $mP = mP'$. As $\ker \phi$ is a subgroup of order m of E_1 all its elements have order dividing m. Now consider $P, P' \in \phi^{-1}(Q)$. Clearly $P - P' \in \ker \phi$ and hence $mP - mP' = \mathcal{O}$, that is, $mP = mP'$.

Now we show that $\sum_{P \in \phi^{-1}(Q)} P - \sum_{T \in \ker \phi} T = mP$ for some $P \in \phi^{-1}(Q)$. Using the descriptions above, we can rewrite the sum as

$$\sum_{P \in \phi^{-1}(Q)} P - \sum_{T \in \ker \phi} T = \sum_{i=1}^{m} P_i - T_i \,.$$

As $P_i = P_1 + T_i$, the sum simplifies to mP_1, proving the statement. □

Theorem 6.3.4. *Let K be a field with $\operatorname{Char} K = 0$. Let E_1, E_2 be two elliptic curves over K and $\phi\colon E_1 \to E_2$ a non-zero isogeny of degree m.*

(a) There exists a unique isogeny $\hat{\phi}\colon E_2 \to E_1$ such that $\hat{\phi} \circ \phi = [m]$.

(b) The map $\hat{\phi}$ is given by the composition

$$E_2 \xrightarrow{\kappa_2} \operatorname{Div}^0 E_2 \xrightarrow{\phi^*} \operatorname{Div}^0 E_1 \xrightarrow{\Sigma} E_1$$

where

$$\kappa_2\colon E_2 \to \operatorname{Div}^0 E_2, \qquad Q \mapsto (Q) - (O) \,,$$

$$\begin{aligned} \phi^*\colon \operatorname{Div}^0 E_2 &\to \operatorname{Div}^0 E_1, & (Q)-(O) &\mapsto \phi^*(Q)-\phi^*(O) \\ \sum\colon \operatorname{Div}^0 E_1 &\to E_1, & \sum n_P(P) &\mapsto \sum [n_P]P\,. \end{aligned}$$

Proof. (a) First we show the uniqueness. Assume there exist $\hat{\phi}$ and $\hat{\phi}'$ such that

$$\hat{\phi}\circ\phi = [m] = \hat{\phi}'\circ\phi\,.$$

Then $(\hat{\phi}'-\hat{\phi})\circ\phi = 0$. As ϕ is non-constant, we deduce that $\hat{\phi}'-\hat{\phi}=0$, i.e., $\hat{\phi}'=\hat{\phi}$, as desired.

As ϕ has degree m, we know that $\#\ker\phi = m$ by 6.3.1, and all the points in it are distinct. This means that the order of each of them divides m ad hence $\ker\phi \subseteq \ker[m]$. By Corollary 6.3.2 we then conclude that there exists an isogeny $\hat{\phi}\colon E_2 \to E_1$ such that $p\hat{h}i\circ\phi = [m]$.

(b) Let $Q \in E_2$ and denote the composition in the statement by ϕ'. Notice that ϕ' clearly is an isogeny. As we are working in characteristic 0, we know that $\phi^{-1}(Q)$ contains exactly m distinct points, 6.3.1(a); the same holds also for $\ker\phi$. Then $\phi^*(Q-\mathcal{O}) = \sum_{P\in\phi^{-1}(Q)} P - \sum_{T\in\ker\phi} T$ by the definition of ϕ^*, see 4.6.9 and 4.6.10. But then, from Lemma 6.3.3, we obtain $\sum(\phi^*(Q-\mathcal{O})) = [m]P$, that is, $\phi'(Q) = [m]P$. This means that ϕ satisfies the condition $\phi'\circ\phi = [m]$, and by the previous point we know that there is a unique isogeny with such a property, namely $\hat{\phi}$, hence $\phi' = \hat{\phi}$.

□

Definition 6.3.5. If $\phi\colon E_1 \to E_2$ is a non-constant isogeny, we define the *dual isogeny* $\hat{\phi}\colon E_2 \to E_1$ to be the one defined in Theorem 6.3.4.

If $\phi = O_2$, then we define $\hat{\phi} = O_1$

Corollary 6.3.6. *Let $\mathcal{E}_K$ denote the set of all elliptic curves over a field K. Then being isogenous defines an equivalence relation on $\mathcal{E}_K$.*

Proof. The statement is true over any field, but here we prove it only in characteristic 0, using previous result.

As the identity is an isogeny, every elliptic curve is isogenous to itself, proving reflexivity.

Let E_1, E_2, E_3 be three elliptic curves and assume there are isogenies $\phi\colon E_1 \to E_2$ and $\psi\colon E_2 \to E_3$. Then clearly $\psi\circ\phi\colon E_1 \to E_3$ is an isogeny, proving transitivity.

Finally, the existence of the dual isogeny proves the reflexivity. □

Finally, we study some properties of the dual isogeny.

Proposition 6.3.7. *Let $\phi\colon E_1 \to E_2$ be an isogeny of degree m.*

(a) Then $\phi\circ\hat{\phi} = [m]$ on E_2 and $\hat{\phi}\circ\phi = [m]$ on E_1.

(b) Let $\lambda\colon E_2 \to E_3$ be another isogeny. Then $\widehat{\lambda\circ\phi} = \hat{\phi}\circ\hat{\lambda}$.

(c) Let $\psi\colon E_1 \to E_2$ be another isogeny. Then $\widehat{\phi+\psi} = \hat{\phi}+\hat{\psi}$.

(d) For all $n \in \mathbb{Z}$ it holds $\widehat{[n]} = [n]$ and $\deg[n] = n^2$.

(e) $\deg\hat{\phi} = \deg\phi$.

(f) $\hat{\hat{\phi}} = \phi$.

Proof. [9, Theorem III.6.2]. □

Corollary 6.3.8. *Let E_1, E_2 be two elliptic curves. The degree map*

$$\deg\colon \operatorname{Hom}(E_1, E_2) \to \mathbb{Z}$$

is a positive definite quadratic form.

Before proceeding with the proof we recall the following definitions.

Definition 6.3.9. If A is an abelian group, a function

$$d\colon A \to \mathbb{R}$$

is a *quadratic form* if

- $d(a) = d(-a)$ for every $a \in A$ and
- the pairing $A \times A \to \mathbb{R}$ defined by $(a, b) \mapsto d(a+b) - d(a) - d(b)$ is bilinear.

A quadratic form $d\colon A \to \mathbb{R}$ is *positive definite* if $d(a) \geq 0$ for every $a \in A$ and $d(a) = 0$ if and only if $a = 0$.

Proof of Corollary 6.3.8. We only need to prove that the induced pairing is bilinear. Consider $\alpha, \beta \in \operatorname{Hom}(E_1, E_2)$ and set $b(\alpha, \beta) := \deg(\alpha + \beta) - \deg(\alpha) - \deg(\beta) \in \mathbb{Z}$. Using the injection $[\,]\colon \mathbb{Z} \to \operatorname{End}(E_1)$, we can consider the multiplication $[b(\alpha, \beta)] \in \operatorname{End}(E_1)$. Using Proposition 6.3.7 we get the following equalities,

$$\begin{aligned}
[b(\alpha,\beta)] &= [\deg(\alpha+\beta)] - [\deg(\alpha)] - [\deg(\beta)] \\
&= (\alpha+\beta) \circ \widehat{(\alpha+\beta)} - \alpha \circ \hat{\alpha} - \beta \circ \hat{\beta} \\
&= \alpha \circ \hat{\beta} + \hat{\alpha} \circ \beta \,.
\end{aligned}$$

From this it follows that $[b(m\alpha, \beta)] = m(\alpha \circ \hat{\beta} + \hat{\alpha} \circ \beta) = [mb(\alpha, \beta)]$. As the map $[\,]$ is injective, we conclude that $b(m\alpha, \beta) = mb(\alpha, \beta)$. The linearity for the second argument is analogous. This shows that b is bilinear, concluding the proof. □

6.4 The endomorphism ring

In this subsection we characterize the ring of endomorphisms of an elliptic curve. Let $E = (C, O)$ be an elliptic curve over a field K.

Definition 6.4.1. We denote by $\operatorname{End}(E)$ the set of endomorphisms of E, that is, the set of isogenies $\phi\colon E \to E$.

Lemma 6.4.2. *The set* $\operatorname{End}(E)$*, endowed with the pointwise addition and the composition has the structure of a ring,* $(\operatorname{End}(E), +, \circ, O = [0], [1])$.

Proof. Exercise. □

Remark 6.4.3. Notice that, in $\mathrm{End}(E)$, the addition is commutative but the multiplication does not need to be so.

Proposition 6.4.4. *The ring* $\mathrm{End}(E)$ *has characteristic* 0 *and no zero-divisors.*

Proof. Proposition 6.2.7 tells us that $\mathbb{Z}$ embedds into $\mathrm{End}(E)$, therefore $\mathrm{End}(E)$ has characteristic 0. To show that there are no zero-divisors, consider $\phi, \psi \in \mathrm{End}(E) \setminus \{0\}$. From Lemma 6.2.3 we know that $\deg(\phi \cdot \psi) = \deg(\phi \circ \psi) = \deg(\phi)\deg(\psi)$. If $\phi \cdot \psi = \mathcal{O}$ then $\deg(\phi \cdot \psi) = 0$ and hence either $\deg \psi = 0$ or $\deg \phi = 0$, hence either $\psi = \mathcal{O}$ or $\phi = \mathcal{O}$, contradicting the initial hypothesis. □

Then recall that we have seen that if ϕ is an isogeny of E, then there exists another isogeny $\hat{\phi}$, *the dual isogeny*, such that $\phi \circ \hat{\phi} = [\deg \phi]$ and $\hat{\hat{\phi}} = \phi$.

Definition 6.4.5. We define the anti-involution

$$\hat{}\colon \mathrm{End}(E) \to \mathrm{End}(E)\ ,\ \phi \mapsto \hat{\phi}\ .$$

Remark 6.4.6. The dual map $\hat{}$ defined *anti*-involution because $\widehat{f \cdot g} = \hat{g} \cdot \hat{f}$. Moreover, and if $\phi \neq O$, then $\phi \cdot \hat{\phi} = [d]$, where $d = \deg \phi \geq 0$, see Proposition 6.3.7(a).

The endomorphism ring is very well studied, and the following result gives a very good grasp of its structure.

Lemma 6.4.7. *Let* E_1, E_2 *be two elliptic curves. Then* $\mathrm{Hom}(E_1, E_2)$ *is a free* $\mathbb{Z}$*-module of rank at most* 4*.*

Proof. [9, Corollary III.7.5]. □

Theorem 6.4.8. *The endomorphism ring* $\mathrm{End}(E)$ *of an elliptic curve* E *over a field* K *is a free* $\mathbb{Z}$*-module of rank at most* 4*. More precisely, it is one of the following types of rings:*

(a) $\mathbb{Z}$*,*

(b) an order in an imaginary quadratic extension of $\mathbb{Q}$*,*

(c) an order in a quaternion algebra over $\mathbb{Q}$*.*

If $\mathrm{Char}\, K = 0$*, then* $\mathrm{End}(E)$ *can only be of type (a) or (b); if* $\mathrm{Char}\, K > 0$*, then* $\mathrm{End}(E)$ *can only be of type (b) or (c).*

Proof. The first statements are [9, Corollary III.9.4]. For the last statement, just notice that the Frobenius is always an isogeny for an elliptic curve over a field with positive characteristic. □

The theorem above gives the motivation for the following definition.

Definition 6.4.9. Let E be an elliptic curve over a field K.
If $\mathrm{Char}\, K = 0$ and

- $\mathrm{End} \cong \mathbb{Z}$, then E is called *ordinary*;
- $\mathrm{End}(E)$ has rank 2, then E is called *singular*.

If $\mathrm{Char}\, K > 0$ and

- $\mathrm{End}(E)$ has rank 2, then E is called *ordinary*;
- $\mathrm{End}(E)$ has rank 4, then E is called *supersingular*.

6.5 Automorphisms of elliptic curves

Let $E = (C, O)$ be an elliptic curve over a field K, and consider the endomorphism ring $\mathrm{End}(E)$.

Definition 6.5.1. We define an *automorphism* of E to be an invertible element of $\mathrm{End}(E)$.
We denote by $\mathrm{Aut}(E) \subseteq \mathrm{End}(E)$ the subset of automorphisms.

Lemma 6.5.2. *The subset* $\mathrm{Aut}(E) \subseteq \mathrm{End}(E)$*, endowed with the composition, is a subgroup.*

Proof. Trivial. □

The following theorem gives us a complete description of the structure of $\mathrm{Aut}(E)$ when $\mathrm{Char}\, K > 3$ in terms of the j-invariant of E. Analogous statements hold in the remaining cases of characteristic 2 and 3.

Theorem 6.5.3. *Let E be an elliptic curve over a field K, with $\mathrm{Char}\, K \neq 2, 3$. The following statement holds.*

$$\mathrm{Aut}\, E \cong \begin{cases} \mathbb{Z}/2\mathbb{Z} \text{ if } j(E) \neq 0, 1728; \\ \mathbb{Z}/4\mathbb{Z} \text{ if } j(E) = 1728; \\ \mathbb{Z}/6\mathbb{Z} \text{ if } j(E) = 0. \end{cases}$$

Proof. As $\mathrm{Char}\, K \neq 2, 3$, the curve E can be brought into very short Weierstrass form, Proposition 5.1.4. Proposition 5.3.1 tells us that the only isomorphisms of elliptic curves preserving the Weierstrass form are of the form

$$x' = u^2 x\,, \quad y' = u^3 y$$

for some invertible element $u \in \overline{K}^\times$, sending the elliptic curve with coefficients a, b to the elliptic curve with coefficients $u^4 a, u^6 b$. Let ψ be such an isomorphism. In order for ψ to be an automorphism of E, we must have that $u^4 a = a$ and $u^6 b = b$.

If $j(E) \neq 0, 1728$, then $a, b \neq 0$ and therefore u must be at the same time a fourth and a sixth root of unity, hence $u = \pm 1$.

If $j(E) = 1728$, then $b = 0$ and u must be a fourth root of unity. Hence we have four possible automorphism. It is easy to see that the set of these four automorphisms with composition forms a group isomorphic to $\mathbb{Z}/4\mathbb{Z}$.

If $j(E) = 0$, then $a = 0$ and u must be a sixth root of unity. Hence we have six possible automorphism. It is easy to see that the set of these six automorphisms with composition forms a group isomorphic to $\mathbb{Z}/6\mathbb{Z}$. □

6.6 Velu's formulas

Let E_1, E_2 be two elliptic curves over an algebraically closed field $K = \overline{K}$ and $\phi\colon E_1 \to E_2$ an isogeny between them. Let $G := \ker \phi$ denote the kernel of ϕ. Then G is a subgroup of $E(\overline{K})$.

Lemma 6.6.1. *The following sequence is exact.*

$$0 \longrightarrow \ker \phi \longrightarrow E_1(\overline{K}) \xrightarrow{\phi} E_2(\overline{K}) \longrightarrow 0 \tag{6.1}$$

In other words, $E_2 \cong E_1/(\ker \phi)$.

Proof. The kernel of ϕ is a subgroup of $E_1(\overline{K})$. Any non-trivial isogeny is surjective □

The above arguments shows that if two elliptic curves are isomorphic, then one is isomorphic to a quotient of the other. In fact, also the opposite is true: if $E_2 = E_1/G$ for some subgroup G of $E_1(\overline{K})$, then it is possible to construct an isogeny $E_1 \to E_2$ whose kernel is exactly G. The argument is due to Velu, and in reporting it we will follow [14, Section 12.3].

Let K be any field and fix an algebraic closure $\overline{K}$. Let E be an elliptic curve over K, given by the Weierstrass form (5.2):

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 \tag{6.2}$$

with $a_1, a_2, a_3, a_4, a_6 \in K$. Set $f := x^3 + a_2x^2 + a_4x + a_6 - (y^2 + a_1xy + a_3y)$, so that $E\colon f = 0$. Let $G \subseteq E(\overline{K})$ be a finite subgroup of $E(\overline{K})$.

Let $Q = (x_Q, y_Q) \in G \subseteq E(\overline{K})$ be a point inside the subgroup G, and assume $Q \neq O = (0:1:0)$. Define the following quantities:

$$\begin{aligned}
f_x(Q) &:= \frac{\partial f}{\partial x}(Q) = 3x_Q^2 + 2a_2x_Q + a4 - a_1y_Q \ , \\
f_y(Q) &:= \frac{\partial f}{\partial y}(Q) = -2y_Q - a_1x_Q - a_3 \ , \\
v(Q) &:= \begin{cases} f_x(Q) & \text{if } \ 2Q = O \\ 2f_x(Q) - a_1f_y(Q) & \text{if } \ 2Q \neq O \end{cases} \ , \\
u(Q) &:= (f_y(Q))^2 \ .
\end{aligned}$$

Let $G_2 := (G \cap E(\overline{K})[2]) \setminus \{O\}$ the set of non-trivial points of order 2 inside G, and choose $R \subset G$ such that

$$G := \{O\} \cup G_2 \cup R \cup -R$$

is a disjoint union. In other words, for every pair $P, -P$ of non 2-torsion points of G, put exactly one of them in R. Set $S := R \cup G_2$ and define

$$v := \sum_{Q \in S} v(Q) \ , \qquad \text{and} \qquad w := \sum_{Q \in S} (f_x(Q)v(Q) + u(Q)) \ .$$

Definition 6.6.2. Define the curve E' over $\overline{K}$ as

$$E'\colon y^2 + A_1xy + A_3y = x^3 + A_2x^2 + A_4x + A_6$$

with

$$\begin{aligned}
A_1 := a_1 \ , \quad A_2 := a_2 \ , \quad A_3 := a_3 \ , \\
A_4 := a_4 - 5v \ , \quad A_6 := a_6 - (a_1^2 + 4a_2)v - 7w \ .
\end{aligned}$$

Lemma 6.6.3. *The curve E' is an elliptic curve.*

Proof. It is enough to prove that E' is smooth. See [14, Lemma 12.17]. □

Proposition 6.6.4. *The map $\sigma\colon E \to E'$ defined by $(x,y) \mapsto (X,Y)$ with*

$$X := x + \sum_{Q \in S} \left(\frac{v(Q)}{x - x_Q} + \frac{u(Q)}{(x - x_Q)^2} \right) ,$$
$$Y := y - \sum_{Q \in S} \left(u(Q) \frac{2y + a_1 x + a_3}{(x - x_Q)^3} + v(Q) \frac{a_1(x - x_Q) + y - y_Q}{(x - x_Q)^2} + \frac{a_1 u(Q) - f_x(Q) f_y(Q)}{(x - x_Q)^2} \right) ,$$

is an isogeny. Moreover, $\ker \sigma = G$.

Proof. This result is due to Vélu [13]. For a proof in a more modern language (and in english), see [14, Theorem 12.16]. □

Corollary 6.6.5. *Let E_1, E_2 be two elliptic curves over K. Then E_1 and E_2 are isogenous if and only if one is isomorphic (over $\overline{K}$) to a quotient of the other.*

Proof. It follows immediately from Lemma 6.6.1 and Proposition 6.6.4. Any isogeny is surjective, see Remark 6.2.2. □

6.7 Exercises

The exercises marked with * are harder; those marked with ! are important.

Exercise 6.7.1.

Show that every elliptic curve E of the form $y^2 = x^3 + a, a \neq 0$ has complex multiplication. Write down all the automorphisms of E.

Chapter 7

Elliptic curves over the complex, real, and rational fields

In this chapter, we will focus on elliptic curves over the main fields with characteristic 0, namely $\mathbb{C}, \mathbb{R}$, and $\mathbb{Q}$.

We will first study elliptic curves over $\mathbb{C}$ and compare them to complex tori. In chapter 1 we have seen that a complex tori is isomorphic to a cubic curve (in very short Weierstrass form). The main result of §7.1 consists in showing that complex tori and elliptic curves over $\mathbb{C}$ are the same thing.

It might happen that a complex elliptic curve can be actually defined by an equation with real coefficients, that is, it is an elliptic curve. As $\mathbb{R}$ is not algebraically closed, the study of the set $E(\mathbb{R})$ becomes more interesting and it will be the main topic of §7.2.

The statements above hold also if we substitute $\mathbb{R}$ with $\mathbb{Q}$. In particular, as $\mathbb{Q}$ is also not complete with respect the Euclidean metric, the group $E(\mathbb{Q})$ becomes even more interesting, also because of its connection to diophantine problems. The structure of $E(\mathbb{Q})$ will be the main object of §7.3.

7.1 Elliptic curves over the complex field

Let T be a complex tori. Then, by definition, T is the quotient $\mathbb{C}/\Lambda$ for some lattice $\Lambda \subset \mathbb{C}$. Theorem 1.5.15 tells us that T is isomorphic to the cubic curve

$$E(\Lambda)\colon y^2 = x^3 - 4g_2x - 16g_3$$

and Lemma 1.5.14 tells us that $E(\Lambda)$ is smooth. Note that $E(\Lambda)$ is already given in very short Weierstrass form, and hence its projective closure contains the point $O = (0 : 1 : 0)$. Hence $E(\Lambda)$ is an elliptic curve. So now on $E(\Lambda)$ we have two group structures:

- the one coming from the elliptic curve structure (§5.4),
- and the one inherited by T using the bijection ϕ in Theorem 1.5.15.

Miraculously, these two group structures coincide.

Theorem 7.1.1. *Let $\Lambda = \langle \omega_1, \omega_2 \rangle \subset \mathbb{C}$ be a lattice of $\mathbb{C}$ with generators ω_1, ω_2, and let $E(\Lambda)$ be the curve associated to Λ. Then the map*

$$\begin{aligned} \phi\colon \mathbb{C}/\Lambda &\to E(\Lambda) \\ z &\mapsto (\wp(z) : \wp'(z)/2 : 1) \\ 0 &\mapsto (0:1:0) = O \end{aligned}$$

is a group isomorphism.

Proof. [9, Proposition VI.3.6(b)]. □

The above theorem shows that every complex torus is isomorphic to an elliptic curve, as Riemann surfaces and also as groups (hence, as Lie groups). The next natural question then is whether every elliptic curve is isomorphic to a complex torus.

Let $E = (C, O)$ be an elliptic curve over $\mathbb{C}$. Since $\mathbb{C}$ has characteristic 0, the curve E can be put into a very short Weierstrass form (Proposition 5.1.4), hence write

$$E\colon y^2 = x^3 + ax + b$$

with $a, b \in \mathbb{C}$ such that $a^3 - 27b^2 \neq 0$.

Theorem 7.1.2 (Uniformization theorem)**.** *Let $a, b \in \mathbb{C}$ such that $a^3 - 27b^2 \neq 0$. Then, up to homotheties, there exists a unique lattice $\Lambda \subset \mathbb{C}$ such that $g_2(\Lambda) = a$ and $g_3(\Lambda) = b$.*

Proof. By Proposition 2.4.10 we know that, up to homotheties, there exists a unique lattice Λ such that $j(\Lambda) = \frac{a^3}{a^3 - 27b^2}$. Then, by definition of the j-function, it follows that

$$\frac{g_2(\Lambda)^3}{g_2(\Lambda)^3 - 27 g_3(\Lambda)^2} = \frac{a^3}{a^3 - 27b^2}$$

and hence there is a $u \in \mathbb{C}^*$ such that $g_2(\Lambda) = u^{-4}a$ and $g_3(\Lambda) = u^{-6}b$ (see the proof of Lemma 2.4.3 for the complete arguement). Then the lattice $\frac{1}{u}\Lambda$ is the one required in the statement. □

Corollary 7.1.3. *Let E be an elliptic curve over $\mathbb{C}$. Then there exists a complex torus T isomorphic (as group and as Riemann surface) to E.*

Proof. As E is defined over $\mathbb{C}$, it can be put in a very short Weierstrass form $E\colon y^2 = x^3 + ax + b$ with $a, b \in \mathbb{C}$ such that $4a^3 + 27b^2 \neq 0$. Define $\alpha := -a/4$, $\beta := -b/16$ and we obtain that

$$-4^4(\alpha^3 - 27\beta^2) = 4a^3 + 27b^2 \neq 0\ ,$$

hence $\alpha^3 - 27\beta^2 \neq 0$. Then, from Theorem 7.1.2, it follows that there exists a lattice Λ (uniquely determined up to homotheties), such that $g_2(\Lambda) = \alpha$ and $g_3(\Lambda) = \beta$. Let T be the torus $\mathbb{C}/\Lambda$. Then Theorem 1.5.8(b) and Theorem 7.1.1 tell us that $\mathbb{C}/\Lambda$ is isomorphic to $E(\Lambda)\colon y^2 = 4x^3 - \alpha x - \beta$ as Riemann surface and as group. By definition of α, β, we know that $E(\Lambda)$ is isomorphic to E, simply using the change of variable used in (1.5.11). □

The content of this section, together with that of §1.5 and §2.1, tells us that complex lattices, complex tori and complex elliptic curves are essentially the same thing. This statement is made clearer by the following result.

Theorem 7.1.4. *The following categories are equivalent:*

(i) (Elliptic curves over $\mathbb{C}$; Isogenies of elliptic curves);

(ii) (Complex tori; Isogenies of complex tori);

(iii) (Lattices up to homotheties; $\{\alpha \in \mathbb{C} \,:\, \alpha\Lambda_1 \subseteq \Lambda_2\}$).

Remark 7.1.5. The results in this section also shows that we can apply all the theory developed for complex tori in chapters 1 and 2 to elliptic curves over $\mathbb{C}$.

The results above tell us that every complex elliptic curve comes from a complex torus $\mathbb{C}/\Lambda$, but the proofs are not constructive. Then one might naturally ask, given a complex elliptic curve $E/\mathbb{C}$, is it possible to explicitly describe the lattice Λ such that $E \cong \mathbb{C}/\Lambda$? The answer is positive, as shown below.

Let $E/\mathbb{C}$ be a complex elliptic curve inside the affine plane $\mathbb{A}^2(x, y)$. As E is isomorphic to a complex torus, its fundamental group is $\pi_1(E) \cong \pi_1(T) \cong \mathbb{Z} \times \mathbb{Z}$. Let $\alpha, \beta \in \pi_1(E)$ denote two generators.

Definition 7.1.6 (Periods of an elliptic curve)**.** We define *the periods* of E to be the quantities

$$\omega_1 := \int_\alpha \frac{dx}{y} \quad \text{and} \quad \omega_2 := \int_\beta \frac{dx}{y}\,.$$

Theorem 7.1.7. *Let $E/\mathbb{C}$ be a complex elliptic curve and let ω_1, ω_2 be its periods. Then $\omega_1, \omega_2 \in \mathbb{C}$ are linearly independent over $\mathbb{R}$.*

Let $\Lambda := \langle \omega_1, \omega_2 \rangle \subset \mathbb{C}$ be the lattice they generate. Then $\mathbb{C}/\Lambda$ is isomorphic to E, and the isomorphism is the one given in Theorem 1.5.15(b).

Proof. [9, Proposition VI.5.2]. □

7.2 Elliptic curves over the real field

In this section, we will always assume E to be an elliptic curve defined over $\mathbb{R}$, that is, $E\colon y^2 = x^3 + ax + b$ with $a, b \in \mathbb{R}$ such that $4a^3 + 27b^2 \neq 0$. As we are working over $\mathbb{R}$, it also possible to draw a picture of the set of rational points $E(\mathbb{R})$. As the picture suggests, the number of connected components of $E(\mathbb{R})$ depends on the discriminant of the curve.

Lemma 7.2.1. *Let E be an elliptic curve over $\mathbb{R}$ with discriminant Δ. Let c be denote the number of connected components of $E(\mathbb{R})$. Then*

$$c = \begin{cases} 1 & \text{if } \Delta < 0 \\ 2 & \text{if } \Delta > 0 \end{cases}\,.$$

Moreover, the number of 2-torsion points of $E(\mathbb{R})$ is

$$\#E(\mathbb{R})[2] = \begin{cases} 2 & \text{if } \Delta < 0 \\ 4 & \text{if } \Delta > 0 \end{cases}\,.$$

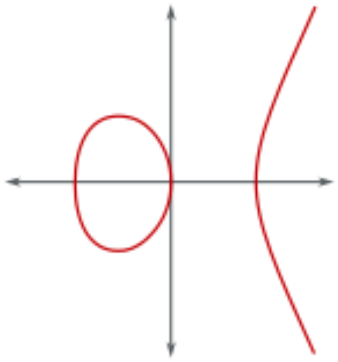


Figure 7.1: An elliptic curve with $\Delta > 0$.

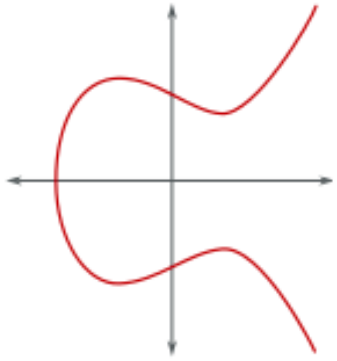


Figure 7.2: An elliptic curve with $\Delta < 0$.

Proof. Recall that as E is an elliptic curve, it is smooth, and hence its determinant is non-zero, $\Delta \neq 0$. Without loss of generality, we may and do assume that E is given in a a very short Weierstrass form. Therefore, it is symmetric with respect the x-axis. Then the first statement follows from Proposition 3.2.8.

To prove the second statement, recall that the non-trivial 2-torsion points are those whose y-coordinate equal to 0. Then, again, the statement follows from Proposition 3.2.8. □

As $\mathbb{R} \subset \mathbb{C}$, we can nevertheless view E as a *complex* elliptic curve and, therefore, as a complex torus. Let ψ be the automorphism as in Theorem 1.5.15. Normalize Λ_E to the lattice $\Lambda = \mathbb{Z} + \tau\mathbb{Z}$ with $\tau \in \mathbb{H}$, see Lemma 2.4.4. Let F denote the fundamental domain of Λ spanned by $\{1, \tau\}$.

Definition 7.2.2. Let γ_1 denote the edge of F going from 0 to 1 and γ_2 the segment going from $\tau/2$ to $\tau/2 + 1$.

Remark 7.2.3. Notice that γ_1 and γ_2 are two homotopic loops in $\mathbb{C}/\Lambda$.

The connected components of E are related to the loops γ_1, γ_2.

Lemma 7.2.4. *Let $E, \psi, F, \tau, \gamma_1, \gamma_2$ be defined as above. Then*

$$\psi(E(\mathbb{R})) = \begin{cases} \gamma_1 & \text{if } \Delta < 0\,, \\ \gamma_1 \cup \gamma_2 & \text{if } \Delta > 0\,. \end{cases}$$

Moreover, if $\Delta > 0$, one has $\tau \in i\mathbb{R}_{>0}$.

Proof. Notice that $E(\mathbb{R})$ is the set of points fixed by the Galois action of $G = \mathrm{Gal}(\mathbb{C}/\mathbb{R})$ on E viewed as a complex elliptic curve. As the $\wp$ function is defined over $\mathbb{R}$, the pre-image $\phi^{-1}(E(\mathbb{R})) = \psi(E(\mathbb{R}))$ is also G-invariant. Moreover, as it is a continuous function, it preserves the number of connected components. If $z \in F$ is in $\psi(E(\mathbb{R}))$, then its conjugate satisfies $\bar{z} \equiv z \mod \Lambda = \langle 1, \tau \rangle$. This trivially implies that $\gamma_1 \subset \Lambda$ is G-invariant, so $\gamma_1 \subseteq \psi(E(\mathbb{R}))$. If we write $z = x + y\tau \in F$ with $x, y \in [0, 1[$ then $\bar{z} = x + y\bar{\tau}$ and hence $z \equiv \bar{z} \mod \Lambda$ if and only if $y(\tau - \bar{\tau}) \in \Lambda$. Write $\tau = a + bi$ with $a, b \in \mathbb{R}, b > 0$, then it yields that $2ybi \in \Lambda = \mathbb{Z} + \tau\mathbb{Z}$ and hence either $y = 0$ or $y = 1/2$ and $\tau = bi$. If $y = 0$ we recover γ_1; if $y = 1/2$ we recover γ_2.

If $\Delta < 0$, then $\#E(\mathbb{R})[2] = 2$ and $E(\mathbb{R})$ has only one connected component, hence $\psi(E(\mathbb{R})) = \gamma_1$, also meaning that τ is not a multiple of i. If $\Delta > 0$, then $\#E(\mathbb{R})[2] = 4$ and $E(\mathbb{R})$ has two connected components. Then the computations above show that they are exactly γ_1 and γ_2, and also that $\tau = bi$, concluding the proof. □

Remark 7.2.5. Recall Definition 7.1.6 of the periods ω_1, ω_2 of E. The loop $\gamma_1 \subset \mathbb{C}/\Lambda$ defined in Definition 7.2.2 can be taken to be an element of the basis, say α. As $\gamma_2 \sim \gamma_1$, from Lemma 7.2.4 it follows that

$$\int_{E(\mathbb{R})} \frac{dx}{y} = \begin{cases} \omega_1 & \text{if } \Delta < 0\,, \\ 2\omega_1 & \text{if } \Delta > 0\,. \end{cases}$$

7.3 Elliptic curves over the rationals

In this section, let E be an elliptic curve defined over $\mathbb{Q}$, that is, $E\colon y^2 = x^3 + ax + b$ with $a, b \in \mathbb{Q}$ such that $4a^3 + 27b^2 \neq 0$. We are interested in understanding the group structure of $E(\mathbb{Q})$. The first thing to notice is that and elliptic curve over $\mathbb{Q}$ always admits a very short Weierstrass form with coefficients in $\mathbb{Z}$.

Lemma 7.3.1. *Let $E/\mathbb{Q}$ be an elliptic curve defined by $E\colon y^2 = x^3 + ax + b$ with $a, b \in \mathbb{Q}$ such that $4a^3 + 27b^2 \neq 0$. Then there exist $a', b' \in \mathbb{Z}$ such that $E'\colon y^2 = x^3 + a'x + b'$ is isomorphic to E.*

Proof. We can write a, b as rational numbers with the same denominator, say

$$a = \frac{p}{q} \quad \text{and} \quad b = \frac{r}{q}\,,$$

with $p, r, q \in \mathbb{Z}$. Then $E\colon y^2 = x^3 + \frac{p}{q}x + \frac{r}{q}$. Multiply both sides of the equation defining E by q^6, obtaining

$$q^6y^2 = q^6x^3 + q^5px + q^6r\,.$$

Then the substitution

$$\begin{cases} x' = q^2x \\ y' = q^3y \end{cases}$$

shows that E is isomorphic to $E'\colon y^2 = x^3 + q^2px + q^6r$. Also notice that $\Delta(E') = u^6\Delta(E) \neq 0$, hence E' is an elliptic curve. □

In studying $E(\mathbb{Q})$, we start with the torsion points.

Definition 7.3.2. We denote by $E(\mathbb{Q})_{\text{tors}}$ the subgroup $E(\mathbb{Q})$ formed by torsion elements:

$$E(\mathbb{Q})_{\text{tors}} := \{P \in E(\mathbb{Q}) \mid \exists m \in \mathbb{Z} : mP = \mathcal{O}\}.$$

An element of $E(\mathbb{Q})_{\text{tors}}$ is called a *(rational) torsion* point of E.

The torsion part is very well understood, as the following result by Mazur shows.

Theorem 7.3.3 (Mazur)**.** *Let $E/\mathbb{Q}$ be an elliptic curve. Then the torsion subgroup $E_{tors}(\mathbb{Q})$ is one of the following fifteen groups:*

$$\begin{aligned} \mathbb{Z}/N\mathbb{Z} \quad & 1 \leq N \leq 10 \ \text{ or } \ N = 12; \\ \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2N\mathbb{Z} \quad & 1 \leq N \leq 4. \end{aligned}$$

Further, each of these groups does occur as an $E(\mathbb{Q})_{tors}$.

Its study is also aided by the following theorem.

Theorem 7.3.4 (Lutz–Nagell)**.** *Let E be an elliptic curve over $\mathbb{Q}$ having Weierstrass equation*

$$E\colon y^2 = x^3 + ax + b$$

with $a, b \in \mathbb{Z}$ and such that no 12-th power of a prime divides $\Delta(E)$. Let $P = (x_P, y_P)$ be a torsion point of E of order $m > 1$. Then

1. *$x_P, y_P \in \mathbb{Z}$,*
2. *if $m = 2$ then $y_P = 0$,*
3. *if $m > 2$ then y_P^2 divides $4a^3 + 27b^2 = \Delta(E)$.*

Remark 7.3.5. The condition on $\Delta(E)$ not to be divisble by any 12-th power will be explained in §9.1.

These results, together with the reduction modulo a prime presented in Proposition 9.3.5, allow practical computations of the torsion part of $E(\mathbb{Q})$. In particular, the reduction modulo a prime is very useful and it is also needed to prove Theorem 7.3.4. Ror this reason, the proof of the theorem is postponed to §9.3.

Studying the points of infinite order is definitely more complicated, and here we will only state the Mordell–Weil theorem. The proof of this theorem is not very complicated, but pretty long and requiring some background.

Theorem 7.3.6 (Mordell–Weil)**.** *Let $E/\mathbb{Q}$ be an elliptic curve. Then the group $E(\mathbb{Q})$ is finitely generated.*

Proof. See [9, VIII.4]. □

We will not focus on the proof of this theorem, but rather on an immediate consequence. From Theorem 7.3 it immediately follows that

$$E(\mathbb{Q}) \cong \mathbb{Z}^r \oplus E(\mathbb{Q})_{\text{tors}},$$

for some integer $r \geq 0$.

Definition 7.3.7. We define r to be the *rank* of $E/\mathbb{Q}$.

At the moment of writing, there is no known algorithm to compute the rank of a given elliptic curve. If E admits a 2-torsion point on $\mathbb{Q}$, then the rank can be computed using a procedure called 2-*descent*. An important conjecture, due to Birch and Swinnerton–Dyer, states that the rank of $E(\mathbb{Q})$ equals the order of the L-function associated with E at 1; for the definition of the L-function of E and the Birch–Swinnerton-Dyer conjecture, see chapter 10.

7.4 Exercises

The exercises marked with * are harder; those marked with ! are important.

Exercise 7.4.1. Prove 5.4.5.ii), iv), and v). [Extra: do not use Proposition 5.4.7.]

Exercise 7.4.2. Let C be an elliptic curve given in Weierstrass form and let P be a point of C. Prove the formula for the coordinates of $2P = P + P$ (cf. Corollary 5.4.9). Give a characterization of the 2-torsion points.

Exercise 7.4.3. Consider the cubic curve C over $\mathbb{Q}$ given by

$$y^2 = x^3 + 17.$$

The points $P_1 = (-2, 3)$ and $P_2 = (-1, 4)$ are on the curve. Compute $P_1 + P_2$. Find all the $\mathbb{Q}$-torsion points of C.

Exercise 7.4.4. Find all the $\mathbb{Q}$-torsion points of the elliptic curve $C\colon y^2 = x^3 - x$.

Exercise 7.4.5. * Find more $\mathbb{Q}$-rational solutions of the following equation:

$$\frac{x}{y+z} + \frac{y}{x+z} + \frac{z}{x+y} = 4$$

(cf. Exercise 5.6.3).

Chapter 8

Elliptic curves over finite fields

In this section we focus on elliptic curves over finite fields. We will briefly recall the basic theory of finite fields. The main goal of the section is to state and prove the Weil conjectures for elliptic curves.

8.1 Finite fields

For an account on this subject you might read [6, Section V.5] or [3, Chapter 12].

A *finite field* is simply a field with finitely many elements.

Example 8.1.1. Let p be a prime number, and define $\mathbb{F}_p$ as the ring obtained by taking $\mathbb{Z}/p\mathbb{Z}$ with the usual sum and multiplication. One can easily verify that $\mathbb{F}_p$ is a field.

Example 8.1.2. Let p be a prime number and let $\mathbb{F}_p$ be the finite field with p elements. Set $q = p^n$ be a power of p and consider an irreducible polynomial $f \in \mathbb{F}_p[X]$ of degree n. Then the field with $q = p^n$ elements, denoted by $\mathbb{F}_q$, can be defined as the quotient $\mathbb{F}_p[X]/(f)$ or, equivalently, as the field $\mathbb{F}_p(\alpha)$ with α a root of f.

Let K be a field (not necessarily finite). We define the characteristic of K, denoted by $\operatorname{Char} K$, to be the smallest non-negative integer n such that $n \cdot 1 = 0$ in K.

Example 8.1.3. The fields $\mathbb{Q}$, $\mathbb{R}$, and $\mathbb{C}$ all contain the ring $\mathbb{Z}$ and therefore they all have characteristic 0.

Example 8.1.4. The fields $\mathbb{F}_p$ and $\mathbb{F}_q$ (cf. 8.1.1 and 8.1.2), have characteristic p.

The following result completely classifies the finite fields.

Theorem 8.1.5 (Moore, 1893)**.** *Let K be a finite field. Then K is of the form $\mathbb{F}_q$ for some prime p and some integer n such that $q = p^n$.*

For every prime power q there is a unique finite field of order q up to isomoprhisms.

In $\mathbb{F}_q$ every element satisfies the equation

$$X^q = X. \tag{8.1}$$

Proof. For a proof, see [3, Theorem 12.1] or [6, Theorem V.5.2]. □

Corollary 8.1.6. *The field $\mathbb{F}_q$ contains the field $\mathbb{F}_{q'}$ if and only if $q = p^n$, $q' = p^m$, and $m \leq n$.*

Let K be a finite field of characteristic p. We define the *Frobenius automorphism* of K as the automorphism given by

$$\Phi \colon x \mapsto x^p.$$

Theorem 8.1.7. *Let K be a finite field of characteristic p Let $\overline{K}$ be an algebraic closure of K. Then the Frobenius map Φ of K defines an automorphism of $\overline{K}$. Furthermore, Φ topologically generates the Galois group $\mathrm{Gal}(\overline{K}/K)$. For every integer n, the set of elements of $\overline{K}$ fixed by Φ^n is a subfield isomorphic to $\mathbb{F}_{p^n}$.*

Proof. See [3, Section 12.5]. □

Remark 8.1.8. Let K be a finite field of characteristic p, and let $\overline{K}$ be an algebraic closure of K. Then $\overline{K}$ is an *infinite* field of characteristic p.

8.2 Isogenies over finite fields

Let $q = p^r$ be a prime power and consider the finite field $\mathbb{F}_q$. Then the Frobenius map $\mathrm{Frob}_q \colon x \mapsto x^q$ acts as the identity on $\mathbb{F}_q$. Let $K = \overline{\mathbb{F}_q}$ be a fixed algebraic closure of $\mathbb{F}_q$ and let E be an elliptic curve defined over K.

Definition 8.2.1. The *Frobenius endomorphism* of E is the isogeny defined by

$$\begin{aligned} \mathrm{Frob}_q \colon E(K) &\to E(K) \\ (x, y) &\mapsto (x^q, y^q)\ . \end{aligned}$$

Clearly, the map acts as the identity on the points in $E(\mathbb{F}_q)$, but not on the others. In fact, it is easy to see that these are exactly the points fixed by the Frobenius endomorphism, i.e., $E(\mathbb{F}_q) = E(K)^{\mathrm{Frob}_q}$. This property is useful in order to count the number of points in $E(\mathbb{F}_q)$.

Remark 8.2.2. The degree of Frob_p is p. To see this, one can use the definition of degree of a map as the degree of the field extension it induces at the level of function fields.

The next natural question one might ask is how to determine whether two elliptic curves are isogenous.

Theorem 8.2.3. *Let E_1, E_2 be two elliptic curves over a finite field K. Then E_1 and E_2 are isogenous over K if and only if they have the same number of K-rational points.*

Proof. The first implication is a direct consequence of [12, Theorem 1]. The reverse implication is [9, Exercise V.5.4(b)]. □

8.3 The Hasse bound

Let K be a finite field with $q = p^n$ elements, and let E be a cubic curve over K. As K is finite, we know that the set $E(K)$ of rational points is also finite. Then the next question is: can we estimate the size of $E(K)$, that is, the number of K-rational points of E. If E has a singular point, then the answer only depends on the type of singularity, as shown by the following result.

Proposition 8.3.1. *Let E/K be a cubic with a singularity in the point $P \in E(K)$. Let $E_{ns}(K) \subset E(K)$ be the set of nonsingular points of E.*

1. *If P is a node and the slopes of the tangent lines to E at P are not defined over K, then $\#E_{ns}(K) = q - 1$.*
2. *If P is a node and the slopes of the tangent lines to E at P are defined over K, then $\#E_{ns}(K) = q + 1$.*
3. *If P is a cusp, then $\#E_{ns}(K) = q$.*

Proof. Let Λ denote the set of lines defined over K passing through P. Then $\Lambda \cong \mathbb{P}^1_K$ and hence $\#\Lambda = q + 1$. As P is a singular point, it has multiplicity 2; as E is a cubic, any other point $Q \in E_{\text{ns}}(K)$ corresponds to a line in Λ not tangent to E at P. Hence $\#E_{\text{ns}}(K) = \#\Lambda_0$, where $\Lambda_0 \subseteq \Lambda$ is the set of lines defined over K passing through P and not tangent to E.

If P is a node and the slopes of the tangent lines to E at P are not defined over K, then $\Lambda_0 = \Lambda$ and hence $\#E_{\text{ns}}(K) = q + 1$. If P is a node and the slopes of the tangent lines are defined over K, then $\#\Lambda_0 = q + 1 - 2 = q - 1$. If P is a cusp, then P admits only one tangent line and it is defined over K, hence $\#\Lambda_0 = q + 1 - 1 = q$, concluding the proof. □

The answer for elliptic curves is not as easy and it depends on the elliptic curve itself. Here we give a bound on the possible values.

Lemma 8.3.2. *Let A be an abelian group and $d\colon A \to \mathbb{Z}$ a positive definite quadratic form. Then for all $a, b \in A$,*

$$|d(a - b) - d(a) - d(b)| \leq 2\sqrt{d(a)d(b)}.$$

Proof. For $a, b \in A$, let

$$L(a, b) := d(a - b) - d(a) - d(b).$$

As d is quadratic, L is bilinear. As d is positive definite, then for $m, n \in \mathbb{Z}$

$$0 \leq d(ma - nb) = m^2 d(a) + mnL(a, b) + n^2 d(b).$$

Then for $m = -L(a, b)$ and $n = 2d(a)$ we have

$$0 \leq d(a)[4d(a)d(b) - L(a, b)^2]$$

If $a \neq 0$, as d is positive definite, $d(a) > 0$ and so $0 \leq 4d(a)d(b) - L(a, b)^2$, leading to the statement.

If $a = 0$, then $d(a) = 0$ and the statement is trivially true. □

Theorem 8.3.3 (Hasse bound)**.** *Let E be defined as above. Then*

$$|\#E(\mathbb{F}_q) - q - 1| \leq 2\sqrt{q}$$

Proof. Choose a Weierstrass equation for E with coefficients in $\mathbb{F}_q$ and consider the Frobenius map

$$\mathrm{Frob}_q \colon (x, y) \mapsto (x^q, y^q).$$

Notice that the map above is the n-th power of the Frobenius morphism. Recall that K is an algebraic closure of $\mathbb{F}_q$ and let $P \in E(K)$. Then, using Theorem 8.1.7, $P \in E(\mathbb{F}_q)$ if and only if $\mathrm{Frob}_q(P) = P$. Therefore $E(\mathbb{F}_q) = \ker(1 - \mathrm{Frob}_q)$ and so $\#E(\mathbb{F}_q) = \#\ker(1 - \mathrm{Frob}_q) = \deg(1 - \mathrm{Frob}_q)$.

The degree is a quadratic form on $\mathrm{End}(E)$ (see Corollary 6.3.8) and the degree of ϕ is q (see Remark 8.2.2), then the result follows from Lemma 8.3.2. □

8.4 The Weil conjectures for elliptic curves

In this subsection we introduce the Weil conjectures for elliptic curves. The whole topic could be trated in greater generality, concerning varieties of any dimension on finite fields, but that would go beyond the scope of these notes.

Let $q = p^r$ be a prime power and $\mathbb{F}_q$ the finite field with q elements. Let $E/\mathbb{F}_q$ be an elliptic curve and recall that for any $n > 0$ one can consider the points of E defined over the extension $\mathbb{F}_{q^n}$, that is, $E(\mathbb{F}_{q^n})$.

Example 8.4.1. Consider $E/\mathbb{F}_5 \colon y^2 = x^3 + x + 1$. Then $\#E(\mathbb{F}_5) = 9$ and $\#E(\mathbb{F}_{25}) = 27$.

Definition 8.4.2. If $F(T) \in \mathbb{Q}[[T]]$ is a power series with no constant term, we define

$$\exp(F(T)) := \sum_{k=0}^{\infty} \frac{F(T)^k}{k!}.$$

Then we define the *zeta function* of $E/\mathbb{F}_q$ as the power series

$$Z(E, T) := \exp\left(\sum_{n=1}^{\infty} \#E(\mathbb{F}_{q^n}) \frac{T^n}{n} \right).$$

In 1949, Weil conjectured some important properties of this function: these are known as *Weil conjectures*. Weil himself proved them for the case of curves and abelian varieties, hence for elliptic curves in particular.

Theorem 8.4.3 (Weil conjectures for elliptic curves)**.** *Let $E/\mathbb{F}_q$ be an elliptic curve. Then the following statements hold.*

1. *Rationality:*
$$Z(E, T) \in \mathbb{Q}(T) .$$
2. *Factorization:*
$$Z(E, T) = \frac{P_1(T)}{P_0(T)P_2(T)}$$
with
$$P_0(T) = 1 - T \text{ and } P_2(T) = 1 - qT$$
and $P_1(T) \in \mathbb{Z}[T]$.

3. *Riemann hypothesis: The polynomial* $P_1(T) \in \mathbb{Z}[T]$ *factors over* $\mathbb{C}$ *as*

$$P_1(T) = \prod_{j=1}(1 - \alpha_j T)$$

with $|a_j| = \sqrt{q}$.

4. *Functional equation:*

$$Z\left(E, \frac{1}{qT}\right) = \pm Z(E, T) \ .$$

In fact, for elliptic curves we know even more.

Definition 8.4.4. We define the *trace* of the Frobenius of E to be the integer

$$a_q := q + 1 - \#E(\mathbb{F}_q) \ .$$

The name 'trace' is justified by the following result.

Theorem 8.4.5. *The following statements hold.*

1. *The Frobenius enodmorphism satisfies the following relation in* $\mathrm{End}(E)$*:*

$$\mathrm{Frob}_q^2 - a\,\mathrm{Frob}_q + q = 0 \ .$$

2. *The factor* P_2 *of* $Z(E, T)$ *is*

$$P_2(T) = 1 - a_q T + qT^2 =: (1 - \alpha_1 T)(1 - \alpha_2 T) \ .$$

3. *For every* $n \geq 1$ *we have*

$$\#E(\mathbb{F}_{q^n}) = q^n + 1 - \alpha_1^n - \alpha_2^n \ .$$

Proof. See [8, §V.2]. □

Remark 8.4.6. From Theorem 8.4.3 we know that α_1, α_2 are complex conjugate and have norm $\sqrt{q}$.

Remark 8.4.7. Notice that the trace of Frob_q on E is exactly the quantity interested by the Hasse bound, see Theorem 8.3.3.

8.5 Exercises

The exercises marked with * are harder; those marked with ! are important.

Exercise 8.5.1. ! Let n be a non-prime integer. Prove that the ring $\mathbb{Z}/n\mathbb{Z}$ is not a field.

Exercise 8.5.2. Let E be the elliptic curve defined by $y^2 = x^3 + x - 1$ over $\mathbb{F}_5$. Compute the number of points of E over $\mathbb{F}_5$ and check that the Hasse bound holds. Do the same over $\mathbb{F}_{25}$.

Chapter 9

L-function of an elliptic curve

In this section, we focus on elliptic curves defined over the rationals. We will study their reduction modulo a prime and define their L-function.

9.1 Minimal Weierstrass model

Fix a prime p. Then one can consider the valuation induced by p:

$$\begin{aligned} v := v_p \colon \mathbb{Z} &\to \mathbb{N} \cup \{\infty\} \\ 0 &\mapsto \infty \\ n &\mapsto e \end{aligned}$$

where e is the greatest power of p dividing n, i.e., $n = p^e \cdot n'$ with $\gcd(p, n') = 1$. Clearly, the valuation is multiplicative, i.e., $v_p(n \cdot m) = v_p(n) + v_p(m)$, and so, by setting $v_p(1/p) = -1$, it extends to a valuation

$$v := v_p \colon \mathbb{Q} \to \mathbb{Z} \cup \{\infty\}.$$

Example 9.1.1. Set $p = 5$. Then $v_5(5) = 1, v_5(7) = 0, v_5(7/25) = -2$.

Let $E/\mathbb{Q}$ be an elliptic curve over $\mathbb{Q}$. In chapter 5 we have seen that then E can be written as the zero set of the polynomial

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

for some $a, b \in \mathbb{Q}$ and that the only changes of variables preserving this form and the field of definition are $t_u \colon (x, y) \mapsto (u^{-2}x, u^{-3}y)$, for some $u \in \mathbb{Q}^*$.

Lemma 9.1.2. *Let $E/\mathbb{Q}$ be defined by $y^2 = x^3 + ax + b$ and let $E' \colon y^2 = x^3 + a'x + b'$ be the image of E under the substitution t_u. Then $a' = u^4 a, b' = u^6 b, \Delta' = u^{12}\Delta$.*

Proof. By direct computations. □

So we see that if we vary among the short Weierstrass equations of an elliptic curve, the discriminant of the curve get scaled by the twelfth power of the parameter. This motivates the following definition.

Definition 9.1.3. A short Weierstrass equation for $E/\mathbb{Q}$ is called *minimal* at v_p if $v_p(a), v_p(b) \geq 0$ and $v_p(\Delta) \geq 0$ is minimal.

Corollary 9.1.4. *Let $E/\mathbb{Q}$ be the elliptic curve given by $y^2 = x^3 + ax + b$ with $v_p(a), v_p(b) \geq 0$. Then the following are equivalent:*

1. *The equation $y^2 = x^3 + ax + b$ is the minimal short Weierstrass equation of E at v_p;*
2. *$v_p(\Delta) < 12$;*
3. *$v_p(a) < 4$;*
4. *$v_p(b) < 6$.*

Proof. It follows immediately from Lemma 9.1.2 and the hypothesis that $v_p(a), v_p(b) \geq 0$. In particular, the latter implies that $v_p(\Delta) \geq 0$. □

Proposition 9.1.5. *Let p be a fixed prime. Then every elliptic curve $E/\mathbb{Q}$ admits a minimal short Weierstrass equation. Moreover, the minimal equation is unique up to change of coordinates t_u with $u \in \mathbb{Z}$ such that $v_p(u) = 0$.*

Proof. Let $y^2 = x^3 + ax + b$ with $a, b \in \mathbb{Q}$ not both zero. If any of the two has negative valuation, we can substitute the variables by t_p until both a, b have positive valuation, cf. Lemma 9.1.2. By stopping as soon as they have positive valuation, we obtain the minimal equation, cf. Corollary 9.1.4.

The second statement follows immediately from Lemma 9.1.2. □

9.2 Reduction mod p

As before, fix a prime $p \geq 5$ and let $E/\mathbb{Q}$ be an elliptic curve. Fix a minimal short Weierstrass equation for E, say

$$E\colon y^2 = x^3 + ax + b.$$

As the equation is minimal, $v_p(a), v_p(b) \geq 0$. In particular, using Proposition 9.1.5, we may assume that $a, b \in \mathbb{Z}$. Then we can consider the reduction modulo p:

$$\begin{aligned} \mathbb{Z} &\to \mathbb{Z}/(p) \cong \mathbb{F}_p \\ n &\mapsto \overline{n} := n \bmod p \end{aligned}$$

Definition 9.2.1. We define the *reduction* of E mod p to be the curve $E_p/\mathbb{F}_p$ defined by

$$E_p\colon y^2 = x^3 + \overline{a}x + \overline{b}.$$

The reduction modulo p also induces a map on the sets of rational points:

$$\begin{aligned} E(\mathbb{Q}) &\to E_p(\mathbb{F}_p) \\ (x : y : z) &\mapsto (\overline{x} : \overline{y} : \overline{z}) \,. \end{aligned}$$

Notice that the map is well defined as the point $(x : y : z)$ can be taken with integer coordinates and with at least one of them not divisible by p.

The main problem with the reduction modulo a prime is that the reduction of an elliptic curve does not need to be an elliptic curve: indeed it can be singular. This motivates the following definition.

Definition 9.2.2. Let $E/\mathbb{Q}$ be an elliptic curve with a given minimal Weierstrass equation at v_p. We say that the reduction E_p is

(a) *good* if it is smooth (and hence E_p is an elliptic curve over $\mathbb{F}_p$),

(b) *multiplicative* if E_p has a node,

(c) *additive* if E_p has a cusp.

If E has multiplicative reduction, then the reduction is said to be *split* if the slopes of the tangent lines at the node are in $\mathbb{F}_p$, otherwise it is called *nonsplit*.

If E has not good reduction, we say that p is a prime *bad reduction* for E with that given equation; we often shorten it by saying that p is a *bad prime* for E.

Example 9.2.3. Consider $p = 5$ and the elliptic curve $E\colon y^2 = x^3 + 5$. Then the reduction $E_5\colon y^2 = x^3$ has a cusp, hence it is not an elliptic curve.

Example 9.2.4. Consider $p = 31$ and the elliptic curve $E\colon y^2 = x^3 + x + 1$. The reduction E_{31} has a node at $(14, 0)$. As 14 is a square $\mod 31$, the prime p is a split prime.

Proposition 9.2.5. *Let $p \geq 5$ be a prime and $E/\mathbb{Q}$ be an elliptic curve with minimal short Weierstrass equation $y^2 = x^3 + ax + b$ with $a, b \in \mathbb{Z}$. Then*

1. *E has good reduction if and only if $v_p(\Delta) = 0$;*
2. *E has multiplicative reduction if and only if $v_p(\Delta) > 0$ and $v_p(a) = 0$;*
3. *E has additive reduction if and only if $v_p(a) > 0$.*

Proof. Notice that the reduction $E_p/\mathbb{F}_p$ is a cubic curve with discriminant equal to $\overline{\Delta} = \Delta \bmod p$. As a cubic curve is singular if and only if it has discriminant equal to 0, the first statement immediately follows.

Now assume $v_p(\Delta) > 0$. As a, b are supposed to be integers, we know that $v_p(a), v_p(b) \geq 0$. If $v_p(a) > 0$ it means that E reduces to the curve $y^2 = x^3 + \bar{b}$ with discriminant $\bar{\Delta} = -16 * 27 * \bar{b}^2 \cong 0 \mod p$. As $p \geq 5$ it follows that $\bar{b} \cong 0 \mod p$ and hence $\bar{E}\colon y^2 = x^3$, the cuspidal cubic. On the other hand, it is immediate to see that if $\bar{E}$ is the cuspidal cubic then $v_p(a) > 0$. As a singular cubic can only have a cusp or a node, this concludes the proof. □

Remark 9.2.6. Proposition 9.2.5 holds also for $p = 2, 3$ if we write $E\colon y^2 = x^3 + 27ax + 54b$. This is not so interesting at this stage, as the reduction of a short Weierstrass form modulo $p = 2, 3$ is always singular.

9.3 Reduction and torsion points: elliptic curves over the p-adics.

Surprisingly, the reduction modulo p gives us information about the torsion points of $E/\mathbb{Q}$. In fact, if p is of good reduction for E and m is an integer coprime with p, we will see there is an embedding of abelian groups

$$E(\mathbb{Q})[m] \hookrightarrow E_p(\mathbb{F}_p).$$

Let $E/\mathbb{Q}$ be an elliptic curve with a model over $\mathbb{Z}$ and let p be a prime. Denote by $\bar{E}$ the reduction of E modulo p. We denote by $\mathbb{Q}_p$ the completion of $\mathbb{Q}$ with respect the p-adic norm, as $\mathbb{Q} \hookrightarrow \mathbb{Q}_p$, one can naturally consider the set of points $E(\mathbb{Q}_p) \supset E(\mathbb{Q})$.

Definition 9.3.1. We define the following subgroups of $\bar{E}(\mathbb{F}_p)$ and $E(\mathbb{Q})$:

$$\begin{aligned} \bar{E}_{\text{ns}}(\mathbb{F}_p) &:= \{\text{non-singular points of } \bar{E}(\mathbb{F}_p)\}, \\ E_0(\mathbb{Q}_p) &:= \{P \in E(\mathbb{Q}_p) \ : \ \bar{P} \in \bar{E}_{\text{ns}}(\mathbb{F}_p)\}, \\ E_1(\mathbb{Q}_p) &:= \{P \in E(\mathbb{Q}_p) \ : \ \bar{P} = \bar{O}\}. \end{aligned}$$

Remark 9.3.2. Clearly, if p is a prime of good reduction for E then $E_0(\mathbb{Q}_p) = E(\mathbb{Q}_p)$.

Proposition 9.3.3. *There is an exact sequence of abelian groups*

$$0 \to E_1(\mathbb{Q}_p) \to E_0(\mathbb{Q}_p) \to \bar{E}_{ns}(\mathbb{F}_p) \to 0 \tag{9.1}$$

where the maps are the inclusion and the reduction modulo p.

Proof. We sketch the steps of the proof; for more details see [9, Proposition VII.2.1].

- First notice that $E_1(\mathbb{Q}_p) \subset E_0(\mathbb{Q}_p)$, as the point at infinity is always a non-singular point for the reduction of a cubic in Weierstrass form.
- The group law on $E(\mathbb{Q})$ naturally induces a group structure on the sets in the statement.
- The point above also implies that thereduction modulo p is a group homomorphism.
- Let ι denote the inclusion $E_1(\mathbb{Q}_p) \hookrightarrow E_0(\mathbb{Q}_p)$ and π the reduction $E_0(\mathbb{Q}_p) \to \bar{E}_{\text{ns}}(\mathbb{F}_p)$. From the first point we know that ι is injective. Also, by definition $E_1(\mathbb{Q}_p) = \ker \pi$.
- The surjectivity of π follows from the completeness of $\mathbb{Q}_p$ and Hensel's lemma.

□

It turns out that $E_1(\mathbb{Q}_p)$ is deeply related to the p-torsion points of E.

Proposition 9.3.4. *Any finite order element of $E_1(\mathbb{Q}_p)$ has order a power of p. In particular, if $m \in \mathbb{N}$ is coprime with p, then there are no elements of order m in $E_1(\mathbb{Q}_p)$.*

Proof. We only give a sketch of the strategy of the proof as in [9]. The group $E_1(\mathbb{Q}_p)$ is isomorphic to the formal group associated with E over $p\mathbb{Z}_p$: see [9, Proposition VII.2.2] for a proof of this fact and [9, §§IV.2–3] for the definition of the formal group associated with E over $p\mathbb{Z}_p$. Then the proof of the statement reduces to [9, Proposition IV.3.2]. □

We are now ready to prove that the reduction modulo a prime gives information about the torsion points.

Proposition 9.3.5. *Let $m \in \mathbb{N}$ be coprime with p and assume $\tilde{E}/\mathbb{F}_p$ is non-singular, then the reduction map*

$$E(\mathbb{Q}_p)[m] \to \tilde{E}(\mathbb{F}_p)$$

is injective.

Proof. As p is a prime of good reduction for E, the exact sequence in (9.1) becomes

$$0 \to E_1(\mathbb{Q}_p) \to E(\mathbb{Q}_p) \to \bar{E}(\mathbb{F}_p) \to 0 \,.$$

Let P be an m-torsion point in $E(\mathbb{Q}_p)$. Proposition 9.3.4 tells us that P is not $E_1(\mathbb{Q}_p)$ and hence it is not in the kernel of the reduction map π. Hence, π induces the desired injection. □

Corollary 9.3.6. *Let $m \in \mathbb{N}$ be coprime with p and assume $\tilde{E}/\mathbb{F}_p$ is non-singular, then the reduction map*

$$E(\mathbb{Q})[m] \to \tilde{E}(\mathbb{F}_p)$$

is injective.

Proof. Just notice that $E(\mathbb{Q}) \subset E(\mathbb{Q}_p)$ and hence $E(\mathbb{Q})[m] \subseteq E(\mathbb{Q}_p)[m]$. □

The p-valuation also allows us to to prove another important result about torsion points: the Lutz–Nagell theorem.

Lemma 9.3.7. *Let p be a prime and E and elliptic curve over $\mathbb{Q}$ having short Weierstrass equation*

$$E\colon y^2 = x^3 + ax + b$$

with $a, b \in \mathbb{Z}$. Let $P = (x_P, y_P) \in E(\mathbb{Q}_p)$ be a torsion point of order $m \geq 2$. Then $x_P, y_P \in \mathbb{Z}_p$.

We will only prove this result for m not a power of p. For a more general statement and the proof also of the case $m = p^n$, see [9, Theorem VII.3.4].

Proof. Recall that v_p denotes the p-adic valuation. If $v_p(x_P)$ and $v_p(y_P)$ are both non-negative then there is nothing to prove.

If $v(x_p) \geq 0$ then

$$2v_p(y_P) = v_p(y_P^2) = v_p(x_P^3 + ax_P + b) \geq \min\{3v_p(x_P), v_p(a) + v_p(x_P), v_p(b)\} \geq 0$$

as $a, b, x_P \in \mathbb{Z}_p$, as desired.

So assume $v_p(x_P) < 0$. Then it follows that

$$2v_p(y_P) = v_p(y_P^2) = v_p(x_P^3 + ax_P + b) \geq \min\{3v_p(x_P), v_p(a) + v_p(x_P), v_p(b)\} \,.$$

As $v_p(x_P) < 0$ while $v_p(a), v_p(b) \geq 0$, then $\min\{3v_p(x_P), v_p(a) + v_p(x_P), v_p(b)\} = 3v_p(x_P)$ and the inequality above is in fact an equality, hence

$$2v_p(y_P) = 3v_p(x_P) = -6s < 0 \,.$$

This means that $v_p(x_P), v_p(y_P) < 0$ and hence $\bar{P} = \bar{O}$, yielding $P \in E_1(\mathbb{Q}_p)$. If m is not a power of p, then the statement follows from Proposition 9.3.4. For $m = p^n$, see [9, Theorem VII.3.4(b)]. □

We are now ready to prove Theorem 7.3.4. For the reader's convenience we recall the statement here, using the terminology introduced in thic chapter.

Theorem 9.3.8 (Lutz–Nagell)**.** *Let p be a prime and E and elliptic curve over $\mathbb{Q}$ having minimal Weierstrass equation*

$$E\colon y^2 = x^3 + ax + b$$

with $a, b \in \mathbb{Z}$. Let $P = (x_P, y_P)$ be a torsion point of E of order $m > 1$. Then

1. $x_P, y_P \in \mathbb{Z}$,
2. *if* $m = 2$ *then* $y_P = 0$,
3. *if* $m > 2$ *then* y_P^2 *divides* $4a^3 + 27b^2 = -\Delta(E)/16$.

Proof. (2) This is just the classification of 2-torsion points of elliptic curves given in short Weierstrass form, see Corollary 5.4.9.

(1) We prove that $x_P, y_P \in \mathbb{Z}$. First assume $m = 2$. Then $y_P = 0$ from point (2). This implies that x_P is the rational solution of a monic polynomial with integral coefficients and hence it is an integer (Gauss' lemma). Assume then $m > 2$. For every prime p one can view P as an element of $E(\mathbb{Q}_p)[m]$. Then Lemma 9.3.7 tells us that $x_P, y_P \in \mathbb{Z}_p$. As this is true for every prime, it follows that $x_P, y_P \in \mathbb{Z}$, proving the statement.

(3) By assumption $m \neq 2$ and hence $y_P \neq 0$ and $2P = (x_{2P}, y_{2P}) \neq O$ is a non-trivial torsion point. From point (1) we then have $x_P, y_P, x_{2P} \in \mathbb{Z}$. The duplication formula Corollary 5.4.9 tells us that

$$x_{2P} = \frac{\phi(x_P)}{4\psi(x_P)}$$

with

$$\phi(x) = x^4 - 2ax^2 - 8bx + a^2 \quad \text{and} \quad \psi(x) = x^3 + ax + b\,.$$

Set $f(x) := 3x^2 + 4a$ and $g(x) = 3x^3 - 5ax - 27b$. Then the following equality holds:

$$4a^3 + 27b^2 = f(x)\phi(x) - g(x)\psi(x)\,.$$

Substituting x with x_P and recalling that $y_P^2 = \psi(x_P)$ and $x_{2P} = \frac{\phi(x_P)}{4\psi(x_P)}$ we obtain

$$4a^3 + 27b^2 = y_P^2(4x_{2P}f(x_P) - g(x_P))\,.$$

As all the quantities involved are integers, the statement follows.

□

9.4 The L-series

Let $E/\mathbb{Q}$ be an elliptic curve, and assume p is a prime of good reduction. Then the reduction E_p of E modulo p is also an elliptic curve and we can consider its zeta function. Thanks to theorems 8.4.3 and 8.4.5 we can write it explicitly:

$$Z(E_p, T) = \frac{L_p(T)}{(1-T)(1-pT)},$$

where

$$L_p(T) = 1 - a_pT + pT^2$$

and

$$a_p = p + 1 - \#E_p(\mathbb{F}_p).$$

We can extend the definition of L_p as follows.

Definition 9.4.1. Let $E/\mathbb{Q}$ be an elliptic curve and $p \in \mathbb{Z}$ a prime of bad reduction for E, then

$$L_p(T) := \begin{cases} 1-T & \text{if } E \text{ has split multiplicative reduction at } p, \\ 1+T & \text{if } E \text{ has nonsplit multiplicative reduction at } p, \\ 1 & \text{if } E \text{ has additive reduction at } p. \end{cases}$$

These definitions are motivated by Proposition 8.3.1. Indeed, we have the following result.

Corollary 9.4.2. *Let $E/\mathbb{Q}$ be an elliptic curve and p any prime. Then*

$$L_p(1/p) = \#E_{p,ns}(\mathbb{F}_p)/p\ .$$

Proof. First assume that p is of good reduction. Then E_p is smooth and $\#E_{p,\mathrm{ns}}(\mathbb{F}_p) = \#E_p(\mathbb{F}_p)$. This yields:

$$L_p(1/p) = 1 - \frac{a_p}{p} + \frac{1}{p} = \frac{\#E_p(\mathbb{F}_p)}{p}\ .$$

If p is of bad reduction, then E_p is either split multiplicative, nonsplit multiplicative, or additive. The result then follows from Proposition 8.3.1. □

Definition 9.4.3. We define the L-series of $E/\mathbb{Q}$ as the product

$$L_E(s) := \prod_p \frac{1}{L_p(p^{-s})}.$$

Theorem 9.4.4. *The L-series converges and gives an analytic function to the whole complex plane.*

Proof. It is possible to prove that the L-series converges and gives an analytic function for $\Re(s) > 3/2$, by using that $|a_p| \leq 2\sqrt{p}$.

The full statement was first proven by Deuring and Weil for elliptic curves with complex multiplication.

Eichler and Shimura proved it for modular K3 surfaces. Hence, in light of the modularity theorem by Wiles, it followed that the result holds for all elliptic curves. □

Lemma 9.4.5. *Let E be an elliptic curve over $\mathbb{Q}$, then its L-function has the following series expansion:*

$$L_E(s) = \sum_{n=1}^{\infty} \frac{a_n(E)}{n^s}$$

with $a_1(E) = 1$, $a_p(E) = a_p$ for every prime of good reduction p, and $a_p(E) = \pm 1$ for every prime of bad reduction. The other coefficients $a_n(E)$ are determined by the coefficients a_p for p prime dividing n.

Proof. By definition, $L_E(s) := \prod_p \frac{1}{L_p(p^{-s})}$. Let p be a prime of good reduction, then the factor $L_p(p^{-s})$ equals $1 - a_pT + pT^2$ with $T = p^{-s}$, again by definition. We write the Taylor expansion of $1/L_p(T)$ at 0:

$$\frac{1}{1 - a_pT + pT^2} = 1 + a_pT + (a_p^2 - p)T^2 + \ldots = \sum_{r=0}^{\infty} \frac{a_{p^r}(E)}{p^{rs}}$$

with $a_p(E) = a_p$. Analogously, if p is a prime of multiplicative reduction one can consider the Taylor series of $1/(1 \pm T)$ at 0, with $T = p^{-s}$, getting

$$1/L_p(T) = 1 \mp T + T^2 + \mp T^3 + \ldots = \sum_{r=0}^{\infty} \frac{(\mp 1)^r}{p^{rs}} \ .$$

Then we can write

$$L_E(s) = \left(\prod_{p \text{ good reduction}} \sum_{r=0}^{\infty} \frac{a_{p^r}(E)}{p^{rs}} \right) \left(\prod_{p \text{ bad reduction}} \sum_{r=0}^{\infty} \frac{(\mp 1)^r}{p^{rs}} \right) \ .$$

As every integer $n \in \mathbb{N}$ can be factored $n = p_1^{e_i} \cdots p_m^{e_m}$ in a unique way, the statement follows. □

9.5 The modularity theorem

The L-series of an elliptic curve plays a crucial role in relating elliptic curves and modular forms.

Definition 9.5.1. Let $E/\mathbb{Q}$ be an elliptic curve. We define the *conductor* of E to be the integer

$$N := \prod_p p^{f_p}$$

where

$$f_p := \begin{cases} 0 & \text{if } E \text{ has good reduction at } p, \\ 1 & \text{if } E \text{ has multiplicative reduction at } p, \\ 2 + \delta_p & \text{if } E \text{ has additive reduction at } p. \end{cases}$$

For $p \neq 2, 3$ we have $\delta_p = 0$. For $p = 2, 3$ the quantity δ_p can be determined using the Ogg–Saito formula.

Theorem 9.5.2 (Ogg–Saito formula)**.** *Let $E/\mathbb{Q}$ be an elliptic curve and p a prime. Choose a minimal model of E at p and let Δ_p denote its discriminant. Then*

$$f_p := v_p(\Delta_p) + 1 - m_p \ ,$$

where m_p is the number of irreducible components of the desingularization $\tilde{E}_p$ of the reduction E_p.

Remark 9.5.3. The quantity m_p basically keeps track of the blow-ups needed to resolve the singularity of E_p in case $p = 2, 3$ is of multiplicative reduction. This number can be determined by computing discriminant and j-invariant of E, see [8, Table 15.1].

Theorem 9.5.4 (Modularity)**.** *Let $E/\mathbb{Q}$ be an elliptic curve. Then there exists a cusp form $f \in S_2(\Gamma_0(N))$*

$$f(q) = \sum_{k=1}^{\infty} b_k q^k \ , \quad q = e^{2\pi i z} \ ,$$

where N is the conductor of E, such that

$$b_p = a_p$$

for every prime p of good reduction for E.

9.6 Exercises

The exercises marked with * are harder; those marked with ! are important.

Exercise 9.6.1. Show that any elliptic curve $E/\mathbb{Q}$ admits a minimal short Weierstrass equation defined over $\mathbb{Z}$.

Exercise 9.6.2. Rewrite Proposition 9.2.5 using the Legendre equation of E.

Exercise 9.6.3. Show that the subsets defined in Definition 9.3.1 are indeed subgroups.

Chapter 10

The Birch–Swinnerton-Dyer conjecture

In §9.4 we have introduced the L-function of an elliptic curve defined over $\mathbb{Q}$. It is conjectured, and partially proven, that the L-function of an elliptic curve is related to the rank of the curve. The conjecture was first stated by Birch and Swinnerton-Dyer, the mathematicians it is named after. This conjecture is in the list of the seven Millennium Problems by the Clay institute.

10.1 The statement

The original statement (over $\mathbb{Q}$) is very easy to state.

Conjecture 10.1.1 (Birch–Swinnerton-Dyer (BSD))**.** *Let E be an elliptic curve over $\mathbb{Q}$ and let r denote the rank of $E(\mathbb{Q})$. Let $L_E(s)$ denote the L-function of E. Then $L_E(s)$ has a zero of order r at $s = 1$.*

The conjecture has been checked numerically for many elliptic curves. It has also been proven that

- if E has complex multiplication and $r > 0$, then $L_E(1) = 0$;
- if $L_E(s) \neq 1$ then $r = 0$;
- if $L_E(1) = 0$ and $L'_E(1) \neq 0$ then $r = 1$.

There is also a stronger version of the BSD conjecture, relating the value of L_E at $s = 1$ and some other important values of E.

10.2 The invariant differential and the real period

Let E be an elliptic curve over $\mathbb{Q}$ described by the minimal short Weierstrass equation $y^2 = x^3+ax+b$ (see §9.1).

Definition 10.2.1. We define the *invariant differential* of E to be the 1-differential form

$$\omega_E := \frac{dx}{2y}$$

Lemma 10.2.2. *Let E and ω_E be defined as above. Then*

$$\omega_E = \frac{dy}{3x^2 + a}$$

Proof. As $y^2 = x^3 + ax + b$ it follows that

$$3x^2 + a = \frac{d(x^3 + ax + b)}{dx} = \frac{y^2}{dx} = \frac{d(y^2)}{dy}\frac{dy}{dx} = 2y\frac{dy}{dx}$$

hence

$$\frac{dy}{3x^2 + a} = \frac{dx}{2y} = \omega_E \ .$$

□

Remark 10.2.3. The adjective 'invariant' is earned as the differential is invariant under translation by an element of E.

Proposition 10.2.4. *Let E and ω_E be defined as above. Then ω_E is holomorphic and non-vanishing, i.e.,* $\operatorname{div}(\omega_E) = 0$.

Proof. By direct computations. Show that if $P \in E \setminus \{\mathcal{O}\}$ then it cannot be a pole nor a zero for ω_E. Then do the same for $\mathcal{O}$ using an affine chart containing it. □

Now consider the real points of E, that is $E(\mathbb{R})$. We can then integrate ω_E over $E(\mathbb{R})$, getting the following quantity

$$\Omega_E := \int_{E(\mathbb{R})} |\omega_E| \ . \tag{10.1}$$

Let $e_E(\mathbb{R})$ denote the number of connected components of $E(\mathbb{R})$: then

$$e_E(\mathbb{R}) = \begin{cases} 1 & \text{if } \Delta(E) < 0 \ , \\ 2 & \text{if } \Delta(E) > 0 \ . \end{cases}$$

If the equation defining E is minimal, then $2\Omega_E / e_E(\mathbb{R})$ is *the real period* of E.

Remark 10.2.5. If we view E as an elliptic curve over $\mathbb{C}$, then E corresponds to a complex torus $\mathbb{C}/\Lambda$, where $\Lambda \subset \mathbb{C}$ is a lattice, see chapter 1. The *real period* of E is then defined as the smallest positive element τ_1 in $\Lambda \cap \mathbb{R}$. In fact, one can write $\Lambda = \tau_1\mathbb{Z} + \tau_2\mathbb{Z}$ for some $\tau_2 \in \mathbb{C}$ such that $\Im(\tau_1/\tau_2) > 0$. So, in particular, $\Omega_E = e_E(\mathbb{R})\tau_1/2$. The real period can be effectively computed in practice. For more information about *the periods* of an elliptic curve see §1.5.

10.3 The Shafarevich–Tate group

Let E be an elliptic curve over $\mathbb{Q}$ and let $\phi \in \mathrm{End}(E)$ be an isogeny. Denote the kernel of ϕ by $E[\phi] := \ker \phi$. As non-constant maps between curves are surjective over algebraically closed fields, we have the following short exact sequence.

$$0 \longrightarrow E[\phi] \longrightarrow E \xrightarrow{\phi} E \longrightarrow 0$$

Let $G = \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ be the absolute Galois group of $\mathbb{Q}$. Then, by taking the G-invariant part of the above short exact sequence and then considering the Galois cohomology, we get the following exact sequence.

$$\begin{array}{l} 0 \longrightarrow E(\mathbb{Q})[\phi] \longrightarrow E(\mathbb{Q}) \xrightarrow{\phi} E(\mathbb{Q}) \xrightarrow{\delta} \\ \quad H^1(G, E[\phi]) \longrightarrow H^1(G, E) \xrightarrow{\phi} H^1(G, E) \end{array} \tag{10.2}$$

Let p be a prime or $p = \infty$ and consider the completion $\mathbb{Q}_p$ and its algebraic closure $\bar{\mathbb{Q}}_p$. Let $G_p := \mathrm{Gal}(\bar{\mathbb{Q}}_p/\mathbb{Q}_p)$ the absolute Galois group of $\mathbb{Q}_p$. We can then consider E over $\bar{\mathbb{Q}}_p$ and proceed with the Galois cohomology, obtaining a short exact sequence analogous to (10.2). In this way we define $H^1(G_p, E)$.

As for every p the group G_p can be embedded into G, considering also the natural embedding $\mathbb{Q} \hookrightarrow \mathbb{Q}_p$, we get a map

$$H^1(G, E) \to \prod_p H^1(G_p, E) \ . \tag{10.3}$$

Definition 10.3.1. We define the Shafarevich–Tate group of E over $\mathbb{Q}$, denoted by $Ш(E/\mathbb{Q})$, as the kernel of (10.3).

Remark 10.3.2. Equivalently, $Ш(E/\mathbb{Q})$ can be defined as the intersection

$$\bigcap_p \ker \left\{ H^1(G, E) \to H^1(G_p, E) \right\} \ .$$

Remark 10.3.3. Given an elliptic curve E over $\mathbb{Q}$, the group $Ш(E/\mathbb{Q})$ is very difficult to compute. In general, it is not even known, only conjectured, that it is finite.

10.4 Heights and the regulator

Let E be an elliptic curve over $\mathbb{Q}$. In this subsection we will construct a pairing for the points of $E(\bar{\mathbb{Q}})$.

First consider an embedding of E inside $\mathbb{P}^2$. Let $P = (x_P : y_P : z_P) \in E(\mathbb{Q}) \subset \mathbb{P}^2$ be a point with integer coordinates $x_P, y_P, z_P \in \mathbb{Z}$.

Definition 10.4.1. We define the *height* of P to be

$$H(P) := \max\{|x_P|, |y_P|, |z_P|\} \ .$$

We define its *logarithmic height* to be

$$h(P) := \log H(P) \ .$$

Remark 10.4.2. As x_P, y_P, z_P are integers not all equal to 0, it follows that $h(P) \geq 0$ for all $P \in E(\mathbb{Q})$.

An analogous construction of h works on projective spaces of any dimension and it can be generalized to any algebraic extension of $\mathbb{Q}$.

Let $f \in \bar{K}(E)$ be a function of E, i.e., f defines a map $f\colon E \to \mathbb{P}^1$ sending a point P to $(1:0)$ if P is a pole and to $(f(P):1)$ otherwise.

Definition 10.4.3. We define the *height on E relative to f* to be

$$h_f\colon E(\mathbb{Q}) \to \mathbb{R}, \quad h_f(P) := h(f(P)) \,.$$

Let $f \in K(E)$ be a nonconstant even function on E and, for $P \in E(\bar{\mathbb{Q}})$ and $N \in \mathbb{N}$ consider the quantity

$$4^{-N} h_f(2^N P) \,.$$

This quantity clearly depends on f, but letting N run to infinity it becomes independent of it.

Lemma 10.4.4. *The limit*

$$\frac{1}{\deg f} \lim_{N\to\infty} 4^{-N} h_f(2^N P)$$

exists and it is independent of f.

Proof. [9, Proposition VIII.9.1]. □

Definition 10.4.5. Let $f \in K(E)$ be a nonconstant even function. We define the *canonical (or Néron–Tate) height* on $E/\mathbb{Q}$, denoted by $\hat{h}$, to be the function

$$\hat{h}\colon E(\bar{\mathbb{Q}}) \to \mathbb{R} \,, \quad P \mapsto \frac{1}{\deg f} \lim_{N\to\infty} 4^{-N} h_f(2^N P) \,.$$

Consider then the pairing,

$$\langle \cdot\,,\, \cdot \rangle\colon E(\bar{\mathbb{Q}}) \times E(\bar{\mathbb{Q}}) \to \mathbb{R} \,, \quad \langle P, Q\rangle := \hat{h}(P+Q) - \hat{h}(P) - \hat{h}(Q) \,. \tag{10.4}$$

Theorem 10.4.6. *The canonical height $\hat{h}$ is quadratic and the pairing in (10.4) is bilinear. Moreover, it extends to a positive definite quadratic form on the real vector space $E(\mathbb{Q}) \times \mathbb{R} \cong \mathbb{R}^r$.*

Proof. See [9, Theorem VIII.9.3] and [9, Proposition VIII.9.6]. □

Mordell–Weil theorem tells us that $E(\mathbb{Q})$ is finitely generated and hence $E(\mathbb{Q})/E_{\text{tors}}(\mathbb{Q})$ is a free abelian group, that is, it is isomorphic to $\mathbb{Z}^r$ for some r. Let $P_1, \dots P_r$ be generators of $E(\mathbb{Q})/E_{\text{tors}}(\mathbb{Q})$.

Definition 10.4.7. We define the *ellliptic regulator of $E/\mathbb{Q}$*, denoted by $R_{E/\mathbb{Q}}$ to be

$$R_{E/\mathbb{Q}} := \det\left(\langle P_i, P_j\rangle\right)_{1\leq i,j\leq r} \,.$$

We set $R_{E/\mathbb{Q}} := 1$ if $r = 0$.

Remark 10.4.8. Notice that $R_{E/\mathbb{Q}}$ does not depend on the choice of the generators of $E(\mathbb{Q})/E_{\text{tors}}(\mathbb{Q})$. Moreover, Theorem 10.4.6 implies that $R_{E/\mathbb{Q}} > 0$.

10.5 The fudge factors

Let E be an elliptic curve over $\mathbb{Q}$ and let p be a prime. In §9.3 we defined the following subgroups of $E(\mathbb{Q})$:

$$\begin{aligned}\bar{E}_{\mathrm{ns}}(\mathbb{F}_p) &:= \{\text{non-singular points of } \bar{E}(\mathbb{F}_p)\},\\ E_0(\mathbb{Q}_p) &:= \{P \in E(\mathbb{Q}_p) \ : \ \bar{P} \in \bar{E}_{\mathrm{ns}}(\mathbb{F}_p)\},\\ E_1(\mathbb{Q}_p) &:= \{P \in E(\mathbb{Q}_p) \ : \ \bar{P} = \bar{O}\}.\end{aligned}$$

One can then consider the quotient $E(\mathbb{Q}_p)/E_0(\mathbb{Q}_p)$. A very deep result by Kodaira and Néron implies that $E(\mathbb{Q}_p)/E_0(\mathbb{Q}_p)$ is finite. In fact more is true.

Corollary 10.5.1. *The quotient $E(\mathbb{Q}_p)/E_0(\mathbb{Q}_p)$ is finite.*
If E has split multiplicative reduction at p, then $E(\mathbb{Q}_p)/E_0(\mathbb{Q}_p)$ is cyclic of order $-\mathrm{ord}_p(j(E))$. In all the other cases it has order at most 4.

Proof. See [9, Corollary C15.2.1]. □

Definition 10.5.2. We define the *fudge factor* of $E/\mathbb{Q}$ at p as the order

$$c_p := \#\frac{E(\mathbb{Q}_p)}{E_0(\mathbb{Q}_p)}\ .$$

10.6 The strong BSD

We now have all the elements to state the strong version of the Birch–Swinnerton-Dyer conjecture.

Conjecture 10.6.1 (Strong BSD)**.** *Let E be an elliptic curve over $\mathbb{Q}$ with rank r. Then the following equality holds:*

$$\lim_{s\to 1}\frac{L_E(s)}{(s-1)^r} = \frac{2^r\Omega\#Ш(E/\mathbb{Q})R(E/\mathbb{Q})\prod_p c_p}{\#E_{tors}(\mathbb{Q})^2}\ .$$

Remark 10.6.2. As the number of points is invariant under isogenies, also the L-series is invariant under isogenies and hence so is $\lim_{s\to 1}\frac{L_E(s)}{(s-1)^r}$. This implies that also the quantity

$$\frac{2^r\Omega\#Ш(E/\mathbb{Q})R(E/\mathbb{Q})\prod_p c_p}{\#E_{\mathrm{tors}}(\mathbb{Q})^2}$$

is invariant under isogenies, although none of the elements involved is invariant. The invariance was proved by Cassels.

Chapter 11

The 2-Selmer group

In this section we will define the Selmer group of an elliptic curve E over $\mathbb{Q}$, we will see its properties and how to use it to get information about the rank of $E(\mathbb{Q})$.

11.1 Definition using Galois cohomology

Let E be an elliptic curve over $\mathbb{Q}$ and let $[2] \in \mathrm{End}(E)$ be the isogeny given by the multiplication by 2. As non-constant maps between curves are surjective over algebraically closed fields, we have the following short exact sequence.

$$0 \longrightarrow E[2] \longrightarrow E \xrightarrow{2} E \longrightarrow 0$$

Let $G := \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ be the absolute Galois group. As in §10.3 we consider the long exact sequence involving the Galois cohomology groups.

$$\begin{array}{l} 0 \longrightarrow E(\mathbb{Q})[2] \longrightarrow E(\mathbb{Q}) \xrightarrow{2} E(\mathbb{Q}) \xrightarrow{\delta} \\ \quad H^1(G, E[2]) \longrightarrow H^1(G, E) \xrightarrow{2} H^1(G, E) \end{array} \tag{11.1}$$

From the above sequence we obtain the following short exact sequence.

$$0 \longrightarrow E(\mathbb{Q})/2E(\mathbb{Q}) \xrightarrow{\delta} H^1(G, E[2]) \longrightarrow H^1(G, E)[2] \longrightarrow 0$$

As in the case for the Shafarevich group, for every place p (finite or infinite) we consider the p-adic completion $\mathbb{Q}_p$ and the absolute Galois group $G_p := \mathrm{Gal}(\bar{\mathbb{Q}}_p/\mathbb{Q}_p) \hookrightarrow G$. Then we can repeat the whole argument over $\mathbb{Q}_p$ as above, getting the following morphism of short exact sequences.

$$\begin{array}{ccccccccc} 0 & \longrightarrow & E(\mathbb{Q})/2E(\mathbb{Q}) & \xrightarrow{\delta} & H^1(G, E[2]) & \longrightarrow & H^1(G, E)[2] & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & \prod_p E(\mathbb{Q}_p)/2E(\mathbb{Q}_p) & \xrightarrow{\delta} & \prod_p H^1(G_p, E[2]) & \longrightarrow & \prod_p H^1(G_p, E)[2] & \longrightarrow & 0 \end{array}$$

Definition 11.1.1. We define the 2-*Selmer group* of $E/\mathbb{Q}$ to be the kernel $S^{(2)}(E/\mathbb{Q})$ of the map

$$H^1(G, E[2]) \to \prod_p H^1(G_p, E)[2] \ .$$

Theorem 11.1.2. *Let E be an elliptic curve over $\mathbb{Q}$. The 2-Selmer group $S^{(2)}(E/\mathbb{Q})$ is a finite elementary abelian 2-group and it sits in the following short exact sequence.*

$$0 \longrightarrow E(\mathbb{Q})/2E(\mathbb{Q}) \longrightarrow S^{(2)}(E/\mathbb{Q}) \longrightarrow Ш(E/\mathbb{Q})[2] \longrightarrow 0 \tag{11.2}$$

Proof. See [9, Theorem X.4.2]. □

Remark 11.1.3. As opposed to the Tate–Shafarevich group, the 2-Selmer group is actually computable in practice. Theorem 11.1.2 tells us that $S^{(2)}(E/\mathbb{Q})$ is isomorphic to $(\mathbb{Z}/2\mathbb{Z})^s$, for some $s \in \mathbb{N}$, and that $E(\mathbb{Q})/2E(\mathbb{Q}) \hookrightarrow S^{(2)}(E/\mathbb{Q})$. As $E(Q) \cong E_{\text{tors}}(\mathbb{Q}) \oplus \mathbb{Z}^r$, Mazur's theorem yields

$$E(\mathbb{Q})/2E(\mathbb{Q}) \cong (\mathbb{Z}/2\mathbb{Z})^{r+d},$$

where d is the number of non-trivial 2-torsion elements in $E(\mathbb{Q})[2]$, hence $d = 0, 1, 3$. Then it follows $r + d \leq s$. As d is easy to compute, we get the following upper bound for the rank of E:

$$r \leq s - d \ . \tag{11.3}$$

In the next subsections, we will try to give an idea of how to compute it.

11.2 Homogeneous spaces

The first approach to compute the 2-Selmer group is geometric. Let E be an elliptic curve over $\mathbb{Q}$.

Definition 11.2.1. An homogeneous space for $E/\mathbb{Q}$ is a smooth curve $C/\mathbb{Q}$ with a morphism

$$\mu \colon C \times E \to C$$

such that

(i) $\mu(p, O) = O$ for every $p \in C$,

(ii) $\mu(\mu(p, P), Q) = \mu(p, P + Q)$ for every $p \in C$ and $P, Q \in E$,

(iii) for every $p, q \in C$ there exists a unique $P \in E$ such that $\mu(p, P) = q$.

The properties above motivate the notation $p + P := \mu(p, P) \in C$.

Remark 11.2.2. In other words, C is a smooth curve endowed with a simply transitive group action of E. From this, it immediately follows that C is isomorphic to E as curve, i.e., C is a genus 1 curve. Given a point $p_0 \in C$, then we have an isomorphism

$$E \to C, \ P \mapsto p_0 + P$$

which is defined over $\mathbb{Q}(p_0)$, meaning the field extension of $\mathbb{Q}$ obtained adjoining the coordinates of p_0. In particular, $C/\mathbb{Q}$ is a *twist* of $E/\mathbb{Q}$, i.e., C is isomorphic to E over $\bar{\mathbb{Q}}$. Recall that, by Proposition 6.2.14, every twist of an elliptic curve is the composition of an isogeny with a translation.

Remark 11.2.3. Using the last property, one can define a 'subtraction' between points of C, which takes value in E. In this way we get that using the $+$ and $-$ notation provides the right intuition.

Let $\mathrm{HS}(E)$ denote the set of all homogeneous spaces of E.

Definition 11.2.4. Let $(C/\mathbb{Q}, \mu), (C'/\mathbb{Q}, \mu')$ be two homogeneous spaces of $E/\mathbb{Q}$. We say that they are equivalent, denoted by $(C/\mathbb{Q}, \mu) \sim (C'/\mathbb{Q}, \mu')$ if there is an isomorphism $\theta\colon C \to C'$ compatible with the E-group action, that is, for every $p \in C, P \in E$

$$\theta(p + P) = \theta(p) + P \ .$$

Notice that $E \in \mathrm{HS}(E)$.

Definition 11.2.5. We call the *Weil–Châtelet group for* $E/\mathbb{Q}$ the quotient $\mathrm{HS}(E/\mathbb{Q})/\sim$, denoted by $\mathrm{WC}(E/\mathbb{Q})$. Given a homogeneous space $C \in \mathrm{HS}(E/\mathbb{Q})$, we denote by $\{C\}$ its class in $\mathrm{WC}(E/\mathbb{Q})$.

It is possible to define an operation on $\mathrm{WC}(E)$.

Lemma 11.2.6. *Let $C_1, C_2 \in \mathrm{HS}(E)$ be two homogeneous spaces. Then, up to $\sim$, there is a uniquely determined $C_3 \in \mathrm{HS}(E)$ and a morphism $\phi\colon C_1 \times C_2 \to C_3$ such that*

$$\phi(p_1 + P_1, p_2 + P_2) = \phi(p_1, p_2) + P_1 + P_2 \ .$$

Proof. [9, Exercise 10.2(a),(b)]. □

Using Lemma 11.2.6 we can then define an operation in $\mathrm{WC}(E)$.

Definition 11.2.7. Let C_1, C_2, C_3 be as in Lemma 11.2.6. We define the sum $\{C_1\} + \{C_2\}$ to be $\{C_3\}$.

Proposition 11.2.8. *The set $\mathrm{WC}(E/\mathbb{Q})$ with the sum defined in Definition 11.2.7 is a group with $\{E\}$ as the neutral element. Moreover, it is isomorphic to $H^1(G, E)$ via the map sending the class $\{C\}$ to the cocycle $\{\sigma \mapsto p_0^\sigma - p_0\}$, where p_0 is any point of C.*

Proof. [9, Theorem X.3.6] and [9, Exercise 10.2(c)]. □

Corollary 11.2.9. $\{C\} = \{E\} \iff C(\mathbb{Q}) \neq \emptyset$.

The two results above allow us to view $S^{(2)}(E/\mathbb{Q})$ as the kernel of the map

$$H^1(G, E[2]) \to \prod_p \mathrm{WC}(E/\mathbb{Q}_p)[2] \ .$$

From here, we start to see that the non-trivial elements of $S^{(2)}(E/\mathbb{Q})$ are related to covers of E that have points everywhere locally but not over $\mathbb{Q}$. From Equation 11.2 it also follows that $Ш(E/\mathbb{Q})[2]$ is isomorphic to the quotient $\frac{S^{(2)}(E/\mathbb{Q})}{E(\mathbb{Q})/2E(\mathbb{Q})}$ and so we can see how the non-trivial 2-torsion elements of $Ш(E/\mathbb{Q})$ correspond to the covers of E for which the local-global principle fails.

11.3 Covering spaces

In this subsection we re-introduce the homogeneous spaces in the case as 2-covering spaces. Let $E/\mathbb{Q}$ be an elliptic curve and consider the isogeny $[2]\colon E \to E$ given by the multiplication by 2. Let $C/\mathbb{Q}$ be *a twist* of E, that is, C is isomorphic to E over $\bar{\mathbb{Q}}$. Let $\theta\colon C \to E$ be the isomorphism over $\bar{\mathbb{Q}}$.

Definition 11.3.1. We say that $C/\mathbb{Q}$ is a 2-covering of $E/\mathbb{Q}$ if there is a map ν over $\mathbb{Q}$ such that for every $p \in C$ one has $\nu(p) = 2\theta(p)$. In other words, the following diagram commutes.

$$\begin{array}{ccc} C & & \\ \downarrow{\scriptstyle\theta} & \searrow^{\nu} & \\ E & \xrightarrow{2} & E \end{array}$$

Definition 11.3.2. Let $(C_1, \theta_1, \nu_1), (C_2, \theta_2, \nu_2)$ be two 2-coverings of E. We say that C_1 and C_2 are equivalent if there is a birational map $\phi\colon C_1 \to C_2$ over $\mathbb{Q}$ such that the following diagram commutes:

$$\begin{array}{ccc} C_1 & \xrightarrow{\phi} & C_2 \\ \downarrow{\scriptstyle\theta_1} & & \downarrow{\scriptstyle\theta_2} \\ E & \xrightarrow{\tau_T} & E \end{array}$$

where $\tau_T\colon P \mapsto P + T$ is the translation by a 2-torsion point $T \in E[2]$.

Lemma 11.3.3. *A 2-covering of $E/\mathbb{Q}$ correspond to an element of $\mathrm{HS}(E/\mathbb{Q})$. Its class in $\mathrm{WC}(E/\mathbb{Q})$ has order 2. The converse also holds.*

Proof. See [1] or exercise. □

From this it follows that the set of 2-coverings of E forms a group, namely $\mathrm{WC}(E/\mathbb{Q})[2]$.

Lemma 11.3.4. *Every non-trivial element of $\mathrm{WC}(E/\mathbb{Q})[2]$ can be written as the class of*

$$C\colon y^2 = ax^4 + bx^3 + cx^2 + dx + e$$

with $a, b, c, d, e \in \mathbb{Q}$.

Definition 11.3.5. Let $C/\mathbb{Q}$ be a curve given by $C\colon y^2 = ax^4 + bx^3 + cx^2 + dx + e$. We define the following quantities for C:

$$\begin{aligned} I &:= 12ae - 3bd + c^2\ , \\ J &:= 72ace + 9bcd - 27ad^2 - 27eb^2 - 2c^3\ . \end{aligned}$$

Lemma 11.3.6. *Let $C/\mathbb{Q}$ be a curve given by $C\colon y^2 = ax^4 + bx^3 + cx^2 + dx + e$. Then C is a 2-covering of $E\colon y^2 = x^3 - 27Ix - 27J$.*

Let C' be another 2-covering of E. Then $C \sim C'$ if and only if $I' = \lambda^4 I$ and $J' = \lambda^6 J$ for some $\lambda \in \mathbb{Q}^*$.

Given these results, in order to compute $S^2(E/\mathbb{Q})$ for an elliptic curve $E\colon y^2 = x^3 + Ax + B$ we have to perform the following steps:

1. find all the degree-4 polynomials $g(x) \in \mathbb{Q}[x]$ such that $I = A$ and $J = B$; for each such $g(x)$, consider the 2-covering of E given by $C\colon y^2 = g(x)$;
2. reduce the list by taking only one C for equivalence class;
3. discard the coverings C for which there is place p such that $C(\mathbb{Q}_p) = \emptyset$;
4. from the remaining coverings, discard those who have a point over $\mathbb{Q}$ (as they again yield the trivial covering)

See [1, Theorem 1]. For an implementation see [2, Section III.6].

Chapter 12

Double covers of the line

In this section we present elliptic curves as double covers of the projective line ramified above four points. This approach has the advantage of introducing the Legendre equation and the j-invariant of an Elliptic curve in a more natural way.

12.1 The cross-ratio

In this subsection we will mostly follow [7, §2.3]. Let $z_1, z_2, z_3, z_4 \in \mathbb{C}$ be pairwise distinct points.

Definition 12.1.1. We define the *cross-ratio* of the 4-tuple $(z_1, z_2, z_3, z_4) \in \mathbb{C}^4$ of pairiwse distinct points as the quantity

$$(z_1, z_2; z_3, z_4) := \frac{z_1 - z_3}{z_1 - z_4} : \frac{z_2 - z_3}{z_2 - z_4} = \frac{(z_1 - z_3)(z_2 - z_4)}{(z_1 - z_4)(z_2 - z_3)} .$$

Using the embedding $\mathbb{C} \hookrightarrow \mathbb{P}^1_{\mathbb{C}},\ z \mapsto (1 : z)$, one can extend the definition of the cross-ratio to four pairwise distinct points $z_i = (a_i : b_i) \in \mathbb{P}^1_{\mathbb{C}}$.

Definition 12.1.2. We define the cross-ratio of the 4-tuple $(z_1, z_2, z_3, z_4) \in (\mathbb{P}^1_{\mathbb{C}})^4$ as the quantity

$$(z_1, z_2; z_3, z_4) := \frac{[13][24]}{[14][23]} \in \mathbb{P}^1_{\mathbb{C}},$$

where

$$[ij] := \det \begin{pmatrix} a_i & a_j \\ b_i & b_j \end{pmatrix}.$$

Remark 12.1.3. Notice that if $z_1 = \infty = (0 : 1)$, then

$$(z_1, z_2; z_3, z_4) = ((0 : 1), (1 : b_2); (1 : b_3), (1 : b_4)) = \frac{b_2 - b_4}{b_2 - b_3}.$$

From this we deduce that the cross-ratio of three pairwise distinct points in $\mathbb{C} \subset \mathbb{P}^1_{\mathbb{C}}$ and $\infty \in \mathbb{P}^1_{\mathbb{C}}$ is just the ratio obtained from Definition 12.1.1 deleting the terms in which ∞ appears.

Example 12.1.4. The cross-ratio of the points $1, 2, 3, 4 \in \mathbb{P}^1$ is

$$\frac{-2}{-3} : \frac{-1}{-2} = \frac{4}{3}.$$

The cross-ratio of the points $1, 2, 3, \infty \in \mathbb{P}^1$ is

$$\frac{-2}{-1} = 2.$$

One can further extend the definition of the cross-ratio for 4-tuple of points in $\mathbb{P}^1_{\mathbb{C}}$ such that no three of them are equal.

Definition 12.1.5. Let $U \subset (\mathbb{P}^1_{\mathbb{C}})^4$ be the set of 4-tuples of points such that no three of the points are equal. Then we define the cross-ratio as above.

$$(-;-)\colon U \to \mathbb{P}^1_{\mathbb{C}}$$

Lemma 12.1.6. *The cross-ratio $(-;-)\colon U \to \mathbb{P}^1_{\mathbb{C}}$ is surjective.*

Proof. For every $z \in \mathbb{P}^1_{\mathbb{C}} \setminus \{0, 1, \infty\}$ we have that $(0, \infty; z, 1) = z$.

Moreover

$$\begin{aligned}(a, a; z_3, z_4) &= (a, a; b, b) = (z_1, z_2; b, b) = 1\\ (a, z_2; a, z_4) &= (a, b; a, b) = (z_1, b; z_3, b) = 0\\ (a, z_2; z_3, a) &= (a, b; b, a) = (z_1, b; b, z_4) = \infty.\end{aligned}$$

□

The group PGL_2 acts on $\mathbb{P}_1$: let $g = \begin{pmatrix}\alpha & \beta\\ \gamma & \delta\end{pmatrix}$ be an element in PGL_2, then it sends the point $z = (a : b) \in \mathbb{P}^1$ to the point

$$z' = g \cdot z := \begin{pmatrix}\alpha & \beta\\ \gamma & \delta\end{pmatrix}\begin{pmatrix}a\\ b\end{pmatrix} = (\alpha a + \beta b : \gamma a + \delta b).$$

Remark 12.1.7. An element of $\mathrm{PGL}_2(\mathbb{C})$ viewed as an automorphism of $\mathbb{P}^1_{\mathbb{C}}$ is also called a *Möbius transformation*.

Proposition 12.1.8. *The group $\mathrm{PGL}_2(\mathbb{C})$ acts sharply 3-transitively on $\mathbb{P}^1_{\mathbb{C}}$, i.e., for any triple of pairwise distinct points $z_1, z_2, z_3 \in \mathbb{P}^1_{\mathbb{C}}$ and $x_1, x_2, x_3 \in \mathbb{P}^1_{\mathbb{C}}$ there is exactly one element $g \in \mathrm{PGL}_2(\mathbb{C})$ such that $g \cdot x_i = z_i$ for $i = 1, 2, 3$.*

Proof. Notice that it is enough to consider $(x_1, x_2, x_3) = (0, \infty, 1)$. Let $v_1, v_2, v_3 \in \mathbb{C}^2$ be three vectors representing z_1, z_2, z_3, respectively. As the points z_1, z_2, z_3 are pairwise distinct, the vectors v_1, v_2, v_3 are pairwise linearly independent so we can write $v_3 = \lambda v_1 + \mu v_2$ for some $\lambda, \mu \in \mathbb{C}^*$. We can then define an automorphism of $\mathbb{C}^2$ by sending the standard basis $(e_1, e_2) = ((1, 0), (0, 1))$ to $(\lambda v_1, \mu v_2)$. Denote this automorphism by $\gamma \in \mathrm{GL}_2(\mathbb{C})$ and notice that $\gamma \cdot (e_1 + e_2) = v_3$. Let $g := [\gamma]$ its image in $\mathrm{PGL}_2(\mathbb{C})$ and notice that

$$g \cdot x_1 = g \cdot 0 = [\lambda v_1] = z_1,$$

$$g \cdot x_2 = g \cdot \infty = [\mu v_2] = z_2,$$
$$g \cdot x_3 = g \cdot 1 = [\lambda v_1 + \mu v_2] = z_3,$$

proving the statement. □

The action of PGL_2 on $\mathbb{P}_1$ diagonally induces an action on $(\mathbb{P}_1)^4$. One might then wonder how is the cross-ratio affected by this action. It turns out that the cross-ratio is invariant, as shown by the following result.

Proposition 12.1.9. *The cross-ratio $(-;-)\colon U \to \mathbb{P}^1_{\mathbb{C}}$ is invariant under the action of $\mathrm{PGL}_2(\mathbb{C})$ on $U \subset (\mathbb{P}^1_{\mathbb{C}})^4$.*

Proof. For $i = 1, 2, 3, 4$, consider the point $z_i = (a_i : b_i) \in \mathbb{P}^1$ and take $g \in \mathrm{PGL}_2$. Let $z_i' = (a_i' : b_i')$ denote $g \cdot z_i$. Then

$$\det \begin{pmatrix} a_i' & a_j' \\ b_i' & b_j' \end{pmatrix} = \det \left(g \cdot \begin{pmatrix} a_i & a_j \\ b_i & b_j \end{pmatrix} \right) = \det g \cdot \det \begin{pmatrix} a_i & a_j \\ b_i & b_j \end{pmatrix}.$$

From this it immediately follows that

$$(z_1, z_2; z_3, z_4) = (z_1', z_2'; z_3', z_4').$$

□

In Proposition 12.1.8 we have seen that PGL_2 acts 3-transitively on $\mathbb{P}^1$. The cross ratio is useful to see when two 4-tuples of pairwise distinct points lie in the same orbit in $(\mathbb{P}^1)^4$.

Proposition 12.1.10. *Let x_1, x_2, x_3, x_4 and z_1, z_2, z_3, z_4 be two 4-tuples of pairwise distinct points in $\mathbb{P}^1_{\mathbb{C}}$. Then there is a Möbius transformation $g \in \mathrm{PGL}_2(\mathbb{C})$ sending z_i to x_i for $i = 1, 2, 3, 4$ if and only if*

$$(x_1, x_2; x_3, x_4) = (z_1, z_2; z_3, z_4).$$

If this is the case, then g is unique.

Proof. As before, it is enough to consider $(x_1, x_2, x_3, x_4) = (x_1, 1, 0, \infty)$, with $x_1 \in \mathbb{C}$. Then, by Proposition 12.1.8, there is a unique transformation $g \in \mathrm{PGL}_2(\mathbb{C})$ sending z_i to x_i for $i = 2, 3, 4$. It is easy to see that g is the transformation defined by:

$$g\colon z \mapsto \frac{z - z_3}{z - z_4} \frac{z_2 - z_4}{z_2 - z_3}.$$

Then

$$g(z_1) = \frac{z_1 - z_3}{z_1 - z_4} \frac{z_2 - z_4}{z_2 - z_3} = (z_1, z_2; z_3, z_4)$$

and $x_1 = (x_1, 1, 0, \infty) = (x_1, x_2, x_3, x_4)$, proving the statement. □

Corollary 12.1.11. *Let (z_1, z_2, z_3, z_4) be a 4-tuple of pairwise distinct points and let λ denote its cross-ratio. Then there exists an element of PGL_2 sending (z_1, z_2, z_3, z_4) to $(\lambda, 1, 0, \infty)$.*

Proof. Notice that $(z_1, z_2; z_3, z_4) = (\lambda, 1; 0, \infty)$. Then the statement follows directly from Proposition 12.1.10. □

Let z_1, z_2, z_3, z_4 be four pairwise distinct points of $\mathbb{P}^1$. Then the permutation group S_4 acts on them by changing the order and one might ask how this action affects their cross-ratio.

Proposition 12.1.12. *Let z_1, z_2, z_3, z_4 be four pairwise distinct points of $\mathbb{P}^1$ and let S_4 act on them by permutation. Let $\lambda := (z_1, z_2; z_3, z_4) \in \mathbb{P}^1$ denote their cross-ratio. Then:*

- *the cycles $1, (12)(34), (13)(24), (14)(23)$ act trivially on λ;*
- *the cycles (12) and (34) send λ to $\frac{1}{\lambda}$;*
- *the cycles (14) and (23) send λ to $1-\lambda$;*
- *the cycles (13), (24), and (1234) send λ to $\frac{\lambda}{\lambda-1}$;*
- *the cycle (123) sends λ to $\frac{\lambda-1}{\lambda}$;*
- *the cycle (132) sends λ to $\frac{1}{1-\lambda}$.*

The orbit of λ under the action of S_4 is

$$\left\{\lambda, \frac{1}{\lambda}, 1-\lambda, \frac{\lambda}{\lambda-1}, \frac{1}{1-\lambda}, \frac{\lambda-1}{\lambda}\right\}.$$

Proof. By direct computations. □

Notice that the stabilizer of λ is the group given by $1, (12)(34), (13)(24), (14)(23)$, i.e., the Klein group V_4.

Proposition 12.1.12 means that there is an action of S_4 on $\mathbb{P}^1$, that is, a group homomorphism

$$\chi\colon S_4 \to \mathrm{PGL}_2(\mathbb{C}). \tag{12.1}$$

Moreover, the kernel of χ is the group given by $1, (12)(34), (13)(24), (14)(23)$, i.e., the Klein group V_4.

Remark 12.1.13. As the quotient S_4/V_4 is isomorphic to S_3, the map χ induces an action of S_3 on PGL_4. Moreover, the group S_3 is given the classes of the elements

$$\{1, (12), (23), (13), (123), (132)\}.$$

Alternatively, one can write S_3 as the following subgroup of $\mathrm{GL}_2(\mathbb{Z})$:

$$\left\{\begin{pmatrix}1&0\\0&1\end{pmatrix}, \begin{pmatrix}0&1\\1&0\end{pmatrix}, \begin{pmatrix}-1&1\\0&1\end{pmatrix}, \begin{pmatrix}1&0\\1&-1\end{pmatrix}, \begin{pmatrix}0&1\\-1&1\end{pmatrix}, \begin{pmatrix}1&-1\\1&0\end{pmatrix}\right\}.$$

Let $\mathbb{P}^1/S_4$ denote the quotient of $\mathbb{P}^1$ modulo the action of S_4 given by χ, then we have the following corollary.

Corollary 12.1.14. *The map*

$$(-,-)\colon (\mathbb{P}^1)^4 \supset U \to \mathbb{P}^1/S_4\,,$$

given by composing the cross-ratio with the projection $\mathbb{P}^1 \to \mathbb{P}^1/S_4$, is invariant under the action of $\mathrm{PGL}_2 \times S_4$ on $(\mathbb{P}^1)^4$.

12.2 The j-function

In §12.1 we have seen that the permutations of four elements induce an action of $S_3 \cong S_4/V_4$ on $\mathbb{P}^1$ via the cross-ratio. Generically, we have seen that the orbit of λ has length six:

$$\left\{\lambda, \frac{1}{\lambda}, 1-\lambda, \frac{\lambda}{\lambda-1}, \frac{1}{1-\lambda}, \frac{\lambda-1}{\lambda}\right\}.$$

Nevertheless, some (non-trivial) elements of S_3 admit fixed points, making the orbits of these points shorter.

Lemma 12.2.1. *The non-trivial permutations in $S_3 \cong S_4/V_4$ have the following fixed points:*

$$\begin{aligned} (12): &\quad 1\,,\ -1\,; \\ (23): &\quad \infty\,,\ \frac{1}{2}\,; \\ (13): &\quad 0\,,\ 2\,; \\ (123),\ (132): &\quad \zeta_6\,,\ \zeta_6^5 = \bar{\zeta_6} = \zeta_6^{-1}\,; \end{aligned}$$

where $\zeta_6 = \frac{1+i\sqrt{3}}{2}$ is the primitive sixth root of unity.

These eight points are grouped into three orbits:

$$\{0, 1, \infty\}, \quad \{-1, 1/2, 2\}, \quad \{\zeta_6, \zeta_6^5\}.$$

Proof. By direct computations using Proposition 12.1.12. For example, we compute the fixed points of (12). We know that (12) sends λ to $1/\lambda$, hence its fixed points are the solutions to the equation

$$\lambda = 1/\lambda,$$

i.e., $\lambda = \pm 1$. All the other statements are proven in a similar way. □

The action of S_3 on $\mathbb{P}^1$ induces an action of S_3 on $\mathbb{C}(\lambda)$, by simply sending an element $f(\lambda)$ to $f(g(\lambda))$, for $g \in S_3$. Then it is interesting to find out what are the elements of $\mathbb{C}(\lambda)$ that are invariant under this action, that is, we want to compute $\mathbb{C}(\lambda)^{S_3}$. Clearly the polynomial

$$(x-\lambda)\cdot\left(x-\frac{1}{\lambda}\right)\cdot(x-(1-\lambda))\cdot\left(x-\frac{\lambda}{\lambda-1}\right)\cdot\left(x-\frac{1}{1-\lambda}\right)\cdot\left(x-\frac{\lambda-1}{\lambda}\right) \tag{12.2}$$

is invariant under S_3. It is easy to show that this polynomial is equal to the palyndromic polynomial

$$x^6 - 3x^5 - Ax^4 + Bx^3 - Ax^2 - 3x + 1,$$

with

$$A = \frac{(\lambda^2-\lambda+1)^3}{\lambda^2(\lambda-1)^2} - 6 \quad \text{and} \quad B = 2\cdot\frac{(\lambda^2-\lambda+1)^3}{\lambda^2(\lambda-1)^2} - 7.$$

This motivates the following definition.

Definition 12.2.2 (Klein)**.** The j-function is the function $j\colon \mathbb{P}^1 \to \mathbb{P}^1$ defined by sending λ to

$$j(\lambda) := 2^8 \cdot \frac{(\lambda^2-\lambda+1)^3}{\lambda^2(\lambda-1)^2}.$$

Theorem 12.2.3. $\mathbb{C}(\lambda)^{S_3} = \mathbb{C}(j)$.

Proof. By construction, we know that $j(\lambda)$ is S_3-invariant, hence

$$\mathbb{C}(j) \subseteq \mathbb{C}(\lambda)^{S_3} \subseteq \mathbb{C}(\lambda).$$

We are left to show that the reverse inclusion holds.

On the one hand, $\mathbb{C}(\lambda)/\mathbb{C}(\lambda)^{S_3}$ is a Galois extension of degree 6 and with Galois group S_3; on the other hand, λ satisfies the following algebraic relation of degree 6 over $\mathbb{C}(j)$:

$$2^8 \cdot (\lambda^2 - \lambda + 1)^3 - j \cdot \lambda^2(\lambda - 1)^2.$$

Because of the inclusion chain above, the statement follows. □

One can finally consider the composition of the cross-ratio with the j-function.

Theorem 12.2.4. *The map*

$$(\mathbb{P}^1)^4 \supset U \to \mathbb{P}^1,\ (z_1, z_2, z_3, z_4) \mapsto j((z_1, z_2; z_3, z_4))$$

is invariant under the action of $\mathrm{PGL}_2 \times S_4$ *on* U.

The fiber above $t \neq \infty$ *consists of exactly one orbit.*

The fiber above ∞ *consists of two orbits: the orbit of* $(0, 0, 1, \infty)$ *and the orbit of* $(0, 0, \infty, \infty)$.

Proof. By Proposition 12.1.9, the cross-ratio is invariant under the action PGL_2 on U; by Theorem 12.2.3 the j-function is invariant under the action of S_4, recalling that $S_3 = S_4/V_4$ and V_4 acts as the identity on the cross-ratio, cf. Proposition 12.1.12. This proves the first statement.

Let $(z_1, z_2, z_3, z_4), (x_1, x_2, x_3, x_4) \in U$ be two 4-tuples sent to $t \neq \infty$. If $t \neq \infty$, then $j^{-1}(t) \in \mathbb{P}^1 \setminus \{0, 1, \infty\}$. This means that $(x_1, x_2; x_3, x_4), (z_1, z_2; z_3, z_4) \in \mathbb{P}^1 \setminus \{0, 1, \infty\}$ and so, the two 4-tuples are of pairwise distinct points (cf. Exercise 1). As they are sent to the same j-invariant, their cross-ratios are in the same S_3-orbit. This means that, up to the action of S_3, we may assume that

$$(x_1, x_2; x_3, x_4) = (z_1, z_2; z_3, z_4).$$

By Proposition 12.1.10 we know that two 4-tuples of pairwise distinct points have the same cross-ratio if and only if they are in the same PGL_2-orbit, proving the second statement.

Finally, consider a 4-tuple (z_1, z_2, z_3, z_4) sent to ∞. As $j^{-1}(\infty) = \{0, 1, \infty\}$, we know that $(z_1, z_2; z_3, z_4) \in \{0, 1, \infty\}$. This implies that at least on point is repeated. If only one point is repeated, using the action of $\mathrm{PGL}_2 \times S_4$ we may assume that the 4-tuple is $(0, 0, 1, \infty)$ and let $\mathcal{O}$ denote its orbit. If two points are repeated, then we may assume that the 4-tuple is $(0, 0, \infty, \infty)$ and let $\mathcal{O}'$ denote its orbit. Hence the fiber over ∞ is the union $F = \mathcal{O} \cup \mathcal{O}'$. □

12.3 Elliptic curves as double covers of the projective line

In this subsection, we introduce the elliptic curves as covers of the projective line $\mathbb{P}^1$ ramified above four distinct points.

Definition 12.3.1. We define an *elliptic curve* to be the double cover of $\mathbb{P}^1$ ramified above four pairwise distinct points.

Let E, E' be the elliptic curves given as double covers of $\mathbb{P}^1$ ramified above the points z_1, z_2, z_3, z_4 and z_1', z_2', z_3', z_4' respectively. We say that E and E' are *isomorphic* if (z_1, z_2, z_3, z_4) and (z_1', z_2', z_3', z_4') are in the same $\mathrm{PGL}_2 \times S_4$-orbit.

Proposition 12.3.2. *Every elliptic curve is isomorphic to the projective closure of the plane curve defined by*

$$y^2 = x(x-1)(x-\lambda)$$

for some $\lambda \in \mathbb{C} \setminus \{0,1\}$.

In particular, if E *is the double cover of* $\mathbb{P}^1$ *ramified above* z_1, z_2, z_3, z_4, *then* $\lambda = (z_1, z_2; z_3, z_4)$.

Proof. Let E be an elliptic curve as defined in Definition 12.3.1. Then E is the double cover of $\mathbb{P}^1$ ramified above four points, say $z_1, z_2, z_3, z_4 \in \mathbb{P}^1$. By Corollary 12.1.11, there is an element of PGL_2 sending z_1, z_2, z_3, z_4 to $\lambda, 1, 0, \infty$, with $\lambda = (z_1, z_2; z_3, z_4)$. As the four points are pairwise distinct, $\lambda \in \mathbb{C} \setminus \{0,1\}$. The double cover of $\mathbb{P}^1$ ramified above $\lambda, 1, 0, \infty$ can be written as the projective curve

$$\overline{E}\colon Y^2Z = X(X-Z)(X-\lambda Z),$$

and the projection

$$\begin{aligned} \pi\colon \overline{E} &\to \mathbb{P}^1 \\ (x:y:1) &\mapsto (x:1) = x \\ (0:1:0) &\mapsto (1:0) = \infty. \end{aligned}$$

As the point $(0:1:0)$ is the only point with $Z = 0$, the map is well defined. It is easy to see that the map is generically 2-to-1 except above the points $\lambda, 1, 0, \infty$, proving the statement. □

Remark 12.3.3. The equation $y^2 = x(x-1)(x-\lambda)$ is called the *Legendre equation* of the elliptic curve E. See also Remark 5.2.4.

Using the j-function defined in §12.2, we can define the j-invariant of an elliptic curve. Indeed, if E is an elliptic curve, then E can be written as $E\colon y^2 = x(x-1)(x-\lambda)$.

Definition 12.3.4. We define the j-invariant of $E\colon y^2 = x(x-1)(x-\lambda)$ as the quantity

$$j(E) := 2^8 \cdot \frac{(\lambda^2 - \lambda + 1)^3}{\lambda^2(\lambda-1)^2}.$$

Remark 12.3.5. We can also define the *discriminant* of E as

$$\Delta(E) = 16\lambda^2(\lambda-1)^2.$$

Theorem 12.3.6. *Two elliptic curves are isomorphic if and only if they have the same* j*-invariant.*

Proof. Let E and E' be the elliptic curves given as double covers of $\mathbb{P}^1$ ramified above the points z_1, z_2, z_3, z_4 and z_1', z_2', z_3', z_4' respectively. This means that we can write

$$E\colon y^2 = x(x-1)(x-\lambda) \text{ and } E'\colon y^2 = x(x-1)(x-\lambda')$$

where λ and λ' are the cross-ratios of z_1, z_2, z_3, z_4 and z_1', z_2', z_3', z_4' respectively.

Assume that E and E' are isomorphic, i.e., there is an element of $\mathrm{PGL}_2 \times S_4$ sending z_1, z_2, z_3, z_4 to z_1', z_2', z_3', z_4'. This means that

$$\lambda' \in \left\{\lambda, \frac{1}{\lambda}, 1-\lambda, \frac{\lambda}{\lambda-1}, \frac{1}{1-\lambda}, \frac{\lambda-1}{\lambda}\right\},$$

i.e., λ' is in the S_4-orbit of λ. As the j-function is S_4-invariant, it follows that $j(E) = j(E')$.

Now assume $j(E) = j'(E)$. As the the four points are pairwise distinct, $j(E) = j'(E) = t \neq \infty$, and hence the two 4-tuples are in the same orbit of $\mathrm{PGL}_2 \times S_4$, cf. Theorem 12.2.4. □

12.4 From the Legendre to the Weierstrass equation

Let E be an elliptic curve given as the double cover of $\mathbb{P}^1$ ramified above four pairwise distinct points $z_1, z_2, z_3, z_4 \in \mathbb{P}^1$. Above we have seen that we can always assume that the four points are the points $\lambda, 1, 0, \infty$, with $\lambda = (z_1, z_2; z_3, z_4)$. Then E can be expressed as the curve defined by the equation

$$E\colon y^2 = x(x-1)(x-\lambda),$$

called the *Legendre equation* of E (cf. Remark 12.3.3). Nevertheless, in §5.1 we have seen that every elliptic curve can be also written as the curve defined by a cubic equation in Weiertrass form. In this subsection we see how to pass from the Legendre equation to the Weierstrass one, and vice-versa.

Proposition 12.4.1. *Consider the elliptic curve $E\colon y^2 = x(x-1)(x-\lambda)$. Then E has the following Weierstrass equation:*

$$y^2 = x^3 + ax + b,$$

where

$$a = -\frac{\lambda^2 - \lambda + 1}{3} \text{ and } b = -\frac{2\lambda^3 - 3\lambda^2 - 3\lambda + 2}{27}.$$

Conversely, if E is given by the Weierstrass equation $y^2 = x^3 + ax + b$, then it admits the following Legendre equation:

$$y^2 = x(x-1)(x-\lambda),$$

where $\lambda = (\alpha_1, \alpha_2; \alpha_3, \infty)$ and $\alpha_1, \alpha_2, \alpha_3$ are the complex roots of $x^3 + ax + b = 0$.

Example 12.4.2. To pass from the Legendre form to the Weierstrass one, just consider the transformation

$$\begin{cases} y' &= y \\ x' &= x - \frac{\lambda+1}{3} \end{cases},$$

then the statement follows.

Conversely, just notice that the $E : y^2 = x^3 + ax + b = (x-\alpha_1)(x-\alpha_2)(x-\alpha_3)$ is the double cover of $\mathbb{P}^1$ ramified above $\alpha_1, \alpha_2, \alpha_3, \infty$. Then the statement follows from Proposition 12.3.2.

Remark 12.4.3. It is easy to see that the definition of $\Delta(E)$ and $j(E)$ for the Weierstrass equation and the Legendre equation match if we pass from one to another.

12.5 Exercises

1. Show that if $(z_1, z_2, z_3, z_4) \in (\mathbb{P}^1_{\mathbb{C}})^4$ are pairwise distinct, then the cross-ratio $(z_1, z_2; z_3, z_4) \in \mathbb{P}^1_{\mathbb{C}}$ is different from $0, 1, \infty$.
2. Show that the points A, B, C, D and A', B', C', D' in Figure 12.1 have the same cross-ratio.
3. Compute the Legendre form of the double cover of $\mathbb{P}^1$ ramified above the points $\{1, 2, 3, 4\} \subset \mathbb{P}^1$.
4. Compute the following values of the j-function as defined in Definition 12.2.2: $j(0), j(1), j(-1), j(\infty), j(\zeta_6)$.
5. Give an example of two isomorphic elliptic curves with different Legendre form.
6. Given an elliptic curve in its Legendre form, transform it into a short Weierstrass form.

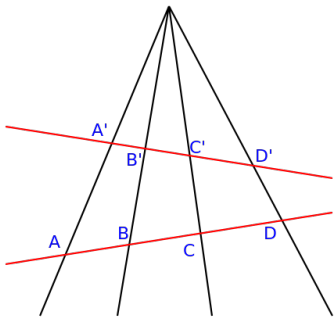


Figure 12.1

Bibliography

[1] B. J. Birch and H. P. F. Swinnerton-Dyer. Notes on elliptic curves. I. *J. Reine Angew. Math.*, 212:7–25, 1963.

[2] J. E. Cremona. *Algorithms for modular elliptic curves*. Cambridge University Press, Cambridge, second edition, 1997.

[3] D. J. H. Garling. *A course in Galois theory*. Cambridge University Press, Cambridge, 1986.

[4] R. Hartshorne. *Algebraic geometry*. Springer-Verlag, New York-Heidelberg, 1977. Graduate Texts in Mathematics, No. 52.

[5] N. Koblitz. *Introduction to elliptic curves and modular forms*, volume 97 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, second edition, 1993.

[6] S. Lang. *Algebra*, volume 211 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, third edition, 2002.

[7] M. Lehn. Modulformen. Notes for the master course, in German, 2020.

[8] J. H. Silverman. *Advanced topics in the arithmetic of elliptic curves*, volume 151 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1994.

[9] J. H. Silverman. *The arithmetic of elliptic curves*, volume 106 of *Graduate Texts in Mathematics*. Springer, Dordrecht, second edition, 2009.

[10] J. H. Silverman and J. T. Tate. *Rational points on elliptic curves*. Undergraduate Texts in Mathematics. Springer, Cham, second edition, 2015.

[11] P. Stevenhagen. Elliptic curves. Notes available at http://pub.math.leidenuniv.nl/~luijkrmvan/elliptic/2011/ec.pdf, 2008.

[12] J. Tate. Endomorphisms of Abelian varieties over finite fields. *Invent. Math.*, 2:134–144, 1966.

[13] Jacques Vélu. Isogénies entre courbes elliptiques. *C. R. Acad. Sci. Paris Sér. A-B*, 273:A238–A241, 1971.

[14] Lawrence C. Washington. *Elliptic curves*. Discrete Mathematics and its Applications (Boca Raton). Chapman & Hall/CRC, Boca Raton, FL, 2003. Number theory and cryptography.