The Weil Conjectures for Elliptic Curves

Matthew Dupraz

June 6, 2022

Contents

Introduction

In this paper, we will follow closely the structure of Silverman's *Arithmetic of Elliptic Curves* [Sil09] with the goal to state the Weil conjectures, and prove them for the case of elliptic curves, which are projective curves of genus 1. The Weil conjectures give some properties of the zeta function, which is a generating function derived from counting points on algebraic varieties over finite fields. In particular, one of the conjectures gives a link between the rank of homology groups of algebraic varieties defined over the complex numbers and the form of the zeta function of a related algebraic variety defined over a finite field. To make this link for the case of elliptic curves, in Section 3, we will for one calculate the zeta function for elliptic curves defined over finite fields, and then in Section 4, we will study the topological structure of elliptic curves defined over complex numbers.

We will start by defining all the necessary notions to be able to understand the Weil conjectures and then we will define important constructions that will be used in the proof of the Weil conjectures. Throughout this paper we assume known the content of the course *Algebraic Curves* given by Dimitri Wyss.

Whenever we talk about algebraic varieties defined over a field K, we will assume K is an algebraically closed field, unless stated otherwise. Furthermore, throughout this paper, we will assume that $\mathrm{char}(K) \notin \{2, 3\}$, as these cases lead to subtleties that go outside the scope of this paper.

1 Varieties and Curves

In this section we will introduce all the prerequisites to start studying elliptic curves and the Weil conjectures.

1.1 Algebraic Varieties

For the Weil conjectures we will be concerned with counting the number of points on an algebraic variety that have coordinates in some subfield of $L \subset K$. In order for this to make sense, the variety V in question has to be given by polynomials whose coefficients all lie in L, otherwise the notion of points belonging to L is not invariant by isomorphism. For example the curves defined over C given by the equations $y = x + a$ for a irrational are isomorphic to $\mathbb{A}^1$, but their sets of rational points (the sets of points which has coordinates lying in $\mathbb{Q}$) are different (one being the empty set, while the other being $\mathbb{Q} \subset \mathbb{A}^1$).

Definition 1.1. Let V be a algebraic variety. Let L be a subfield of K. We say that V is *defined over* L when the ideal of V can be generated by polynomials in $L[X]$. We will denote this by V/L.

A point whose coordinates belong to a certain subfield $L \subset K$ is called an L-rational point. The following definition makes this precise

Definition 1.2. Let $L \subseteq K$ a subfield. We define the set $\mathbb{A}^n(L) \subseteq \mathbb{A}^n$ as

$$\mathbb{A}^n(L) := \{(x_1, \dots, x_n) \in \mathbb{A}^n \mid x_i \in L\}.$$

We call this set the *set of L-rational* points of $\mathbb{A}^n$. Similarly, we define

$$\mathbb{P}^n(L) := \{[x_1, \dots, x_{n+1}] \in \mathbb{P}^n \mid x_i \in L\},$$

the set of L-rational points of $\mathbb{P}^n$.

For an algebraic variety defined over L, we can then talk about its L-rational points.

Definition 1.3. Let $L \subset K$ a subfield. Let V/L be an algebraic variety defined over L. We define the set of L-rational points of V

$$V(L) := \begin{cases} V \cap \mathbb{A}^n(L) & \text{if } V \text{ is affine;} \\ V \cap \mathbb{P}^n(L) & \text{if } V \text{ is projective.} \end{cases}$$

In this paper we will be primarily interested in *smooth* projective varieties. We will first define what this means for affine varieties and then extend the definition to projective varieties.

Definition 1.4. Let $V \subseteq \mathbb{A}^n$ be an affine variety, $P \in V$ and $f_1, \ldots, f_m \in K[X_1, \ldots, X_n]$ a set of generators of $I(V)$. Then V is *non-singular*, or *smooth* at P if the Jacobian of $(f_1, \ldots, f_m)$ at P has rank $n - \dim(V)$. In the other case we say P is a singular point of V. If V is non-singular at every point, then V is *non-singular*, or *smooth*.

We remind that projective space $\mathbb{P}^n$ can be covered by copies of $\mathbb{A}^n$. Define

$$U_i := \{[x_0, \ldots, x_n] \in \mathbb{P}^n \mid x_i \neq 0\},$$

then U_i is isomorphic to $\mathbb{A}^n$ via the chart

$$\phi_i : U_i \to \mathbb{A}^n, [x_0, \ldots, x_n] \mapsto \left(\frac{x_1}{x_i}, \ldots, \frac{x_{i-1}}{x_i}, \frac{x_{i+1}}{x_i}, \ldots, \frac{x_n}{x_i}\right)$$

Now we can define smoothness for projective varieties.

Definition 1.5. Let $V \subseteq \mathbb{P}^n$ be a projective variety, $P \in V$ and choose $U_i \subseteq \mathbb{P}^n$ such that $P \in U_i$. Then V is *non-singular*, or *smooth* at P if $V \cap U_i$ is smooth at P (as an affine variety).

Let us remind some important definitions from the course *Algebraic curves*.

Definition 1.6. Let $V \subset \mathbb{P}^n$ be a quasi-projective variety. A map $f : V \to K$ is regular at $P \in V$ if there exists some open neighbourhood $U \subset V$ of P and $g, h \in K[X_1, \ldots, X_{n+1}]$ homogeneous of the same degree such that $h(u) \neq 0$ and $f(u) = g(u)/h(u)$ for all $u \in U$.

The ring of regular functions on V is denoted $\mathcal{O}(V)$.

Definition 1.7. A morphism between two algebraic varieties V, W is a continuous map $\phi : V \to W$ such that for every open set $U \subset W$ and every $f \in \mathcal{O}(U)$, the map

$$f \circ \phi : \phi^{-1}(U) \to K$$

is regular.

We will make use of an equivalent definition of morphisms for projective varieties that is easier to manipulate in practice. First we define the notion of a rational map.

Definition 1.8. Let $V_1 \subseteq \mathbb{P}^n, V_2 \subseteq \mathbb{P}^m$ be projective varieties. A *rational map* from V_1 to V_2 is a map of the form

$$\begin{aligned} \phi : V_1 &\to V_2 \\ P &\mapsto [f_0(P), \ldots, f_m(P)], \end{aligned}$$

where $f_0, \ldots, f_m \in K(V_1)$ are such that for all $P \in V_1$ at which $f_0, \ldots, f_n$ are all defined, $\phi(P) \in V_2$.

We can now define the notion of regularity rational maps. Naively, we would like to say a rational map is regular at P if its constituent maps f_i are all regular at P. However the coordinates of points in projective space being all defined up to multiplication by a constant, we need to take that into account.

Definition 1.9. A rational map $\phi = [f_0, \dots, f_m] : V_1 \to V_2$ is *regular* at $P \in V_1$ if there is a function $g \in K(V_1)$, such that

(i) each gf_i is regular at P

(ii) for some i, $(gf_i)(P) \neq 0$

If such a g exists, we set

$$\phi(P) = [(gf_0)(P), \dots, (gf_m)(P)]$$

Finally, we get an equivalent definition of morphisms of projective varieties.

Proposition 1.10. *Let $\phi = [f_1, \dots, f_m] : V_1 \to V_2$ be a rational map. Then ϕ is regular at all $P \in V_1$ if and only if ϕ is a morphism.*

Proof. Suppose first that ϕ is a morphism, let $P \in V_1$. Choose i such that $\phi(P) \in U_i \subseteq V_2$, where $U_i = \{[x_0, \dots, x_m] \in \mathbb{P}^m \mid x_i \neq 0\}$. For each j, define the map

$$\begin{aligned} h_j : V_2 \cap U_i &\to K \\ [x_0, \dots, x_m] &\mapsto \frac{x_j}{x_i} \end{aligned}$$

By definition, $h_j \in \mathcal{O}(V_2 \cap U_i)$. Since ϕ is a morphism, we get that $h_j \circ \phi = \frac{f_j}{f_i} : \phi^{-1}(V_2 \cap U_i) \to K$ is regular. Setting $g = 1/f_i \in K(V_1)$, we get that gf_j is regular at P for all j and $gf_i = 1 \neq 0$. Hence ϕ is regular at P.

For the other implication, suppose ϕ is regular at all $P \in V_1$. Let $W \subseteq V_2$ open and $f \in \mathcal{O}(W)$, we have to show that $f \circ \phi : \phi^{-1}(W) \to K$ is regular. Let $P \in \phi^{-1}(W)$, then since ϕ is regular at P, there exists $g \in K(V_1)$ such that each gf_i is regular at P and for some i, $(gf_i)(P) \neq 0$. Since f is regular at $\phi(P)$, there exist polynomials $p, q \in K[x_0, \dots, x_n]$ homogeneous of the same degree with $q(\phi(P)) \neq 0$ and $f(Q) = \frac{p(Q)}{q(Q)}$ for all $Q \in W \setminus q^{-1}(0)$. Then

$$f \circ \phi = \frac{p(f_0, \dots, f_m)}{q(f_0, \dots f_m)} = \frac{p(gf_0, \dots, gf_m)}{q(gf_0, \dots, gf_m)}$$

We have that both $p(gf_0, \dots, gf_m)$ and $q(gf_0, \dots, gf_m)$ are regular. Furthermore, $q(gf_0, \dots, gf_m)(P) \neq 0$, since we supposed $q(\phi(P)) \neq 0$. and hence we deduce that $f \circ \phi$ is regular. This implies that ϕ is a morphism. $\square$

1.2 Projective Curves

Through most of this paper we will be looking at projective curves, which are projective varieties of dimension one. Recall that for a projective variety V, its dimension dimension is given by

$$\dim V = \dim V \cap U_i = \dim(\Gamma(V \cap U_i))$$

where $U_i = \{X_i \neq 0\} \subset \mathbb{P}^n$ is such that $U_i \cap V \neq \emptyset$. Hence V is an projective curve iff the coordinate ring of $V \cap U_i$ is of Krull dimension 1, i.e. every non-zero prime ideal is maximal.

By a *curve* we will always mean a *projective* curve, unless stated otherwise.

Proposition 1.11. *Let C be a curve and $P \in C$ a smooth point. Then $\mathcal{O}_P(C)$ is a discrete valuation ring.*

Proof. The case of plane curves was proven in the course *Algebraic curves* (Corollary 4.4). For a full proof see [Har77, I.5.1] and [AM69, 9.2]. □

Since $\mathcal{O}_P(C)$ is a DVR we can use its valuation to define the notion of order of functions on C. Recall that $K(C) = \mathrm{Frac}(\mathcal{O}_P(C))$ for any $P \in C$.

Definition 1.12. Let C be a curve and $P \in C$ a smooth point. The *valuation* on $\mathcal{O}_P(C)$ is given by

$$\begin{aligned} \mathrm{ord}_P : \mathcal{O}_P(C) &\to \mathbb{N} \cup \{\infty\} \\ f &\mapsto \max\{d \in \mathbb{N} \mid f \in \mathfrak{m}_P^d\}. \end{aligned}$$

where $\mathfrak{m}_P$ is the maximal ideal of $\mathcal{O}_P(C)$. We extend this definition to $K(C)$ using

$$\begin{aligned} \mathrm{ord}_P : K(C) &\to \mathbb{Z} \cup \{\infty\} \\ f/g &\mapsto \mathrm{ord}_P(f) - \mathrm{ord}_P(g). \end{aligned}$$

For $f \in K(C)$, we call $\mathrm{ord}_P(f)$ the order of f at P. If $\mathrm{ord}_P(f) > 0$, then f has a *zero* at P, if $\mathrm{ord}_P(f) < 0$, then f has a *pole* at P, if $\mathrm{ord}_P(f) \geq 0$, then f is *regular* at P.

A *uniformizer* for C at P is a function $t \in K(C)$ with $\mathrm{ord}_P(t) = 1$ (so a generator of $\mathfrak{m}_P$)

Thanks $O_P(C)$ being a DVR, we have that smooth projective curves have a really nice structure. For example, we can deduce that all rational maps between a curve and another variety are regular wherever the curve is smooth.

Proposition 1.13. *Let C be a curve, $V \subseteq \mathbb{P}^n$ a variety, $P \in C$ a smooth point, and $\phi : C \to V$ a rational map. Then ϕ is regular at P. In particular, if C is smooth, then ϕ is a morphism.*

Proof. Write $\phi = [f_0, \dots f_n]$ with $f_i \in K(C)$ and choose an uniformizer $t \in K(C)$ for C at P. Let

$$n = \min_{0 \le i \le n} \{\operatorname{ord}_P f_i\}$$

Then $\operatorname{ord}_P(t^{-n} f_i) \ge 0$ for all i and $\operatorname{ord}_P(t^{-n} f_j) = 0$ for some j. Hence each $t^{-n} f_i$ is regular at P and $(t^{-n} f_j)(P) \ne 0$. So ϕ is regular at P. □

We also get the following theorem, which is the projective counterpart of a similar theorem for compact Riemann surfaces.

Theorem 1.14. *Let $\phi : C_1 \to C_2$ be a morphism of curves. Then ϕ is either constant or surjective.*

Proof. Admitted. See [Har77, II.6.8]. □

Corollary 1.14.1. *Let C be a smooth curve and $f \in K(C)$. Then if f has no poles, $f \in K$.*

Proof. We have that f induces a rational map

$$\begin{aligned} [f, 1] : C &\to \mathbb{P}^1 \\ P &\mapsto [f(P), 1] \end{aligned}$$

By 1.13, $[f, 1]$ is a morphism and so by 1.14, we have that $[f, 1]$ is either constant or surjective. If $[f, 1]$ is constant, f is constant and so $f \in K$. Else $[f, 1]$ is surjective, so there is some $P \in C$ such that $[f, 1](P) = [1, 0]$, but then P is a pole of f. □

Proposition 1.15. *Let C be a smooth curve and $f \in K(C)^\times$. Then there are only finitely many points of C at which f has a pole or a zero.*

Proof. We have that $[f, 1] : C \to \mathbb{P}^1$ is a morphism, hence continuous. It follows that $f^{-1}(0) = [f, 1]^{-1}([0, 1])$ is a closed subset of C. Since $f \ne 0$, we have that $f^{-1}(0) \ne C$. Let $U_i = \{X_i \ne 0\} \subset \mathbb{P}^n$ for any i. $f^{-1}(0) \cap U_i \subset \mathbb{A}^n$ being closed, it can be written as a finite union of irreducible algebraic sets in $C \cap U_i \subset \mathbb{A}^n$. $C \cap U_i$ being of dimension 1, the only irreducible algebraic sets strictly included in $C \cap U_i$ are singletons, hence $f^{-1}(0) \cap U_i$ is a finite set. Furthermore, $\mathbb{P}^n$ can be covered by U_i for $i \in \{0, \dots, n\}$. This shows f has a finite amount of zeros.

f having a finite number of poles follows from the fact that $1/f$ has a finite number of zeros. □

Recall that a rational map $\phi : C_1 \to C_2$ induces a map fixing K

$$\begin{aligned} \phi^* : K(C_2) &\to K(C_1) \\ f &\mapsto f \circ \phi. \end{aligned}$$

We call this map the *pullback*.

By the above theorem, if ϕ is not constant, then it is surjective and hence ϕ^* is an injection. One can show that $K(C_1)/\phi^* K(C_2)$ is a finite extension (see [Har77, II.6.8]). It follows that we can consider the norm on this extension. We can see $K(C_1)$ as a $\phi^* K(C_2)$-vector space in which case elements of $K(C_1)$ act on $K(C_1)$ via multiplication, which is a $\phi^* K(C_2)$-linear transformation. The norm $N_{K(C_1)/\phi^* K(C_2)}(f)$ of an element $f \in K(C_1)$ is then defined to be the determinant of this $\phi^* K(C_2)$-linear transformation. By definition, $N_{K(C_1)/\phi^* K(C_2)}(f) \in \phi^* K(C_2)$, and so by injectivity of ϕ^*, we can take the inverse

$$\phi_*(f) := (\phi^*)^{-1} \circ N_{K(C_1)/\phi^* K(C_2)}(f).$$

This defines a map of function fields, which we call the *pushforward*.

$$\phi_* : K(C_1) \to K(C_2).$$

We can also consider the degree the extension $K(C_1)/\phi^* K(C_2)$, which will define the degree of a map of curves.

Definition 1.16. Let $\phi : C_1 \to C_2$ be a map of curves defined over K. If ϕ is constant, we define the *degree* of ϕ to be 0. Otherwise we define the degree of ϕ by

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

Let S be the separable closure of $\phi^* K(C_2)$ inside $K(C_1)$. We define the *separable degree* of ϕ to be

$$\deg_s \phi = [S : \phi^* K(C_2)],$$

and the *inseparable degree*

$$\deg_i \phi = [K(C_1) : S].$$

The following proposition shows that for any injection of function fields $K(C_2) \to K(C_1)$ which fixes K, we can find a (unique) map of curves $C_1 \to C_2$, such that its pullback is this injection.

Proposition 1.17. *Let C_1, C_2 be curves and let $\iota : K(C_2) \to K(C_1)$ be an injection of function fields fixing K. Then there exists a unique non-constant map $\phi : C_1 \to C_2$ such that $\phi^* = \iota$.*

Proof. Assume $C_2 \subset \mathbb{P}^n$ and $C_2 \not\subset \{[X_0, \ldots, X_n] \in \mathbb{P}^n \mid X_0 = 0\}$ (we can relabel the X_i's if necessary). Let $g_i \in K(C_2)$ defined by

$$g_i(X_0, \ldots, X_n) = X_i / X_0.$$

Then define $\phi : C_1 \to C_2$ by

$$\phi = [1, \iota(g_1), \ldots, \iota(g_n)].$$

We then have that

$$\phi^*(g_i) = g_i\left([1, \iota(g_1), \ldots, \iota(g_n)]\right) = \iota(g_i)/1 = \iota(g_i)$$

Since $K(C_2) = K(g_1, \ldots, g_n)$, we deduce $\phi^* = \iota$.

Suppose there is some other map $\psi = [f_0, \ldots, f_n] : C_1 \to C_2$ such that $\psi^* = \iota$. Then for each i,

$$f_i/f_0 = \psi^*(g_i) = \iota(g_i),$$

which shows

$$\psi = [1, f_1/f_0, \ldots, f_n/f_0] = [1, \iota(g_1), \ldots, \iota(g_n)] = \phi.$$

□

We also get the following useful corollary.

Corollary 1.17.1. *Let C_1 and C_2 be smooth curves, and let $\phi : C_1 \to C_2$ be a map of degree 1. Then ϕ is an isomorphism.*

Proof. By definition we have that if $\deg \phi = 1$, then $\phi^* K(C_2) = K(C_1)$, hence ϕ^* is an isomorhism of function fields. In particular, from 1.17 applied to $(\phi^*)^{-1} : K(C_1) \to K(C_2)$, we get the existence of $\psi : C_2 \to C_1$, such that $\psi^* = (\phi^*)^{-1}$. Since C_2 is smooth, ψ is a morphism by 1.13. Since $(\phi \circ \psi)^* = \psi^* \circ \phi^* = \mathrm{id}^*_{C_2}$ and $(\psi \circ \phi)^* = \phi^* \circ \psi^* = \mathrm{id}^*_{C_1}$, it follows by the unicity part of 1.17 that $\phi \circ \psi = \mathrm{id}_{C_2}$ and $\psi \circ \phi = \mathrm{id}_{C_1}$, and hence ϕ is an isomorphism. □

Now, suppose we have a non-constant map of smooth curves $\phi : C_1 \to C_2$, then we might expect the preimage of any point Q by this map to be of cardinality $\deg \phi$. However, this is not always the case. If we imagine ϕ as a cover with $\deg \phi$ sheets, it could happen that some sheets intersect above some point $Q \in C_2$ in which case $\#\phi^{-1}(Q) < \deg \phi$. The ramification index measures the extent to which this happens.

Definition 1.18. Let $\phi : C_1 \to C_2$ be a non-constant map of smooth curves, and let $P \in C_1$. The *ramification index* of ϕ at P, denoted $e_\phi(P)$, is given by

$$e_\phi(P) = \mathrm{ord}_P(\phi^* t_{\phi(P)})$$

where $t_{\phi(P)} \in K(C_2)$ is a uniformizer at $\phi(P)$. We say that ϕ is *unramified* at P if $e_\phi(P) = 1$. ϕ is *unramified* if it is unramified at every point C_1.

The following proposition will make sense of the intuition we gave above.

Proposition 1.19. *Let $\phi : C_1 \to C_2$ be a non-constant map of smooth curves.*

(a) For every $Q \in C_2$,

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

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

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

(c) Let $\psi : C_2 \to C_3$ be another non-constant map. Then for all $P \in C_1$,

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

Proof. Admitted. See [Sil09, II.2.6]. □

In particular, if ϕ is separable, then for all but finitely many $Q \in C_2$, we get that $\#\phi^{-1}(Q) = \deg(\phi)$. Intuitively this means that the sheets of the cover ϕ intersect at a finite amount of points. This already hints at the fact that separability is a very important property of maps between smooth curves, as it will allow us to count points in the maps' preimages.

Next, we will define the so-called Frobenius morphism. This morphism is going to play a central role in the proof of the Weil conjectures for elliptic curves, as it will allow us to count the number of points of the curve that lie over some finite field.

Definition 1.20. Suppose $\mathrm{char}(K) = p \neq 0$ and let $q = p^r$. For any polynomial $f \in K[X]$ define $f^{(q)}$ to be the polynomial obtained from f by raising each coefficient of f to the q^{th} power. For any curve C/K we can define a new curve $C^{(q)}/K$ corresponding to the ideal generated by $\{f^{(q)} : f \in I(C)\}$.

The q^{th}-*power Frobenius morphism* is defined by

$$\begin{aligned} \phi : C &\to C^{(q)} \\ [x_0, \ldots, x_n] &\mapsto [x_0^q, \ldots, x_n^q] \end{aligned}$$

This map is well defined as for any $P = [x_0, \ldots, x_n] \in C$, and for any generator $f^{(q)}$ of $I(C^{(q)})$,

$$\begin{aligned} f^{(q)}(\phi(P)) &= f^{(q)}(x_0^q, \ldots, x_n^q) \\ &= (f(x_0, \ldots, x_n))^q && \text{since } \mathrm{char}(K) = p \\ &= (f(P))^q = 0 \end{aligned}$$

Notice that if C is defined over $\mathbb{F}_q \subset K$, then $C^{(q)} = C$, and ϕ becomes and endomorphism.

In the case where C is defined over $\mathbb{F}_q$, the Frobenius map ϕ_q gives us a way to find $C(\mathbb{F}_q)$. Indeed, the q^{th} power map on $\overline{\mathbb{F}_q}$ fixes exactly $\mathbb{F}_q$ (see course on Rings and Fields), hence we see that the set of fixed points of ϕ_q is exactly $C(\mathbb{F}_q)$ This will play an important role in computing $\#C(\mathbb{F}_q)$.

1.3 Divisors

We will now define so-called divisors. These give us a practical way to talk about zeroes and poles of functions and will be very useful when defining a group structure on elliptic curves.

Definition 1.21. The *divisor group of a curve* C, denoted $\mathrm{Div}(C)$ is the free abelian group generated by the points of C. We write $D \in \mathrm{Div}(C)$ as the formal sum

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

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

The *degree* of D is defined by

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

The *divisors of degree* 0 form a subgroup of $\mathrm{Div}(C)$, which we denote by

$$\mathrm{Div}^0(C) = \{D \in \mathrm{Div}(C) \mid \deg D = 0\}.$$

We can associate to each function $f \in K(C)^\times$ a divisor, which carries the information about the order of zeros and poles of f.

Definition 1.22. Let C be a smooth curve and $f \in K(C) \setminus \{0\}$. We associate to f the divisor $\mathrm{div}(f)$ given by

$$\mathrm{div}(f) = \sum_{P \in C} \mathrm{ord}_P(f) \cdot (P)$$

Proposition 1.15 guarantees that this is well defined.

Remark. Since each ord_P is a valuation, the map

$$\mathrm{div} : K(C)^\times \to \mathrm{Div}(C)$$

is a homomorphism of abelian groups.

In fact, as we will soon see, not all divisors correspond to functions in this way. The divisors that do form a subgroup.

Definition 1.23. A divisor $D \in \mathrm{Div}(C)$ is *principal* if it has the form $D = \mathrm{div}(f)$ for some $f \in K(C)$. The subgroup of principal divisors is denoted $\mathrm{PDiv}(C)$. Two divisors D_1, D_2 are *linearly equivalent*, which we denote $D_1 \sim D_2$, if $D_1 - D_2$ is principal.

In a way analogous to how a map between smooth curves $\phi : C_1 \to C_2$ induces maps on function fields

$$\phi_* : K(C_1) \to K(C_2) \qquad \text{and} \qquad \phi^* : K(C_2) \to K(C_1),$$

we can define maps between divisor groups.

Definition 1.24. Let $\phi : C_1 \to C_2$ be a non-constant between smooth curves. Then ϕ induces maps between the divisor groups of C_1 and C_2. The *pullback* is defined by

$$\begin{aligned} \phi^* : \mathrm{Div}(C_2) &\to \mathrm{Div}(C_1) \\ (Q) &\mapsto \sum_{P \in \phi^{-1}(Q)} e_\phi(P) \cdot (P). \end{aligned}$$

The *pushforward* is defined by

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

These maps have many useful properties, as the following proposition shows.

Proposition 1.25. *Let $\phi : C_1 \to C_2$ be a non-constant map of smooth curves.*

(a) $\deg(\phi^* D) = (\deg \phi)(\deg D)$ *for all* $D \in \mathrm{Div}(C_2)$.

(b) $\phi^*(\mathrm{div}\, f) = \mathrm{div}(\phi^* f)$ *for all* $f \in K(C_2)^\times$.

(c) $\deg(\phi_* D) = \deg(D)$ *for all* $D \in \mathrm{Div}(C_1)$.

(d) $\phi_*(\mathrm{div}\, f) = \mathrm{div}(\phi_* f)$ *for all* $f \in K(C_1)^\times$

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

(f) If $\psi : C_2 \to C_3$ *is another such map, then*

$$(\psi \circ \phi)^* = \phi^* \circ \psi^* \qquad \textit{and} \qquad (\psi \circ \phi)_* = \phi_* \circ \psi_*$$

Proof. (a) We have that if $D = \sum n_Q (Q)$,

$$\phi^* D = \sum_{Q \in C_2} n_Q \sum_{P \in \phi^{-1}(Q)} e_\phi(P) \cdot (P).$$

From 1.19(a) it follows that

$$\deg(\phi^* D) = \sum_{Q \in C_2} n_Q \deg(\phi) = \deg(D) \deg(\phi).$$

(b) Let $P \in C_1$, and let $t_{\phi(P)}$ be an uniformizer at $\phi(P)$. Then let $k = \operatorname{ord}_{\phi(P)}(f)$, we have that $f = t_{\phi(P)}^k g$ for some g of order 0 at $\phi(P)$. It follows that

$$\begin{aligned}\operatorname{ord}_P(\phi^* f) &= \operatorname{ord}_P((\phi^* t_{\phi(P)})^k(\phi^* g)) \\ &= \operatorname{ord}_P(\phi^* t_{\phi(P)}) \cdot k + \operatorname{ord}_P(\phi^* g) \\ &= e_\phi(P) \operatorname{ord}_{\phi(P)}(f),\end{aligned}$$

since $\phi^* g$ is regular at P, since ϕ is a morphism. Then we get

$$\begin{aligned}\operatorname{div}(\phi^* f) &= \sum_{P \in C_1} \operatorname{ord}_P(\phi^* f) \cdot (P) \\ &= \sum_{P \in C_1} e_\phi(P) \operatorname{ord}_{\phi(P)}(f) \cdot (P) \\ &= \sum_{Q \in C_2} \sum_{P \in \phi^{-1}(Q)} e_\phi(P) \operatorname{ord}_Q(f) \cdot (P) \\ &= \phi^*(\operatorname{div} f).\end{aligned}$$

(c) Clear from the definition of ϕ_*.

(d) Admitted. See [Sil09, II.3.6(d)].

(e) For all $Q \in C_2$, using 1.19(a),

$$\begin{aligned}\phi_* \circ \phi^*((Q)) &= \phi_* \left(\sum_{P \in \phi^{-1}(Q)} e_\phi(P) \cdot (P) \right) \\ &= \sum_{P \in \phi^{-1}(Q)} e_\phi(P) \cdot (Q) \\ &= \deg(\phi) \cdot (Q).\end{aligned}$$

(f) Let $R \in C_3$, then using 1.19(c),

$$\begin{aligned}(\psi \circ \phi)^*(R) &= \sum_{P \in (\psi\circ\phi)^{-1}} e_{\psi\circ\phi}(P) \cdot (P) \\ &= \sum_{P \in (\psi\circ\phi)^{-1}} e_\phi(P) e_\psi(\phi(P)) \cdot (P) \\ &= \sum_{Q \in \psi^{-1}(R)} \sum_{P \in \phi^{-1}(Q)} e_\phi(P) e_\psi(Q) \cdot (P) \\ &= \phi^* \circ \psi^*(R).\end{aligned}$$

The second equality follows clearly from definition.

□

Thanks to these properties, we can show that principal divisors have degree 0, making $\operatorname{PDiv}(C)$ a subgroup of $\operatorname{Div}^0(C)$.

Proposition 1.26. *Let $D \in \operatorname{Div}(C)$ be a principal divisor, then* $\deg D = 0$.

Proof. Let $f \in K(C)^\times$ such that $D = \operatorname{div} f$. It follows from the definition of div and 1.25(a) that

$$\deg \operatorname{div}(f) = \deg([f,1]^*((0) - (\infty))) = \deg([f,1]) \deg((0) - (\infty)) = 0.$$

The first equality comes from the fact

$$\begin{aligned}
[f,1]^*((0) - (\infty)) &= \sum_{P \in [f,1]^{-1}(0)} e_{[f,1]}(P) - \sum_{P \in [f,1]^{-1}(\infty)} e_{[f,1]}(P) \\
&= \sum_{P \in [f,1]^{-1}(0)} \operatorname{ord}_P(f) - \sum_{P \in [f,1]^{-1}(\infty)} \operatorname{ord}_P(1/f) \\
&= \operatorname{div}(f)
\end{aligned}$$

Hence $\deg D = 0$ □

We now define the notion of divisor class group. Essentially, we identify linearly equivalent divisors. This will come in handy as it will allow us to define a group law on elliptic curves.

Definition 1.27. The *divisor class group* of a curve C, denoted $\operatorname{Cl}(C)$, is the quotient $\operatorname{Div}(C)/\operatorname{PDiv}(C)$. Principal divisors have degree 0 and hence it makes sense to speak about the degree of elements in $\operatorname{Cl}(C)$. The sugroup of elements of $\operatorname{Cl}(C)$ of degree 0 is denoted $\operatorname{Cl}^0(C)$.

Remark. By 1.25, for $\phi : C_1 \to C_2$ a non-constant map of smooth curves, ϕ_* and ϕ^* take degree 0 divisors to degree 0 divisors and principal divisors to principal divisors. In particular, they induce the maps

$$\phi^* : \operatorname{Cl}^0(C_2) \to \operatorname{Cl}^0(C_1) \qquad \text{and} \qquad \phi_* : \operatorname{Cl}^0(C_1) \to \operatorname{Cl}^0(C_2)$$

Divisor allow us to express certain conditions on the zeroes and poles of a function. To do this we define a partial order on $\operatorname{Div}(C)$, which will allow us to compare divisors.

Definition 1.28. A divisor $D = \sum n_P(P) \in \operatorname{Div}(C)$ is *positive* (or *effective*), denoted by $D \geq 0$, if $n_P \geq 0$ for all $P \in C$. For two divisors $D_1, D_2 \in \operatorname{Div}(C)$, we write $D_1 \geq D_2$ to indicate that $D_1 - D_2$ is positive.

We may for example demand that a function f has poles of order less than n_P at $P \in E$. We can encode this information in a divisor $D = \sum n_P(P)$, which allows us to express this condition neatly as $\operatorname{div}(f) \geq -D$. In fact, we have a notation for the set of functions that satisfy such a condition.

Definition 1.29. Let $D \in \mathrm{Div}(C)$. We associate to D the set of functions

$$\mathcal{L}(D) = \{f \in K(C)^\times : \mathrm{div}(f) \geq -D\} \cup \{0\}.$$

It can be shown $\mathcal{L}(D)$ is a finite-dimensional K-vector space. We denote its dimension by

$$l(D) = \dim_K \mathcal{L}(D).$$

Proposition 1.30. *If* $\deg D < 0$*, then* $\mathcal{L}(D) = \{0\}$ *and* $l(D) = 0$*.*

Proof. Suppose ad absurdum there is some $f \in \mathcal{L}(D) \setminus \{0\}$. Then $\mathrm{div}\, f \geq -D$ and so in particular

$$0 = \deg \mathrm{div}\, f \geq \deg(-D) = -\deg D > 0,$$

but this is absurd. $\square$

1.4 Differentials

In this section we introduce the notion of differential forms on a curve. This will allow us to state the Riemann-Roch theorem and define the genus of a curve. Furthermore, differentials turn out to be very useful for determining when map between curves is separable. For the goals of this paper, it will suffice to gloss over the main definitions and properties without providing proofs.

Definition 1.31. Let C be a curve. The *space of (meromorphic)* differential forms on C, denoted Ω_C, is the $K(C)$-vector space generated by symbols of the form *df* for $f \in K(C)$, subject to the following relations:

1. $d(x + y) = dx + dy$
2. $d(xy) = x\, dy + y\, dx$
3. $da = 0$

for all $x, y \in K(C)$ and $a \in K$.

A non-constant map of curves $\phi : C_1 \to C_2$ (again) induces a map on the spaces of differential forms.

Definition 1.32. Let $\phi : C_1 \to C_2$ be a non-constant map of curves. Then ϕ induces maps between the spaces of meromorphic forms of C_1 and C_2. The *pullback* is defined by

$$\begin{aligned} \phi^* : \Omega_{C_2} &\to \Omega_{C_1} \\ f\, dx &\mapsto (\phi^* f)\, d(\phi^* x). \end{aligned}$$

Since a curve is one-dimensional, we might expect its space of differential forms to also be one-dimensional. And indeed, that is the case.

Proposition 1.33. *Let C be a curve, then Ω_C is a 1-dimensional $K(C)$-vector space. Furthermore, if $t \in K(C)$ is a uniformizer at P, then dt generates Ω_C.*

Proof. See [Sil09, II.1.4, II.4.2]. □

This gives us a correspondence between differential forms and functions on C.

Notation. Let $\omega \in \Omega_C$. Then by 1.33 there exists $g \in K(C)$ such that $\omega = g\,dt$. We denote g by ω/dt.

Using this identification, we may define the order of a differntial. A priori this may depend on the choice of uniformizer, but the following proposition says that's not the case.

Proposition 1.34. *Let $P \in C$ and $t \in K(C)$ a uniformizer at P. For $\omega \in \Omega_C$, the quantity*

$$\mathrm{ord}_P(\omega/dt)$$

is independent of the choice of uniformizer t.

Proof. See [Sil09, II.4.3(c)]. □

Definition 1.35. We call $\mathrm{ord}_P(\omega/dt)$ the order of ω at P and denote it by $\mathrm{ord}_P(\omega)$.

Notice that if $t \in K(C)$ is a uniformizer at $P \in C$, then $\mathrm{ord}_P(dt) = \mathrm{ord}_P(dt/dt) = \mathrm{ord}_P(1) = 0$ by definition.

Proposition 1.36. *For all but finitely many $P \in \mathbb{C}$,*

$$\mathrm{ord}_P(\omega) = 0.$$

Proof. See [Sil09, II.4.3(e)]. □

This proposition guarantees that the divisor of a differential is well defined.

Definition 1.37. Let $\omega \in \Omega_C$. The divisor associated to ω is

$$\mathrm{div}(\omega) = \sum_{P \in C} \mathrm{ord}_P(\omega) \cdot (P) \in \mathrm{Div}(C)$$

Definition 1.38. A differential $\omega \in \Omega_C$ is *regular* (or *holomorphic*) if for all $P \in C$,

$$\mathrm{ord}_P(\omega) \geq 0.$$

If is *non-vanishing* if for all $P \in C$,

$$\mathrm{ord}_P(\omega) \leq 0.$$

The case of $\mathbb{P}^1$ is an important example.

Example 1.39. Let $t : \mathbb{P}^1 \to K, [X, Y] \mapsto X/Y$ be the coordinate function on $\mathbb{P}^1$. Then $t - \alpha$ is an uniformizer at $[\alpha, 1]$. It follows that

$$\mathrm{ord}_{[\alpha,1]}(dt) = \mathrm{ord}_{[\alpha,1]}(d(t - \alpha)) = 0.$$

At $\infty = [1, 0] \in \mathbb{P}^1$, we have that $1/t$ is a uniformizer. Furthermore,

$$0 = d(1) = d(t/t) = 1/t \cdot dt + td(1/t)$$

and hence $dt = -t^2 d(1/t)$. It follows that

$$\mathrm{ord}_\infty(dt) = \mathrm{ord}_\infty(-t^2 d(1/t)) = \mathrm{ord}_\infty(-t^2) = -2$$

Hence we obtain $\mathrm{div}(dt) = -2(\infty)$ and hence dt is not holomorphic. But for any non-zero $\omega \in \Omega_{\mathbb{P}^1}$, we have that there exists some $g \in K(\mathbb{P}^1)$ such that $\omega = gdt$, but then for all $P \in \mathbb{P}^1$, and u a uniformizer at P,

$$\mathrm{ord}_P(\omega) = \mathrm{ord}_P\left(g\frac{dt}{du}\right) = \mathrm{ord}_P(g) + \mathrm{ord}_P\left(\frac{dt}{du}\right) = \mathrm{ord}_P(g) + \mathrm{ord}_P(dt).$$

It follows that

$$\deg \mathrm{div}\, \omega = \deg(\mathrm{div}(g) + \mathrm{div}(dt)) = -2$$

so ω is not holomorphic either. Hence there are no non-zero holomorphic differentials on $\mathbb{P}^1$.

Now, if ω_1 and $\omega_2 \in \Omega_C$ are non-zero differentials, then there exists $f \in K(C)^\times$ such that $\omega_1 = f\omega_2$. This implies that

$$\mathrm{div}(\omega_1) = \mathrm{div}(f) + \mathrm{div}(\omega_2).$$

It follows that the divisors of all differentials are in the same class in $\mathrm{Cl}(C)$ and so the following definition makes sense.

Definition 1.40. The *canonical divisor class* on C is the image in $\mathrm{Cl}(C)$ of $\mathrm{div}(\omega)$ for any non-zero differential $\omega \in \Omega_C$. Any divisor in this class is called a *canonical divisor.*

1.5 Genus of a Curve and the Riemann-Roch Theorem

We can finally define what the genus of a curve is.

Definition 1.41. Let C be a curve, let K_C be a canonical divisor, the *genus* of C is defined to be $\dim_K \mathcal{L}(K_C) = l(K_C)$.

Example 1.42. The projective line $\mathbb{P}^1$ has genus 0. Let $K_C = \operatorname{div}(\omega)$ be a canonical divisor of $\mathbb{P}^1$. By 1.39, $\deg(K_C) = -2 < 0$. In particular, since $\deg \operatorname{div} f = 0$ for all $f \in K(C)^\times$, $\operatorname{div} f \not\geq -K_C$, so $f \notin \mathcal{L}(K_C)$. It follows that $\mathcal{L}(K_C) = \{0\}$ and hence $l(K_C) = 0$.

The genus is an important invariant of algebraic curves. For example, we have the Riemann-Roch theorem, which will allow us to calculate $l(D)$ for any divisor D if we know the genus of the curve. This will be very useful, as it will allow us to show that elliptic curves, which are by definition smooth curves of genus 1, are isomorphic to plane curves given by a specific cubic equation.

Theorem 1.43 (Riemann-Roch)**.** *Let C be a smooth curve of genus g and K_C a canonical divisor on C. Then for every divisor $D \in \operatorname{Div}(C)$,*

$$l(D) - l(K_C - D) = \deg D - g + 1.$$

Proof. Admitted. See [Har77, IV.1.3] □

We get also the following corollary, part (b) being especially useful because it will allow us to avoid working with canonical divisors.

Corollary 1.43.1. *In the same setup as the Riemann-Roch theorem, we have the following properties*

(a) $\deg K_C = 2g - 2$.

(b) If $\deg(D) > 2g - 2$, *we have that*

$$l(D) = \deg(D) - g + 1$$

Proof. (a) From definition, $l(K_C) = g$, so for $D = K_C$ and using $l(0) = 1$, since $\mathcal{L}(0) = 0$ by 1.14.1, we get the result using 1.43.

(b) From (a), we have that $\deg(K_C - D) < 0$. From 1.30, we have that $l(K_C - D) = 0$ and so from 1.43, the result follows.

□

For example, we get that for curves of genus 1, if $\deg(D) > 0$, then $l(D) = \deg(D)$, from which we can deduce many useful properties, such as the following.

Proposition 1.44. *Let C be a curve of genus 1, and let $P, Q \in C$. Then*

$$(P) \sim (Q) \quad \textit{if and only if} \quad P = Q$$

Proof. Suppose $(P) \sim (Q)$, then there exists some $f \in K(C)$ such that

$$\operatorname{div}(f) = (P) - (Q).$$

We have that $f \in \mathcal{L}((Q))$ and by Riemann-Roch (1.43.1), it follows that

$$\dim \mathcal{L}((Q)) = \deg((Q)) - g + 1 = 1.$$

Since $\mathcal{L}((Q))$ already contains the constant functions, $f \in \mathcal{L}((Q)) = K$ and so $P = Q$. □

Thanks to the Riemann-Roch theorem, we can also link the genera of curves that admit some non-constant separable map between them. The following theorem makes this concrete.

Theorem 1.45 (Riemann-Hurwitz)**.** *Let C_1, C_2 be smooth curves of genus g_1, g_2 respectively. Let $\phi : C_1 \to C_2$ be a non-constant separable map, then*

$$2g_1 - 2 \geq (\deg \phi)(2g_2 - 2) + \sum_{P \in C_1} (e_\phi(P) - 1).$$

Furthermore, the above is an equality if and only if either:

(i) $\operatorname{char}(K) = 0$*, or*

(ii) $\operatorname{char}(K) = p > 0$ *and p does not divide $e_\phi(P)$ for all $P \in C_1$.*

Proof. Admitted. See [Sil09, II.5.9] □

For our purposes, the inequality in the Riemann-Hurwitz formula will always be an equality, as we can always suppose $\operatorname{char}(K)$ to be zero, or large enough.

Using the Riemann-Hurwitz formula, we get a very simple formula describing the genus of a plane curve.

Corollary 1.45.1. *Let $F \in K[X, Y, Z]$ be homogeneous of degree $d \geq 1$, and suppose that the curve C in $\mathbb{P}^2$ given by the equation $F = 0$ is non-singular. Furthermore, suppose* $\operatorname{char}(K) = 0$ *or* $\operatorname{char}(K) > d$*. Then*

$$\operatorname{genus}(C) = \frac{(d-1)(d-2)}{2}.$$

Proof. Using a change of variables if necessary, we can write

$$F(X, Y, 1) = Y^d + a_{d-1}(X)Y^{d-1} + \cdots + a_0(X).$$

It follows that $O = [0, 1, 0] \notin C$. Furthermore, we can suppose up to using another change of variables that C intersects $\{Z = 0\} \cong \mathbb{P}^1$ in exactly d points (which is the case by Bézout's theorem as long as each intersection of C with $\{Z = 0\}$ is transverse).

Define $\phi : C \to \mathbb{P}^1$ the morphism given by the projection on the x-coordinate, i.e.

$$\phi([X, Y, Z]) = [X/Z, 1]$$

For points at infinity, we can use $[X/Z, 1] = [1, Z/X]$, since we supposed $[0, 1, 0] \notin C$ and hence we get that all points at infinity are sent to $[1, 0]$.

Let $x : C \to K, [X, Y, Z] \mapsto X/Z$ and $y : C \to K, [X, Y, Z] \mapsto Y/Z$ be the coordinate functions on C and $t : \mathbb{P}^1 \to K, [X, Y] \mapsto X/Y$ the coordinate function on $\mathbb{P}^1$. Then $\phi^*(t) = x$ and hence

$$\deg(\phi) = [K(C) : \phi^* K(\mathbb{P}^1)] = [K(x, y) : K(x)]$$

We have that y satisfies the polynomial $G(u) := F(x, u, 1)$ and hence is algebraic over $K(x)$ of degree at most d.

By definition of ϕ, for all but finitely many $Q \in \mathbb{P}^1$,

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

Indeed, for $Q = [x_Q, 1] \in \mathbb{P}^1$, we get that all points in $\#\phi^{-1}(Q)$ are exactly those that lie on the line $X = Zx_Q$ and hence by Bézout's theorem, there will be in general d intersection points of this line with C. This implies by 1.19 that $d = \deg_s(\phi) \leq \deg(\phi) \leq d$ and hence ϕ is separable of degree d.

We can now apply the Riemann-Hurwitz formula 1.45, which thanks to the assumption $\mathrm{char}(K) = 0$ or $\mathrm{char}(K) > d$ is an equality (by 1.19, $e_\phi(P) \leq d$ for all p). Let $g = \mathrm{genus}(C)$, we have that $\mathrm{genus}(\mathbb{P}^1) = 0$ by 1.42. Hence the formula is written

$$g = 1 - d + \frac{1}{2} \sum_{P \in C} (e_\phi(P) - 1)$$

Intuitively, ϕ is ramified at P iff the tangent of C at P is vertical (which is when $\frac{\partial F}{\partial Y}(P) = 0$). So we may be interested in looking at the intersections $F \cap \frac{\partial F}{\partial Y}$. In fact, the result follows from Bézout's theorem if we show that for all $P \in C$,

$$e_\phi(P) - 1 = I\left(P, F \cap \frac{\partial F}{\partial Y}\right),$$

since $\deg(F) = d$ and $\deg\left(\frac{\partial F}{\partial Y}\right) = d - 1$, which implies

$$\sum_{P \in C} (e_\phi(P) - 1) = \sum_{P \in C} I\left(P, F \cap \frac{\partial F}{\partial Y}\right) = d(d-1).$$

Then the result follows directly.

So let's show this claim. Let $P = [x_P, y_P, 0] \in C$ a point at infinity, then by assumption ϕ is unramified at P. Furthermore, $O \notin C$, so $x_P \neq 0$. We can write the tangent of C at P under the form

$$a(y_P X - x_P Y) + bZ = 0$$

for some $a, b \in K$ (since P has to satisfy the equation). By assumption, C intersects $\{Z = 0\}$ transversally at P and hence $a \neq 0$, but this implies $\frac{\partial F}{\partial Y}(P) \neq 0$, so $I\left(P, F \cap \frac{\partial F}{\partial Y}\right) = 0 = e_\phi(P) - 1$.

Now, let $P = (x_P, y_P) = [x_P, y_P, 1] \in C$ a point in $\{Z \neq 0\}$. Up to a translation, we can suppose $P = (0,0)$. Then we have that $I\left(P, F \cap \frac{\partial F}{\partial Y}\right) = \mathrm{ord}_P^F\left(\frac{\partial F}{\partial Y}(x, y, 1)\right)$ and $e_\phi(P) = \mathrm{ord}_P^F(\phi^* t) = \mathrm{ord}_P^F(x)$.

We can write

$$\begin{aligned} F(X, Y, 1) = &\left(\frac{\partial F}{\partial X}(0,0) + Q(X, Y)\right) X \\ &+ a_1(0)Y + \cdots + a_{d-1}(0)Y^{d-1} + Y^d, \end{aligned}$$

where $Q(0,0) = 0$, so in $\mathcal{O}_P(C)$, we have that

$$\left(\frac{\partial F}{\partial X}(0,0) + Q(x, y)\right) x = -a_1(0)y - \cdots - a_{d-1}(0)y^{d-1} - y^d,$$

where $\frac{\partial F}{\partial X}(0,0) + Q(x, y)$ is invertible, since non-zero at $(0,0)$. It follows that $\mathrm{ord}_P^F(x) = \min\{k \mid a_k(0) \neq 0\} =: m$.

Furthermore, we have that

$$\frac{\partial F}{\partial Y}(x, y, 1) = x\frac{\partial Q}{\partial Y}(x, y) + a_1(0) + \cdots + a_{d-1}(0)(d-1)y^{d-2} + dy^{d-1}.$$

Since $x\frac{\partial Q}{\partial Y}(x, y)$ is of order at least m and the rest of the right hand side is of order $\min\{k \mid a_k(0) \neq 0\} - 1 = m - 1$, we deduce $\mathrm{ord}_P^F\left(\frac{\partial F}{\partial Y}(x, y, 1)\right) = m - 1$, which shows our claim and completes the proof. $\square$

2 Elliptic Curves

2.1 Definition and basic properties

We now have all the prerequisites to define what an elliptic curve is.

Definition 2.1. An *elliptic curve* is a smooth curve E of genus 1 with a specified point $O \in E$.

We will see later that E can be given the structure of a group, which is the reason why we specify a point O, which will act as the identity element.

Remark. From 1.45.1, we get that any smooth cubic plane curve with a specified point O is an elliptic curve.

A *Weierstrass equation* is an equation of a cubic plane curve $C \subset \mathbb{P}^2$ of the form

$$Y^2Z + aXYZ + bYZ^2 = X^3 + cX^2Z + dXZ^2 + eZ^3.$$

We can consider the set $U_Z = \{Z \neq 0\} \subset \mathbb{P}^2$. We have that $C \cap U_Z$ is an affine curve for which the set of points $[X, Y, 1] \in C \cap U_Z$ is specified by the dehomogenized equation

$$Y^2 + aXY + bY = X^3 + cX^2 + dX + e.$$

To ease notation, we will use the dehomogenized equation to define the projective curve C, remembering that there is the point at infinity $[0, 1, 0]$.

We will see that any elliptic curve can be, up to isomorphism, characterized by a Weierstrass equation. Before proving this, we will need the following lemma about singular curves given by a Weierstrass equation.

Lemma 2.2. *If a curve C given by a Weierstrass equation is singular, then there exists a rational map $\phi : E \to \mathbb{P}^1$ of degree 1.*

Proof. Making a linear change of variables, we may assume that the singular point is $(x, y) = (0, 0)$. By checking the partial derivatives, we have that the Weierstrass equation is of the form

$$C : y^2 + axy = x^3 + cx^2.$$

The rational map

$$\phi : E \to \mathbb{P}^1, (x, y) \mapsto [x, y]$$

Induces an isomorphism

$$\phi : U \to V$$

Where $U = E \setminus \{[0, 0, 1], [0, 1, 0]\} \subset E$ and $V = \mathbb{P}_1 \setminus \{[1, 0], [0, 1]\} \subset \mathbb{P}^1$ with inverse given by $[1, t] \mapsto (t^2 + at - c, t^3 + at^2 - ct)$ (indeed, if we set $t = \frac{y}{x}$, and note that if we divide the equation for C by x^2, we obtain

$t^2 + a_1 t = x + a_2$, so $\phi(x, y) = [1, t]$ is indeed mapped to $[x, tx] = [x, y]$) Hence ϕ induces an isomorphism of function fields $\phi^* : K(V) \to K(U)$ and hence $\phi^* : K(\mathbb{P}^1) \to K(E)$ is an isomorphism (since $K(V) = K(\mathbb{P}^1)$ and $K(U) = K(E)$). It follows that $\deg \phi = 1$. □

The following proposition allows us to identify elliptic curves with smooth curves given by a Weierstrass equation.

Proposition 2.3. *Let (E, O) be an elliptic curve defined over K.*

(a) There exist functions $x, y \in K(E)$ such that the map

$$\begin{aligned} \phi : E &\to \mathbb{P}^2 \\ P &\mapsto [x(P), y(P), 1] \end{aligned}$$

gives an isomorphism of E onto a curve given by the Weierstrass equation

$$C : Y^2 + aXY + bY = X^3 + cX^2 + dX + e$$

with coefficients $a, b, c, d, e \in K$ and such that $\phi(O) = [0, 1, 0]$. We call x, y the Weierstrass coordinate functions on E.

(b) Any two equations for E as in (a) are related by a linear change of variables of the form

$$\begin{aligned} X &= u^2 X' + r \\ Y &= u^3 Y' + su^2 X' + t \end{aligned}$$

with $u, r, s, t \in K, u \neq 0$.

Proof. Consider the vector spaces $\mathcal{L}(n\,(O))$ for $n \in \mathbb{N}$. By the Riemann-Roch theorem, since elliptic curves have genus 1,

$$l(n\,(O)) = \dim(\mathcal{L}(n\,(O))) = \deg(n\,(O)) = n$$

for all $n \geq 1$. Hence we can choose $x, y \in K(E)$, such that $\{1, x\}$ is a basis for $\mathcal{L}(2\,(O))$ and $\{1, x, y\}$ is a basis for $\mathcal{L}(3\,(O))$. Since $x \in \mathcal{L}(2\,(O)) \setminus \mathcal{L}((O))$, and $y \in \mathcal{L}(3\,(O)) \setminus \mathcal{L}(2\,(O))$, we have that x and y have poles at O of exact order 2 and 3 respectively.

Now, $\mathcal{L}(6\,(O))$ is of dimension 6, but it contains the seven functions $1, x, y, x^2, xy, y^2, x^3$ (which we see easily by looking at the order of the pole at O). Hence there has to be some linear relation

$$A_1 + A_2 x + A_3 y + A_4 x^2 + A_5 xy + A_6 y^2 + A_7 x^3 = 0,$$

with the A_i not all zero. Since $1, x, y, x^2, xy$ all have a pole of different order at O, we have necessarily that A_6 and A_7 are non-zero. We replace x by $-A_6 A_7 x$ and y by $A_6 A_7^2 y$, then if we divide the equation by $A_6^3 A_7^4$, we obtain an equation in the Weierstrass form. This equation describes a curve in which lies the image of the map

$$\begin{aligned}\phi : E &\to \mathbb{P}^2\\ P &\mapsto [x(P), y(P), 1]\end{aligned}$$

By definition, ϕ is a morphism, furthermore, it is not constant, so it is surjective. Furthermore, $\phi(O) = [0, 1, 0]$, since y has a higher order pole than x at O.

We will now show that the map $\phi : E \to C \subset \mathbb{P}^2$ is of degree 1. We have that

$$\deg \phi = [K(E) : \phi^* K(C)] = [K(E) : K(x, y)]$$

Consider the map $[x, 1] : E \to \mathbb{P}^1$. Since x has a double pole at (O) and no other poles, we have that (using that Y/X is a uniformizer of $\mathcal{O}_{[1,0]}(\mathbb{P}^1)$)

$$\begin{aligned}\deg[x, 1] &= \sum_{P \in [x,1]^{-1}([1,0])} e_{[x,1]}(P)\\ &= e_{[x,1]}(O) = \operatorname{ord}_O(1/x) = 2.\end{aligned}$$

Hence we get $[K(E) : K(x)] = 2$.

Similarly, we deduce that $[y, 1] : E \to \mathbb{P}^1$ has degree 3, and hence $[K(E) : K(y)] = 3$. It follows that $[K(E) : K(x, y)] = 1$ since $\gcd(2, 3) = 1$. Hence $K(E) = K(x, y)$ and so ϕ has degree 1.

Suppose ad absurdum that C is singular, then 2.2 yields a rational map $\psi : C \to \mathbb{P}^1$ of degree 1. Hence the composition $\psi \circ \phi : E \to \mathbb{P}^1$ is a map of degree 1 between smooth curves and hence an isomorphism (1.17.1). This contradicts the fact that E has genus 1 and $\mathbb{P}^1$ has genus 0 (1.42). Hence C is smooth, so again by 1.17.1, we have that the degree 1 map $\phi : E \to \mathbb{C}$ is an isomorphism, which proves part (a).

For part (b), suppose we have two pairs of Weierstrass coordinate functions (x, y) and (x', y'), then x and x' have poles of order 2 at O and y and y' have poles of order 3 at O. Hence $\{1, x\}$ and $\{1, x'\}$ are two bases for $\mathcal{L}(2\,(O))$ and $\{1, x, y\}$ and $\{1, x', y'\}$ are two bases for $\mathcal{L}(3\,(O))$. We deduce that there are some constants $u_1, u_2, r, s_2, t \in K$ with $u_1 u_2 \neq 0$ such that

$$x = u_1 x' + r \qquad \text{and} \qquad y = u_2 y' + s_2 x' + t$$

But since both (x, y) and (x', y') satisfy Weierstrass equations in which the Y^2 and X^3 terms have coefficient 1, we deduce that $u_1^3 = u_2^2$. So letting $u = u_3/u_1$ and $s = s_2/u^2$, puts the change of variables into the desired form. $\square$

Now, let E be an elliptic curve defined by the Weierstrass equation

$$E : Y^2 + aXY + bY = X^3 + cX^2 + dX + e \tag{1}$$

for some $a, b, c, d, e \in K$ with origin $O = [0, 1, 0]$.

When $\mathrm{char}(K) \notin \{2, 3\}$ (recall we assumed this is true throughout this paper), we can simplify (1) using changes of variables, if we set $Y = Y' - \frac{1}{2}(aX' + b)$ we obtain an equation of the form

$$Y'^2 = X^3 + c'X^2 + d'X + e'$$

with $c', d', e' \in K$. We can also get rid of the term X^2 with the substitution $X = X' - \frac{1}{3}c'$, we obtain an equation of the form

$$Y'^2 = X'^3 + AX' + B$$

with $A, B \in K$. A quick calculation yields $c' = c + \frac{1}{4}a^2$, hence up to using the linear change of variables

$$\begin{aligned} X &= X' - \frac{1}{3}\left(c + \frac{1}{4}a^2\right), \\ Y &= Y' - \frac{1}{2}(aX' + b), \end{aligned}$$

we can always suppose an elliptic curve E is given by the equation

$$E : Y^2 = X^3 + AX + B.$$

From 2.3, we know that a curve given by the an equation of the above form is an elliptic curve whenever it is smooth. The following proposition answers the question of when that is the case.

Proposition 2.4. *Let C be a projective plane curve defined by*

$$C : F(X, Y) = X^3 + AX + B - Y^2 = 0.$$

Let $\Delta = 4A^3 + 27B^2$ be the discriminant of $F(X, 0)$, then C is smooth (and hence an elliptic curve) if and only if $\Delta \neq 0$.

Proof. First, let us verify that $O = [0, 1, 0]$ is not singular. If we look at C in the chart $U_Y = \{Y \neq 0\}$, we get that C is given by the equation

$$G(X, Z) = X^3 + AXZ^2 + BZ^3 - Z = 0.$$

We have that

$$\nabla G(0, 0) = \begin{bmatrix} 0 \\ 1 \end{bmatrix} \neq 0,$$

and so O is a smooth point of C.

Suppose there is a point $P = (x, y) \in C$ that is singular, then we have

$$\nabla F(P) = \begin{bmatrix} 3x^2 + A \\ -2y \end{bmatrix} = 0$$

Hence we have that $\frac{\partial}{\partial X}F(x,0) = 3x^2 + A = 0$. In particular, since $P \in C$, also $F(x,0) = 0$, and hence x is a double root of $F(X,0)$ so we deduce that the discriminant $\Delta = 4A^3 + 27B^2$ is zero.

Suppose instead that $\Delta = 0$, then $F(X,0)$ admits a double root $x \in K$ (recall K is algebraically closed). Then $P = (x,0) \in C$ and

$$\nabla F(P) = \begin{bmatrix} 3x^2 + A \\ 0 \end{bmatrix} = 0,$$

since $3x^2 + A = \frac{\partial}{\partial X}F(x,0) = 0$. It follows that C is singular at P. $\square$

2.2 Group Law

In this section, we will endow elliptic curves with a group structure. Usually, the composition law is defined geometrically for cubic plane curves. To stay as general as possible, we will first define the composition law using the degree 0 part of the divisor class group and then show that the two group laws are the same.

Proposition 2.5. *Let (E,O) be an elliptic curve. The map*

$$\begin{aligned} \kappa : E &\to \mathrm{Cl}^0(E) \\ P &\mapsto \overline{(P) - (O)} \end{aligned}$$

is a bijection.

Proof. Let $D \in \mathrm{Div}^0(E)$ be a divisor. Since E has genus 1, by the Riemann-Roch theorem (1.43), we have that

$$\dim \mathcal{L}(D + (O)) = 1.$$

Let $f \in K(E)$ be a generator for $\mathcal{L}(D + (O))$. Since

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

we have necessarily that

$$\mathrm{div}(f) = -D - (O) + (P)$$

for some $P \in E$. Hence

$$D \sim (P) - (O).$$

Suppose there is some other $P' \in E$, such that $D \sim (P') - (O)$. Then $(P) \sim (P')$, but then $P = P'$ from 1.44.

This allows us to define

$$\sigma : \mathrm{Div}^0(E) \to E,$$

which sends a divisor $D \in \mathrm{Div}^0(E)$ to the corresponding point $P \in E$ as above.

This map is clearly surjective, as $\sigma((P) - (O)) = P$. Furthermore, we have that $\sigma(D_1) = \sigma(D_2)$ if and only if $D_1 \sim D_2$. Indeed, if $D_1 \sim D_2$, then

$$(\sigma(D_1)) - (O) \sim D_1 \sim D_2 \sim (\sigma(D_2)) - (O)$$

and hence $\sigma(D_1) = \sigma(D_2)$ by 1.44. Conversely, if $\sigma(D_1) = \sigma(D_2)$, then clearly

$$D_1 \sim (\sigma(D_1)) - (O) = (\sigma(D_2)) - (O) \sim D_2.$$

We deduce that σ induces a bijection $\widehat{\sigma} : \mathrm{Cl}^0(E) \to E$. Furthermore, clearly $\widehat{\sigma} = \kappa^{-1}$. ☐

Using κ, we can define the composition law $+$ as the unique composition law, which makes κ a group isomorphism. In particular, this gives E the structure of an abelian group with identity element $O = \kappa^{-1}(0)$,

Definition 2.6. We define the composition law $+$ on (E, O), by

$$P + Q = \kappa^{-1}(\kappa(P) + \kappa(Q))$$

for all $P, Q \in E$.

Notation. For $m \in \mathbb{N} \setminus \{0\}$ and $P \in E$ we define

$$[m]P = \underbrace{P + \cdots + P}_{m \text{ times}}.$$

We extend this definition to $m \in \mathbb{Z}$ with $[0]P = O$ and $[m]P = [-m](-P)$ for $m < 0$.

Thanks to how the composition law is defined on E, we get the following criteria that tells us when a divisor is principal.

Proposition 2.7. *Let (E, O) be an elliptic curve and $D = \sum n_P \cdot (P) \in \mathrm{Div}(E)$. Then D is principal if and only if $\sum n_P = 0$ and $\sum [n_P]P = O$*

Proof. Suppose D is principal, so $D \sim 0$. Principal divisors have degree 0, hence $\sum n_P = 0$. It follows that

$$\begin{aligned} \kappa\left(\sum [n_P]P\right) &= \sum n_P \kappa(P) = \sum n_P \cdot \overline{(P) - (O)} \\ &= \overline{\sum n_P \cdot (P)} = 0 \end{aligned}$$

And hence $\sum [n_P]P = 0$ by injectivity of κ.

Now suppose $\sum n_P = 0$ and $\sum [n_P]P = O$, then by the above calculation,

$$\overline{D} = \overline{\sum n_P \cdot (P)} = \kappa\left(\sum [n_P]P\right) = 0$$

and so $D \sim 0$. ☐

We will now introduce another composition law defined for smooth cubic plane curves and show that it coincides with the group law induced from $\mathrm{Cl}^0(E)$. This will not only provide the link with the usual definition of composition on an elliptic curve, but also give another way to compute the sum of two points on an elliptic curve.

Let E be a smooth cubic plane curve. By Bézout's theorem, for any line $L \subset \mathbb{P}^2$, L intersects E in exactly 3 points (taken with multiplicity). This allows us to define a composition law $\oplus$ on E as follows.

Definition 2.8. Let $P, Q \in E$ and L the line connecting P and Q (or the tangent line to E at P if $P = Q$). Let R be the third point of intersection of L with E. Let L' be the line connecting R and O. We define $P \oplus Q$ be the third point of intersection of L' with E.

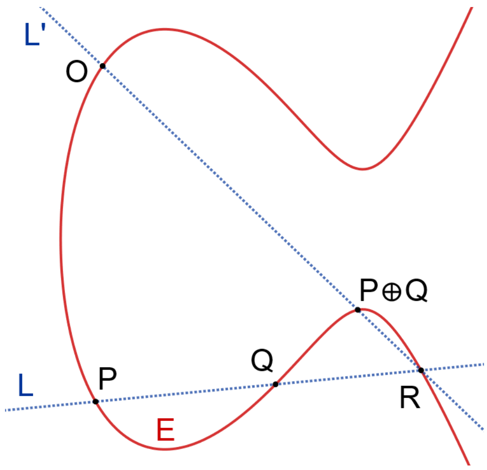

Figure 1: Visualization of geometric composition law

Proposition 2.9. *Let E be a smooth cubic plane curve, then for all $P, Q \in E$,*

$$P \oplus Q = P + Q.$$

Proof. We have to show that for $P, Q \in E$, $\kappa(P \oplus Q) = \kappa(P) + \kappa(Q)$.

Let

$$f(X, Y, Z) = \alpha X + \beta Y + \gamma Z = 0$$

give the line L in $\mathbb{P}^2$ going through P, Q and let R be the third point of intersection. Let $g(X, Y, Z) = 0$ be the equation for the tangent line T to E at O. T intersects E at O with multiplicity at least 2, let $S \in E$ be the third point of intersection (equal to O if O is a flex). Since g is homogeneous of degree 1, $f/g \in K(E)$ and so we get that

$$\begin{aligned}\operatorname{div}(f/g) &= \sum_{P' \in E} \operatorname{ord}_{P'}(f) \cdot (P') - \operatorname{ord}_{P'}(g) \cdot (P') \\ &= \sum_{P' \in E} I(P', E \cap L) \cdot (P') - I(P', E \cap T) \cdot (P') \\ &= (P) + (Q) + (R) - 2(O) - (S).\end{aligned}$$

Now let

$$f'(X, Y, Z) = \alpha' X + \beta' Y + \gamma' Z = 0$$

be the line L' through R and O. Then by the definition of $\oplus$, we have that the third point of intersection of L' with E is $P \oplus Q$. As above, $f'/g \in K(E)$ and we have

$$\operatorname{div}(f'/g) = (R) + (O) + (P \oplus Q) - 2(O) - (S) = (R) + (P + Q) - (O) - (S).$$

It follows that

$$\operatorname{div}(f'/f) = \operatorname{div}(f'/g) - \operatorname{div}(f/g) = (P \oplus Q) - (P) - (Q) + (O)$$

And hence

$$\begin{aligned}\kappa(P \oplus Q) - \kappa(P) - \kappa(Q) &= \overline{(P \oplus Q) - (O)} - \overline{(P) - (O)} - \overline{(Q) - (O)} \\ &= \overline{(P \oplus Q) - (P) - (Q) + (O)} = 0.\end{aligned}$$

□

Remark. As a byproduct of the equivalence of $+$ and $\oplus$, we get essentially for free that E with the geometric composition law $\oplus$ satisfies the group axioms (for example, from the definition of $\oplus$ it is not clear at all why this composition law should be associative).

Thanks to the equivalence of $+$ and $\oplus$, we can calculate explicit formulas for addition on E. As we have seen in Section 2.1, we can suppose up to a curve isomorphism that E is given by the reduced Weierstrass equation

$$E : F(x, y) = y^2 - x^3 - ax - b = 0$$

with origin $O = [0, 1, 0]$.

Let $P = (x_P, y_P) \in E$, then we

$$-P = (x_P, -y_P).$$

Indeed, the line connecting P and $(x_P, -y_P)$, is the line $X = x_P Z$, which has as third intersection point O. The tangent to E at O is given by $Z = 0$, which intersects E with multiplicity 3 at O, hence we obtain that $P + (x_P, -y_P) = O$.

Now let $Q = (x_Q, y_Q) \in E$ different from $-P$. Then $P+Q \neq O$. Suppose $P \neq Q$, then $x_P \neq x_Q$. We have that the line passing through P and Q is given by

$$L : y = \frac{y_Q - y_P}{x_Q - x_P}(x - x_P) + y_P$$

Setting

$$\lambda = \frac{y_Q - y_P}{x_Q - x_P} \quad \text{and} \quad \nu = \frac{x_Q y_P - x_P y_Q}{x_Q - x_P}$$

we can rewrite $L : y = \lambda x - \nu$.

If $P = Q$, then L is the tangent to E at P, which is given by

$$L : (3x_P^2 + a)(x - x_P) - 2y_P(y - y_P) = 0$$

Suppose ad absurdum that $y_P = 0$, then L is the line $x = x_P$ (the term $3x_P^2 + a$ is non-zero, since E is not singular) and so the third point of intersection is O, whence $P + Q = O$, which contradicts our assumption, and so $y_P \neq 0$. To obtain again an equation of the form $L = \lambda x - \nu$, we have to set

$$\lambda = \frac{3x_P^2 + a}{2y_P} \quad \text{and} \quad \nu = \frac{-3x_P^3 - ax_P + 2y_P^2}{2y_P} = \frac{-x_P^3 + ax_P + 2b}{2y_P}.$$

So let λ and ν be as above corresponding to the case. Let R be the third point of intersection of L with E. We have that the equation $F(x, \lambda x+\nu) = 0$ with respect to x admits exactly the zeroes x_P, x_Q, x_R and hence

$$F(x, \lambda x + \nu) = c(x - x_P)(x - x_Q)(x - x_R)$$

Since the coefficient of x^3 in $F(x, \lambda x + \nu)$ is -1, we obtain $c = -1$. By equating the coefficient of x^2, we obtain $\lambda^2 = x_P + x_Q + x_R$ and hence

$$\begin{aligned} x_R &= \lambda^2 - x_P - x_Q \\ y_R &= \lambda x_R + \nu \end{aligned}$$

The line connecting O and R is the line $x = x_R$, which intersects E in the third point $(x_R, -y_R)$. Hence we obtain $P + Q = (x_R, -y_R)$.

This can be summarized in the following proposition:

Proposition 2.10. *Let E be an elliptic curve given by the Weierstrass equation*

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

Let $P = (x_P, y_P), Q = (x_Q, y_Q) \in E$ be two points with $P \neq \pm Q$. Then

1. *The addition formula:*

$$\begin{aligned} x_{P+Q} &= \left(\frac{y_Q - y_P}{x_Q - x_P}\right)^2 - x_P - x_Q \\ y_{P+Q} &= -\frac{y_Q - y_P}{x_Q - x_P} x_{P+Q} + \frac{x_Q y_P - x_P y_Q}{x_Q - x_P} \end{aligned}$$

2. *The duplication formula. Write $P = (x, y)$, then*

$$x_{[2]P} = \left(\frac{3x^2 + a}{2y}\right)^2 - 2x$$
$$y_{[2]P} = -\frac{3x^2 + a}{2y} x_{[2]P} + \frac{-x^3 + ax + 2b}{2y}$$

2.3 Isogenies

In this section we define the notion of a "map of elliptic curves", which we call an isogeny.

Definition 2.11. Let E_1 and E_2 be elliptic curves. An *isogeny* between E_1 and E_2 is a curve morphism

$$\phi : E_1 \to E_2$$

satisfying $\phi(O) = O$. E_1 and E_2 are *isogenous* if there exists a non-constant isogeny ϕ between them.

Thanks to the group isomorphism between an elliptic curve E and $\mathrm{Cl}^0(E)$, we can deduce that the notion of isogeny is compatible with the group structure on E, i.e. an isogeny is also a group morphism.

Theorem 2.12. *Let $\phi : E_1 \to E_2$ be an isogeny, then ϕ is a group homomorphism.*

Proof. If ϕ is constant, then $\phi(P) = O$ for all $P \in E_1$, hence there is nothing to show. Otherwise as we have seen, ϕ induces the map

$$\begin{aligned} \phi_* : \mathrm{Cl}^0(E_1) &\to \mathrm{Cl}^0(E_2) \\ \overline{\sum_{P \in E_1} n_P \cdot (P)} &\mapsto \overline{\sum_{P \in E_1} n_P \cdot (\phi P)}. \end{aligned}$$

We also have the group isomorphisms

$$\begin{aligned} \kappa_i : E_i &\to \mathrm{Cl}^0(E_i) \\ P &\mapsto \overline{(P) - (O)} \end{aligned}$$

for $i \in \{1, 2\}$. Since $\phi(O) = O$, the following diagram commutes:

$$\begin{tikzcd} E_1 \arrow[r, "\kappa_1"] \arrow[d, "\phi"'] & \mathrm{Cl}^0(E_1) \arrow[d, "\phi_*"] \\ E_2 \arrow[r, "\kappa_2"'] & \mathrm{Cl}^0(E_2) \end{tikzcd}$$

We get that $\phi = \kappa_2^{-1} \circ \phi_* \circ \kappa_1$ and hence being a composition of group homomorphisms, it is a group homomorphim. $\square$

In particular, this theorem justifies identifying a general elliptic curve with its counterpart defined by a reduced Weierstrass equation.

Thanks to this theorem, and the explicit formulas we found for addition in E, we can show that addition and negation define curve morphisms.

Theorem 2.13. *Let (E, O) be an elliptic curve, then the maps*

$$\begin{aligned} + : E \times E &\to E \\ (P, Q) &\mapsto P + Q \end{aligned}$$

and

$$\begin{aligned} - : E &\to E \\ P &\mapsto -P \end{aligned}$$

are morphisms.

Proof. From 2.3, we know that there exists an isomorphism ψ between (E, O) and a curve C given by an equation of the reduced Weierstrass form

$$C : y^2 = x^3 + ax + b$$

ψ sends O to $[0, 1, 0]$, hence ψ is an isogeny. In particular, ψ preserves the group structure on E and hence the following diagrams commute.

$$\begin{array}{ccc} E \times E & \xrightarrow{+} & E \\ {\scriptstyle \psi\times\psi}\downarrow & & \downarrow{\scriptstyle \psi} \\ C \times C & \xrightarrow[+]{} & C \end{array} \qquad \begin{array}{ccc} E & \xrightarrow{-} & E \\ {\scriptstyle \psi}\downarrow & & \downarrow{\scriptstyle \psi} \\ C & \xrightarrow[-]{} & C \end{array}$$

It follows that $+$ and $-$ are curve morphisms iff the corresponding maps for C are.

Hence can suppose E is given by the reduced Weierstrass equation

$$E : y^2 = x^3 + ax + b$$

From 2.10 we see that the addition map $+ : E \times E \to E$ is regular at all points except possibly at points of the form $(P, P), (P, -P), (P, O), (O, P)$, since for points not of this form, we have that $P + Q = (x_{P+Q}, y_{P+Q})$, and x_{P+Q} and y_{P+Q} can be written as a polynomial fraction with only a power of $(x_Q - x_P)$ in the denominator, which is well defined for such points.

Now to deal with the other cases, let $Q_1, Q_2 \in E$ be any two points and τ_1, τ_2 the two associated translation maps. Consider the composition of maps

$$\phi : E \times E \xrightarrow{\tau_1 \times \tau_2} E \times E \xrightarrow{+} E \xrightarrow{\tau_1^{-1}} E \xrightarrow{\tau_2^{-1}} E.$$

If we calculate the image of $(P_1, P_2) \in E$ under this map, we get

$$\phi(P_1, P_2) = (P_1 + Q_1) + (P_2 + Q_2) - Q_1 - Q_2 = P_1 + Q_2,$$

since E is an abelian group. Hence the maps ϕ and $+$ are the same.

We have that the τ_i are rational maps (defined by $\tau_i(P) = (x_{P+Q_i}, y_{P+Q_i})$) between smooth curves and so they are morphisms. They're invertible, so they are isomorphisms. It follows that ϕ is regular at all points except possibly at points of the form

$$(P - Q_1, P - Q_2), (P - Q_1, -P - Q_2), (P - Q_1, -Q_2), (-Q_1, P - Q_2)$$

and consequently $+$ is regular at points not of this form. By varying Q_1, Q_2, we deduce that $+$ is regular everywhere and so a morphism.

The map $-$ is a rational map between smooth curves (defined by $-(x_P, y_P) = (x_p, -y_P)$), hence a morphism. □

This proves that E is an algebraic group, that is an algebraic variety with the structure of a group, such that $+$ and $-$ are regular (this makes E an *algebraic group*).

Corollary 2.13.1. *Let E be an elliptic curve, then for $m \in \mathbb{Z}$, the map $[m]$, which sends $P \in E$ to $[m]P$ is an isogeny.*

Proof. Clearly $[m](O) = O$, hence it suffices to show that $[m]$ is a morphism.

If $m = 0$, then $[m]$ is the constant map, hence a morphism. Suppose $m > 0$, then $[m]$ is given by the composition

$$E \xrightarrow{\Delta} E^m \xrightarrow{+} E^{m-1} \xrightarrow{+} \cdots \xrightarrow{+} E$$

where Δ is the diagonal morphism and $+$ is made to act on the last two components of E^k, which is a morphism by 2.13. Hence $[m]$ is a morphism.

If $m < 0$, then $[m] = (-) \circ [-m]$, so being a composition of two morphisms, it is a morphism. □

The $[m]$ isogeny will play an important role in showing the Weil conjectures. The reason is that its kernel is the m-torsion subgroup of E.

Definition 2.14. Let E be an elliptic curve and $m \in \mathbb{Z}$, $m \neq 0$. The *m-torsion subgroup* of E, denoted $E[m]$, is the set of points of order m in E.

$$E[m] = \{P \in E \mid [m]P = O\} = \ker[m].$$

The *torsion subgroup* of E, denoted E_{tors}, is the set of points of finite order in E.

$$E_{\text{tors}} = \bigcup_{m=1}^{\infty} E[m]$$

The m-torsion subgroups have a really nice structure, which we will be able to exploit and extract some valuable information from.

Another important example of isogeny is the Frobenius morphism, which we defined earlier.

Proposition 2.15. *Let E be an elliptic curve given by a Weierstrass equation and suppose* $\mathrm{char}(K) = p \neq 0$. *Let $q = p^r$. We have that $E^{(q)}$ is an elliptic curve and the Frobenius morphism*

$$\begin{aligned} \phi_q : E &\to E^{(q)} \\ (x, y) &\mapsto (x^q, y^q) \end{aligned}$$

is an isogeny.

Proof. $E^{(q)}$ is defined by raising the coefficients of the equation of E to the q^{th} power, hence its is also a cubic plane curve. It follows that it is an elliptic curve provided that it is smooth. If E is given by the equation

$$E : y^2 = x^3 + ax + b$$

then $E^{(q)}$ is given by the equation

$$E^{(q)} : y^2 = x^3 + a^q x + b^q$$

We get that since we're in characteristic p,

$$\Delta(E^{(q)}) = 4\,(a^q)^3 + 27\,(b^q)^2 = \left(4a^3 + 27b^2\right)^q = \Delta(E)^q$$

and so by 2.4, we deduce that $E^{(q)}$ is smooth iff E is. Hence $E^{(q)}$ is an elliptic curve and ϕ_q, being a morphism which sends O to O, is an isogeny. $\square$

Let $\mathbb{F}_q \subset K$ be the subfield of K of order q. If E is defined over $\mathbb{F}_q$, then $E^{(q)} = E$ and ϕ_q becomes an endomorphism. We can look at the set of $\mathbb{F}_q$-rational points of E, i.e. the points whose coordinates lie in $\mathbb{F}_q$,

$$E(\mathbb{F}_q) = \{(x, y) \in E \mid x, y \in \mathbb{F}_q\} \cup \{O\}.$$

As we have noted earlier, $E(\mathbb{F}_q)$ is exactly the set of fixed points of ϕ_q, which we can rewrite thanks to the group structure of E as

$$E(\mathbb{F}_q) = \ker(1 - \phi_q).$$

Since $\ker(1-\phi_q) = (1-\phi_q)^{-1}(O)$ we can now try make use of 1.19 to calculate the cardinality of this set. The issue is that 1.19 gives us the cardinality of the preimage of a non-constant morphism at almost all points, but not all of them. Thankfully, we can rectify this thanks to the group structure of E.

Theorem 2.16. *Let $\phi : E_1 \to E_2$ be a non-constant isogeny. For every $Q \in E_2$,*

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

Furthermore, for every $P \in E_1$,

$$e_\phi(P) = \deg_i(\phi).$$

In particular, if ϕ is separable, it is unramified and

$$\# \ker \phi = \deg \phi.$$

Proof. From 1.19(b), we have that

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

for all but finitely many $Q \in E_2$. Now, let $Q, Q' \in E_2$ and choose $R \in E_1$ such that $\phi(R) = Q' - Q$. Then since ϕ is a group homomorphism, we have that there is a one-to-one correspondence

$$\begin{aligned} \phi^{-1}(Q) &\to \phi^{-1}(Q') \\ P &\mapsto P + R. \end{aligned}$$

It follows that

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

for all $Q \in E_2$.

Now, let $P, P' \in E_1$ with $\phi(P) = \phi(P') = Q$ and let $R = P' - P$. We get that $\phi(R) = O$ and so $\phi \circ \tau_R = \phi$ It follows from 1.19(c) and the fact that τ_R is an isomorphism, that

$$e_\phi(P) = e_{\phi \circ \tau_R}(P) = e_\phi(\tau_R(P)) = e_\phi(P').$$

We deduce that every point in ϕ^{-1} has the same ramification index. Now, we have from 1.19(a) that

$$\begin{aligned} (\deg_s \phi)(\deg_i \phi) = \deg \phi &= \sum_{P \in \phi^{-1}(Q)} e_\phi(P) \\ &= (\#\phi^{-1}(Q))e_\phi(P) \quad \text{for any } P \in \phi^{-1}(Q) \\ &= (\deg_s \phi)e_\phi(P). \end{aligned}$$

Cancelling the $\deg_s \phi$, gives us $\deg_i \phi = e_\phi(P)$ for all $P \in E_1$. ☐

As we see, things work out very nicely when we work with separable isogenies. Luckily for us, $[m]$ and $1 - \phi_q$ are separable isogenies. We will not show this result, but it will turn out to be very important as we will see later.

Proposition 2.17. *Let E be an elliptic curve and $m \in \mathbb{Z}$, $m \neq 0$. If* $\mathrm{char}(K) = 0$ *or m is prime to* $\mathrm{char}(K)$*, then the isogeny $[m]$ is separable.*

Proof. See [Sil09, III.5.4]. □

Proposition 2.18. *Suppose* $\mathrm{char}(K) = p \neq 0$ *and let E be an elliptic curve defined over $\mathbb{F}_q$, where q is a power of p. Let $\phi_q : E \to E$ be the q^{th} power Frobenius endomorphism. Let $m, n \in \mathbb{Z}$. Then the map*

$$m + n\phi : E \to E$$

is separable if and only if $p \nmid m$. In partiular, $1 - \phi_q$ is a separable isogeny.

Proof. See [Sil09, III.5.5] □

In particular, in the light of the above discussion, we get that

$$\#E(\mathbb{F}_q) = \# \ker(1 - \phi_q) = \deg(1 - \phi_q)$$

2.4 The Dual Isogeny

We will now briefly introduce the notion of dual isogenies. Given an isogeny

$$\phi : E_1 \to E_2,$$

we have that ϕ induces a map

$$\phi^* : \mathrm{Cl}^0(E_2) \to \mathrm{Cl}^0(E_1).$$

We can use ϕ^* to construct a map $\hat{\phi} : E_2 \to E_1$ as the composition

$$E_2 \xrightarrow{\kappa_2} \mathrm{Cl}^0(E_2) \xrightarrow{\phi^*} \mathrm{Cl}^0(E_1) \xrightarrow{\kappa_1^{-1}} E_1 \ .$$

It can be shown that $\hat{\phi}$ is an isogeny, however the proof will be ommitted here (see [Sil09, III.6.1]).

Definition 2.19. The isogeny $\hat{\phi}$ is called the *dual isogeny.*

The dual isogeny has many properties that make it behave quite nicely. The following theorem lists a few of those properties.

Theorem 2.20. *Let*

$$\phi : E_1 \to E_2$$

be an isogeny of degree d. Then

(a) We have that

$$\begin{aligned} \hat{\phi} \circ \phi &= [d] \qquad \text{on } E_1; \\ \phi \circ \hat{\phi} &= [d] \qquad \text{on } E_2. \end{aligned}$$

(b) Let $\lambda : E_2 \to E_3$ be another isogeny, then

$$\widehat{\lambda \circ \phi} = \hat{\phi} \circ \hat{\lambda}.$$

(c) For all $m \in \mathbb{Z}$, $[m] = \widehat{[m]}$

(d)

$$\hat{\hat{\phi}} = \phi$$

Proof. (a) We have that $\phi = \kappa_2^{-1} \circ \phi_* \circ \kappa_1$ and hence by 1.25(e)

$$\begin{aligned}\phi \circ \hat{\phi} &= (\kappa_2^{-1} \circ \phi_* \circ \kappa_1) \circ (\kappa_1^{-1} \circ \phi^* \circ \kappa_2) \\ &= \kappa_2^{-1} \circ \phi_* \circ \phi^* \circ \kappa_2 = [d]\end{aligned}$$

Now, we have that

$$(\hat{\phi} \circ \phi) \circ \hat{\phi} = \hat{\phi} \circ [d] = [d] \circ \hat{\phi}$$

and hence $\hat{\phi} \circ \phi = [d]$, since $\hat{\phi}$ is non-constant and hence surjective.

(b) We deduce from 1.25(f)

$$\begin{aligned}\widehat{\lambda \circ \phi} &= \kappa_1^{-1} \circ (\lambda \circ \phi)^* \circ \kappa_3 \\ &= \kappa_1^{-1} \circ \phi^* \circ \lambda^* \circ \kappa_3 \\ &= \hat{\phi} \circ \hat{\lambda}\end{aligned}$$

(c) Admitted. See [Sil09, III.6.2(d)].

(d) We have that

$$\phi \circ \hat{\phi} = [d] = \widehat{[d]} = \widehat{\phi \circ \hat{\phi}} = \hat{\hat{\phi}} \circ \hat{\phi}$$

and hence $\phi = \hat{\hat{\phi}}$, since $\hat{\phi}$ is non-constant and hence surjective.

□

We get thanks to this theorem the following corollary, which will allow us to deduce the cardinality of $E[m]$.

Corollary 2.20.1. *For any $m \in \mathbb{Z}$, we have that* $\deg[m] = m^2$.

Proof. We have that

$$[m] \circ \widehat{[m]} = [m] \circ [m] = [m^2]$$

and hence $\deg[m] = m^2$ by 2.20. □

In the case when $[m]$ is separable, it follows that

$$\#E[m] = \#\ker[m] = \deg[m] = m^2.$$

Being an abelian group, we are close to determining the structure of $E[m]$ up to isomorphism. In fact $E[m]$ is a product of two cyclic groups of order m.

Proposition 2.21. *Let E be an elliptic curve and $m \in \mathbb{Z}$, $m \neq 0$. Suppose that m is prime to p if $p > 0$. Then*

$$E[m] \cong (\mathbb{Z}/m\mathbb{Z}) \times (\mathbb{Z}/m\mathbb{Z})$$

Proof. We have that $\deg[m] = m^2$ and from 2.17, $[m]$ is separable, hence using 2.16, we deduce that

$$\#E[m] = \#\ker[m] = \deg[m] = m^2.$$

Furthermore, for every integer d dividing m, we have that

$$\#E[d] = d^2.$$

From the classification theorem of finite abelian groups, $E[m]$ is isomorphic to a product of cyclic groups.

$$E[m] \cong \prod_i \mathbb{Z}/p_i^{k_i}\mathbb{Z}$$

For any prime $q \in \mathbb{Z}$ dividing m, we have that the q-torsion subgroup of $E[m]$ is of cardinality $q^{\#\{i\in\mathbb{N}:p_i=q\}}$, since for any $k \in \mathbb{N}$, the q-torsion subgroup of $\mathbb{Z}/q^k\mathbb{Z}$ is $q^{k-1}\mathbb{Z}/q^k\mathbb{Z}$, which is of cardinality q. But the q-torsion subgroup of $E[m]$ is exactly $E[q]$, which is of cardinality q^2, hence we deduce

$$\#\{i \in \mathbb{N} : p_i = q\} = 2.$$

It follows that up to reordering the terms,

$$E[m] \cong \mathbb{Z}/q^{k_1}\mathbb{Z} \times \mathbb{Z}/q^{k_2}\mathbb{Z} \times \prod_{i>2} \mathbb{Z}/p_i^{k_i}\mathbb{Z}$$

where neither p_i is equal to q. Let r be the multiplicity of q in the prime decomposition of m. We have that $k_1 + k_2 = 2r$. Then we have from direct calculation that the q^r-torsion subgroup of $E[m]$ is of cardinality $\min\{q^{k_1}, q^r\} \min\{q^{k_2}, q^r\}$. However the q^r-torsion subgroup of $E[m]$ is exactly $E[q^r]$, which is of cardinality q^{2r}. It follows that $k_1, k_2 \geq r$ and hence necessarily $k_1 = k_2 = r$.

Now, let for any prime $q \mid m$, the multiplicity r_q with which it divides m. We get that

$$E[m] \cong \prod_{q|m} \mathbb{Z}/q^{r_q}\mathbb{Z} \times \mathbb{Z}/q^{r_q}\mathbb{Z} \cong \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$$

using the Chinese remainder theorem. □

2.5 The Tate Module

In this section we will construct the *Tate Module*, which will allow us to exploit the structure of $E[m]$.

Let l be a prime that is different from $p = \text{char}(K)$ if $p > 0$. For any isogeny $\phi : E_1 \to E_2$, we have that l^n-torsion points are sent to l^n-torsion points (since it is a group morphism) and hence ϕ induces a map

$$\phi : E_1[l^n] \to E_2[l^n].$$

Thanks to the proposition 2.21, we can identify ϕ to a matrix in $\mathrm{GL}_2(\mathbb{Z}/l^n\mathbb{Z})$ and hence study ϕ by studying the corresponding matrix. This identification involves choosing bases for $E_i[l^n]$, but for example the trace and determinant don't depend on the chosen bases. However, we would prefer to work with matrices over a ring of characteristic 0. The way we can achieve this is to use l-adic numbers. Let's start by reminding the definition of l-adic numbers.

First let us define what an inverse limit of a sequence of rings is

Definition 2.22. Let $(A_n)_{n\in\mathbb{N}}$ be rings and for each $n \in \mathbb{N}$, $f_n : A_n \to A_{n-1}$ a morphism. The inverse (or projective) limit of $(A_n)_{n\in\mathbb{N}}$ with respect to the maps f_n is the ring

$$\varprojlim_n A_n = \left\{ (a_n)_{n\in\mathbb{N}} \in \prod_{n\in\mathbb{N}} A_n \mid \forall n \in \mathbb{N}, f_n(a_n) = a_{n-1} \right\},$$

taken as a subring of $\prod_{n\in\mathbb{N}} A_n$.

We define the inverse limit of a sequence of groups the same way (replace "ring" by "group" in the definition).

We can now define what l-adic integers are.

Definition 2.23. Let l be a prime. The ring of l-adic integers, denoted $\mathbb{Z}_l$, is the inverse limit

$$\mathbb{Z}_l = \varprojlim_n \mathbb{Z}/l^n\mathbb{Z},$$

taken with respect to the morphisms

$$\begin{aligned} \mathbb{Z}/l^{n+1}\mathbb{Z} &\to \mathbb{Z}/l^n\mathbb{Z}, \\ k &\mapsto k \mod l^n. \end{aligned}$$

We will use the construction of inverse limit with the $E[l^n]$ with the goal to get a representation of $\mathrm{Hom}(E_1, E_2)$ over $\mathrm{GL}_2(\mathbb{Z}_l)$.

Definition 2.24. Let E be an elliptic curve and $l \in \mathbb{Z}$ a prime. The (l-adic) *Tate module of* E is the group

$$T_l(E) = \varprojlim_n E[l^n],$$

where the inverse limit is taken with respect to the maps

$$E[l^{n+1}] \xrightarrow{[l]} E[l^n]$$

Since each $E[l^n]$ is a $\mathbb{Z}/l^n\mathbb{Z}$-module, $T_l(E)$ admits naturally the structure of a $\mathbb{Z}_l$-module. For $g \in T_l(E)$ and $r \in \mathbb{Z}_l$, the multiplication is given by

$$r \cdot g = ([r_n]g_n)_{n\in\mathbb{N}}$$

which is well defined, since $[l]([r_n]g_n) = [r_n]([l]g_n) = [r_{n-1}]g_{n-1}$ (as $r_n \equiv r_{n-1} \mod l^{n-1}$).

We can also immediately deduce the structure of $T_l(E)$.

Proposition 2.25. *Let l a prime different from $p = \mathrm{char}(K)$ if $p > 0$. As a $\mathbb{Z}_l$-module, the Tate module is isomorphic to $\mathbb{Z}_l \times \mathbb{Z}_l$.*

Proof.

$$T_l(E) = \varprojlim_n E[l^n] \cong \varprojlim_n (\mathbb{Z}/l^n\mathbb{Z} \times \mathbb{Z}/l^n\mathbb{Z}) = \mathbb{Z}_l \times \mathbb{Z}_l.$$

□

As above, we get that an isogeny $\phi : E_1 \to E_2$ induces a homomorphism $\phi : E_1[l^n] \to E_2[l^n]$ for all $n \in \mathbb{N}$ and we have that $\phi \circ [l] = [l] \circ \phi$ since ϕ is a group homomorphism. It follows that ϕ induces the map

$$\begin{aligned} \phi_l : T_l(E_1) &\to T_l(E_2) \\ (a_n)_{n\in\mathbb{N}} &\mapsto (\phi(a_n))_{n\in\mathbb{N}} \end{aligned}$$

Since $T_l(E_i) \cong \mathbb{Z}_l \times \mathbb{Z}_l$, after choosing bases for $T_l(E_i)$, we can see ϕ_l as an element in $\mathrm{GL}_2(\mathbb{Z}_l)$. As we will see, the trace and determinant of ϕ_l encode very useful quantities.

We can also apply the construction of inverse limits to the multiplicative group $K^\times$. Let μ_{l^n} be the subgroup of $(l^n)^{\text{th}}$ roots of unity of K (recall K is algebraically closed). Then raising to the l^{th} power defines a natural map $\mu_{l^{n+1}} \to \mu_{l^n}$.

Definition 2.26. The (l-adic) *Tate module of K* is the group

$$T_l(\mu) = \varprojlim_n \mu_{l^n},$$

where the inverse limit is taken with respect to the l^{th} power maps.

We have that $\mu_{l^n} \cong \mathbb{Z}/l^n\mathbb{Z}$. Furthermore, if ξ_n is an l^n-th primitive root of unity, this isomorphism is given by

$$\xi_n^k \to k \mod l^n$$

We have that

$$(\xi_n^k)^l = \xi_n^{kl} = \xi_{n-1}^k$$

and so the following diagram commutes:

$$\begin{array}{ccc} \mu_{l^n} & \xrightarrow{(\cdot)^l} & \mu_{l^{n-1}} \\ \downarrow{\cong} & & \downarrow{\cong} \\ \mathbb{Z}/l^n\mathbb{Z} & \xrightarrow{\text{mod } l^{n-1}} & \mathbb{Z}/l^{n-1}\mathbb{Z} \end{array}$$

So we see that $T_l(\mu) \cong \mathbb{Z}_l$ as a group (where multiplication in $T_l(\mu)$ corresponds to addition in $\mathbb{Z}_l$).

We have that $T_l(\mu)$ admits the structure of a $\mathbb{Z}_l$ module via exponentiation (since each μ_{l^n} is a $\mathbb{Z}/l^n\mathbb{Z}$-module via exponentiation). Hence $T_l(\mu)$ is isomorphic to $\mathbb{Z}_l$ as a $\mathbb{Z}_l$ module, in particular, it is torsion-free.

2.6 The Weil Pairing

Let E be an elliptic curve.

The goal of this section is to construct the Weil pairing, i.e. construct a bilinear form with the properties described in the following proposition.

Proposition 2.27. *Suppose $l \in \mathbb{Z}$ is a prime different from $p = \text{char}(K)$ if $p > 0$. There exists a bilinear, alternating, non-degenerate pairing*

$$e : T_l(E) \times T_l(E) \to T_l(\mu)$$

Furthermore, if $\phi : E_1 \to E_2$ is an isogeny, then ϕ and its dual isogeny $\hat{\phi}$ are adjoits for the pairing.

The motivation behind constructing such a bilinear form is that it will provide a link between the trace and determinant of ϕ_l and other quantities related to ϕ, in particular the degree of ϕ and $1 - \phi$. Recall that when ϕ is the Frobenius morphism, $1 - \phi$ is separable, so $\deg(1 - \phi) = \# \ker(1 - \phi) = \#E(\mathbb{F}_q)$.

In what follows we fix an integer $m \geq 2$, prime to $p = \text{char}(K)$ if $p > 0$. The strategy is to first construct a pairing

$$e_m : E[m] \times E[m] \to \mu_m$$

which has the desired properties, and then construct the Weil pairing using the inverse limit. Let $T \in E[m]$, then using 2.7 there is a function $f \in K(E)$ such that

$$\text{div}(f) = m(T) - m(O).$$

A non-constant isogeny is surjective, hence there exists some $T' \in E$ with $[m]T' = T$.

Since $[m]$ is a separable isogeny, $e_{[m]}(P) = 1$ for all $P \in E$.

$$\begin{aligned}
[m]^*(T) - [m]^*(O) &= \sum_{P \in [m]^{-1}(T)} e_{[m]}(P) \cdot (P) - \sum_{P \in [m]^{-1}(0)} e_{[m]}(P) \cdot (P) \\
&= \sum_{P \in E[m]} (T' + P) - (P)
\end{aligned}$$

and since $\sum_{P \in E[m]} T' + P - P = [m^2]T' = O$, it follows that there exists some $g \in K(E)$ such that

$$\operatorname{div}(g) = [m]^*(T) - [m]^*(O)$$

We have that

$$\begin{aligned}
\operatorname{div}(f \circ [m]) &= \operatorname{div}([m]^* f) = [m]^* \operatorname{div}(f) \\
&= m\left([m]^*(T) - [m]^*(O)\right) = m \operatorname{div}(g) = \operatorname{div}(g^m)
\end{aligned}$$

Hence $f \circ [m]$ and g^m are equal up to a constant factor. Multiplying f by an element of $K^\times$, we may assume that

$$f \circ [m] = g^m$$

Now, let $S \in E[m]$ (possibly $S = T$), then for any point $X \in E$,

$$g(X + S)^m = f([m]X + [m]S) = f([m]X) = g(X)^m.$$

Hence we can define a pairing

$$\begin{aligned}
e_m : E[m] \times E[m] &\to \mu_m \\
(S, T) &\mapsto g(X + S)/g(X)
\end{aligned}$$

for any $X \in E$ such that $g(X + S)$ and $g(X)$ are both defined and non-zero. Notice that if τ_S is translation by S, that $g \circ \tau_S$ and g have the same divisor, as $S \in E[m]$. It follows that $g \circ \tau_S / g$ is the constant function and so the pairing does not depend on the choice of X. Furthermore, g is defined up to multiplication by a constant in $K^\times$, but the value of the pairing does not depend on this choice either and hence it is well-defined.

The Weil e_m-pairnig satistfies the properties we were looking for, in particular, it is also compatible with taking the inverse limit. The following proposition makes this precise.

Proposition 2.28. *The Weil e_m-pairing is:*

(a) Bilinear:

$$\begin{aligned}
e_m(S_1 + S_2, T) &= e_m(S_1, T) e_m(S_2, T) \\
e_m(S, T_1 + T_2) &= e_m(S, T_1) e_m(S, T_2)
\end{aligned}$$

so in particular for all $k \in \mathbb{Z}/m\mathbb{Z}$,

$$e_m([k]S, T) = e_m(S, T)^k = e_m(S, [k]T)$$

(b) *Alternating:*

$$e_m(T,T) = 1,$$

so in particular,

$$e_m(S,T) = e_m(T,S)^{-1}$$

(c) *Non-degenerate: If $e_m(S,T) = 1$ for all $S \in E[m]$, then $T = O$.*

(d) *Compatible: If $S \in E[nm]$ and $T \in E[m]$, then*

$$e_{nm}(S,T) = e_m([n]S,T)$$

Proof. Admitted. See [Sil09, III.8.1]. □

Proposition 2.29. *Let $S \in E_1[m]$, $T \in E_2[m]$, and $\phi : E_1 \to E_2$ an isogeny. Then*

$$e_m(S,\hat{\phi}(T)) = e_m(\phi(S),T)$$

Proof. Admitted. See [Sil09, III.8.2]. □

Now to prove proposition 2.27, it suffices to pass the construction of e_{l^n} to the inverse limit. To show that the $e_{l^n} : E[l^n] \times E[l^n] \to \mu_{l^n}$ induce a map $e : T_l(E) \times T_l(E) \to T_l(\mu)$, we have to show that the e_{l^n}-pairings are compatible with taking the inverse limit. The inverse limits for $T_l(E)$ and $\mathbb{T}_l(\mu)$ are formed using the maps

$$E[l^{n+1}] \xrightarrow{[l]} E[l^n] \qquad \text{and} \qquad \mu_{l^{n+1}} \xrightarrow{(\cdot)^l} \mu_{l^n}$$

so we require that

$$e_{l^{n+1}}(S,T)^l = e_{l^n}([l]S,[l]T).$$

We have by properties (a) and (d) of 2.28 that

$$e_{l^{n+1}}(S,T)^l = e_{l^{n+1}}(S,[l]T) = e_{l^n}([l]S,[l]T).$$

Hence the e_{l^n} induce a map $e : T_l(E) \times T_l(E) \to T_l(\mu)$, which inherits all the properties of 2.28, so this shows 2.27.

Remark. The bilinearity property extended to $e : T_l(E) \times T_l(E) \to T_l(\mu)$ implies that for all $a \in \mathbb{Z}_l$

$$e([a]S,T) = e(S,T)^a.$$

Indeed, we have that denoting $a_n \in \mathbb{Z}/l^n\mathbb{Z}$ the projection of a,

$$e_n([a_n]S,T) = e_n(S,T)^{a_n}.$$

by bilinearity and hence the above fact follows from the construction of the inverse limit.

The following proposition finally makes concrete the utility of the Weil pairing. It will serve as the main tool for showing the Weil conjectures for elliptic curves.

Proposition 2.30. *Let* $\psi \in \mathrm{End}(E)$. *Then*

$$\det(\psi_l) = \deg(\psi)$$

and

$$\mathrm{tr}(\psi_l) = 1 + \deg(\psi) - \deg(1 - \psi).$$

In particular, $\det(\psi_l)$ *and* $\mathrm{tr}(\psi_l)$ *are in* $\mathbb{Z}$ *and are independent of* l.

Proof. Fix a $\mathbb{Z}_l$-basis v_1, v_2 for $T_l(E)$. In this basis, ψ_l is written as

$$\psi_l = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$$

with $a, b, c, d \in \mathbb{Z}_l$. Let

$$e : T_l(E) \times T_l(E) \to T_l(\mu)$$

be the Weil pairing (2.27).

We have that using the properties of the pairing,

$$\begin{aligned}
e(v_1, v_2)^{\deg \psi} &= e([\deg \psi] v_1, v_2) \\
&= e(\hat{\psi}_l \psi_l v_1, v_2) \\
&= e(\psi_l v_1, \psi_l v_2) \\
&= e(a v_1 + c v_2, b v_1 + d v_2) \\
&= e(v_1, v_1)^{ab} e(v_1, v_2)^{ad} e(v_2, v_1)^{bc} e(v_2, v_2)^{cd} \\
&= e(v_1, v_2)^{ad - bc} \\
&= e(v_1, v_2)^{\det \psi_l}
\end{aligned}$$

Since e is non-degenerate, we can suppose $e(v_1, v_2) \neq 1$ and hence

$$e(v_1, v_2)^{\deg \psi - \det \psi_l} = 1,$$

which implies $\deg \psi = \det \psi_l$, since $T_l(\mu)$ is torsion-free as a $\mathbb{Z}_l$-module. For a 2×2 matrix A, it follows from direct calculation that

$$\mathrm{tr}(A) = 1 + \det(A) - \det(1 - A)$$

□

3 Weil Conjectures

For this section we fix a prime p and q a power of p. We suppose throughout this section that $\mathrm{char}(K) = p$.

In this section we will state the Weil conjectures and prove them in the case of elliptic curves.

If K is of characteristic p, it contains a unique subfield of order p^n for any $n \in \mathbb{N}$ (see course *Rings and Fields*), we will denote this subfield by $\mathbb{F}_{p^n}$. We will be studying the set of $\mathbb{F}_{q^n}$-rational points of a projective variety.

Definition 3.1. Let $V/\mathbb{F}_q$ be a projective variety. The zeta function of $V/\mathbb{F}_q$ is defined as the power series

$$Z(V/\mathbb{F}_q; T) = \exp\left(\sum_{n=1}^{\infty} (\#V(\mathbb{F}_{q^n}))\frac{T^n}{n}\right)$$

Notation. When $V/\mathbb{F}_q$ is known from context, we write simply $Z(T)$ instead of $Z(V/\mathbb{F}_q; T)$

Theorem 3.2 (Weil Conjectures)**.** *Let $V/\mathbb{F}_q$ be a smooth projective variety of dimension N.*

(a) Rationality: $Z(T) \in \mathbb{Q}(T)$. More precisely, there is a factorization

$$Z(T) = \frac{P_1(T) \cdots P_{2n-1}(T)}{P_0(T)P_2(T) \cdots P_{2n}(T)},$$

where $P_0(T) = 1 - T, P_{2n}(T) = 1 - q^nT$ and for each $1 \leq i \leq 2n-1$, $P_i(T)$ factors (over $\mathbb{C}$) as

$$P_i(T) = \prod_j (1 - \alpha_{ij}T)$$

(b) Functional Equation: The zeta function satisfies

$$Z\left(\frac{1}{q^NT}\right) = \pm q^{N\frac{\epsilon}{2}} T^{\epsilon} Z(T),$$

for some integer ϵ (called the Euler characteristic of V)

(c) Riemann Hypothesis: $|\alpha_{ij}| = q^{i/2}$ for all $1 \leq i \leq 2n-1$ and all j.

(d) Betti Numbers: If $V/\mathbb{F}_q$ is a good reduction mod p of a non-singular projective variety W/K, where K is a number field embedded in the field of complex numbers, then the degree of P_i is the i^{th} Betti number (i.e. rank of the i^{th} homology group) of the space of complex points of W.

We won't define what a "good reduction" means in general, but we can look at the case of elliptic curves given by a Weierstrass equation.

If K be a number field (seen as a subfield of its algebraic closure $\overline{K}$) and $\mathcal{O}$ its ring of integers. Suppose E is an elliptic curve given by a Weierstrass equation defined over K, i.e. E is of the form

$$E : y^2 = x^3 + ax + b$$

with $a, b \in K$. We have that $K = \mathrm{Frac}(\mathcal{O})$ and so we can write $a = a_1/a_2$ and $b = b_1/b_2$ for some $a_1, b_1 \in \mathcal{O}$, and $a_2, b_2 \in \mathcal{O} \setminus \{0\}$. We can (uniquely) decompose the ideal (a_2b_2) into a product of prime ideals (see course *Algebraic Number Theory*).

$$(a_2b_2) = \mathfrak{p}_1 \dots \mathfrak{p}_s$$

Then choosing a prime ideal $\mathfrak{p}$ of $\mathcal{O}$ different from $\mathfrak{p}_i$ for any i, we get that $a_2, b_2 \notin \mathfrak{p}$. Hence we can see E as being defined over $\mathcal{O}_\mathfrak{p}$. The maximal ideal $\mathfrak{P}$ of $\mathcal{O}_\mathfrak{p}$ is just the image of $\mathfrak{p}$ under the localization. We deduce

$$\mathcal{O}_\mathfrak{p}/\mathfrak{P} \cong (\mathcal{O}/\mathfrak{p})_\mathfrak{p} = \mathcal{O}/\mathfrak{p} \cong \mathbb{F}_q,$$

where q is a power of p, where $(p) = \mathfrak{p} \cap \mathbb{Z}$.

This gives us a new curve C obtained by reducing E modulo $\mathfrak{P}$.

$$C : y^2 = x^3 + \bar{a}x + \bar{b},$$

defined over the residue field isomorphic to $\mathbb{F}_q$. We say that C is a *good* reduction of E modulo p if it is also smooth. That is the case if and only if its discriminant

$$\Delta(C) = 4\bar{a}^3 + 27\bar{b}^2$$

is non-zero. But notice that the discriminant of C is just the residue of $\Delta(E) = 4a^3 + 27b^2$ modulo $\mathfrak{P}$. Hence the reduction of E mod p is "good" if $\Delta(E) \notin \mathfrak{P}$. We will show that (d) of 3.2 holds for elliptic curves given by Weierstrass equations in Section 4.

In the rest of this section, we will prove the Weil conjectures (save part (d)) for the case of elliptic curves. For that, we will make use of the relation found in 2.30. In the following proposition we get a formula for $\#E(\mathbb{F}_{q^n})$, which we will be able to use for proving the Weil conjectures.

Proposition 3.3. *Let $E/\mathbb{F}_q$ be an elliptic curve, and*

$$\phi : E \to E, (x, y) \mapsto (x^q, y^q)$$

the q^{th}-power Frobenius endomorphism. Let $\alpha, \beta \in \mathbb{C}$ be the roots of the characteristic polynomial of ϕ_l, that is

$$\det(T - \phi_l) = T^2 - \mathrm{tr}(\phi_l)T + \det(\phi_l),$$

then α, β are complex conjugates satisfying $|\alpha| = |\beta| = \sqrt{q}$. Furthermore, for every $n \geq 1$, we have

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

Proof. We have by 2.18 and 2.16 that

$$\#E(\mathbb{F}_q) = \deg(1 - \phi)$$

and from 2.30, we have that

$$\det(\phi_l) = \deg(\phi) = q;$$

For all $m/n \in \mathbb{Q}$, with $p \nmid m$, we have using 2.18 that

$$\det\left(\frac{m}{n} - \phi_l\right) = \frac{\det(m - n\phi_l)}{n^2} = \frac{\deg(m - n\phi_l)}{n^2} \geq 0$$

Hence the polynomial $\det(T - \phi_l)$ is non-negative for $T \in \mathbb{R}$ (by continuity). If α, β are the roots of $\det(T - \phi_l)$, it follows that α, β are complex conjugates (they can be equal). So $|\alpha| = |\beta|$ and since $\alpha\beta = \det(\phi_l) = q$, it follows that $|\alpha| = |\beta| = \sqrt{q}$.

Now, for $n \geq 1$ the $(q^n)^{\text{th}}$-power Frobenius endomorphism ϕ^n satisfies

$$\#E(\mathbb{F}_{q^n}) = \deg(1 - \phi^n) = \det(1 - \phi_l^n)$$

We have that

$$\det(T - \phi_l^n) = (T - \alpha^n)(T - \beta^n)$$

since the eigenvalues of ϕ_l^n are the n^{th} powers of the eigenvalues of ϕ_l. From 2.30, we have that

$$\operatorname{tr}(\phi_l^n) = 1 + \deg(\phi^n) - \deg(1 - \phi^n) = 1 + q^n - \#E(\mathbb{F}_{q^n}).$$

and hence

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

□

At last, we can state and prove the Weil conjectures for the case of elliptic curves.

Theorem 3.4. *Let $E/\mathbb{F}_q$ be an elliptic curve. Then there exists an $a \in \mathbb{Z}$ such that*

$$Z(T) = \frac{1 - aT + qT^2}{(1 - T)(1 - qT)}.$$

Furthermore,

$$Z\left(\frac{1}{qT}\right) = Z(T)$$

and

$$1 - aT + qT^2 = (1 - \alpha T)(1 - \beta T)$$

with $|\alpha| = |\beta| = \sqrt{q}$

Proof. Using the definition of $Z(E/\mathbb{F}_q;T)$, we get

$$\begin{aligned}\log Z(E/\mathbb{F}_q;T) &= \sum_{n=1}^{\infty}(\#E(\mathbb{F}_{q^n}))\frac{T^n}{n} \\ &= \sum_{n=1}^{\infty}(q^n+1-\alpha^n-\beta^n)\frac{T^n}{n} \qquad (3.3) \\ &= -\log(1-qT)-\log(1-T)+\log(1-\alpha T)+\log(1-\beta T)\end{aligned}$$

and hence we get

$$Z(E/\mathbb{F}_q;T) = \frac{(1-\alpha T)(1-\beta T)}{(1-T)(1-qT)},$$

which has the desired form. Indeed from (3.3), $|\alpha| = |\beta| = \sqrt{q}$, and

$$\begin{aligned}a = \alpha+\beta = \operatorname{tr}(\phi_l) &= 1+\deg(\phi)-\deg(1-\phi) \\ &= 1+q-\#E(\mathbb{F}_q) \in \mathbb{Z}.\end{aligned}$$

□

Hence the Weil conjectures are verified for elliptic curves. Notice that using the notation from theorem 3.2, $\deg P_0 = 1$, $\deg P_1 = 2$, $\deg P_2 = 1$, hence if $C/\mathbb{F}_q$ is a good reduction of E/K, where K is a number field embedded in the field of complex numbers, we would expect the Betti numbers of the space of complex points of E to coincide with these values, and indeed, as we will see in the following section, this is indeed the case.

4 Elliptic Curves as Complex Tori

The goal of this section is to show an elliptic curve defined over $\mathbb{C}$ is isomorphic to a torus as a Riemann surface (and actually even as a complex lie group). In particular, this will allow us to verify that the point (d) of the Weil Conjectures is true for elliptic curves.

Throughout this section, we suppose $K = \mathbb{C}$.

4.1 Riemann Surface Structure

First, let's discuss the Riemann surface structure that an elliptic curve is given.

Definition 4.1. The *complex topology* on $\mathbb{P}^n$ is the quotient topology induced by the Euclidean topology on $\mathbb{C}^{n+1}$.

Throughout this section we will consider $\mathbb{P}^n$ with the complex topology, and hence an elliptic curve $E \subset \mathbb{P}^2$ will be equipped with the subspace topology.

Proposition 4.2. *Let $E \subset \mathbb{P}^2$ be an elliptic curve, then E admits the structure of a Riemann surface.*

Proof. Let $y^2 - x^3 - ax - b = f(x, y) = 0$ be the equation defining E. So for all $P = (x_P, y_P) \in E$ with $y_P \neq 0$, $\frac{\partial f}{\partial y}(P) \neq 0$ and hence by the implicit function theorem there exists an open set $V_P \subseteq \mathbb{C}$ containing x_P and an analytic function $g_P : V_P \to \mathbb{C}$, such that $g_P(x_P) = y_P$ and $f(x, g_P(x)) = 0$ for all $x \in V_P$. Furthermore $U_P = (\mathrm{id} \times g_P)(V_P) \subset E$, is an open subset of E. Indeed, $U_P = \pi_x^{-1}(V_P)$, where $\pi_x : E \setminus \{O\} \to \mathbb{C}, (x, y) \mapsto x$. Hence we define $\phi_P = \pi_x|_{U_P}$ which is a homeomorphism to its image $\phi_P(U_P) = V_P$ (the inverse to which is given by $x \mapsto (x, g_P(x))$).

For all $P = (x_P, 0) \in E$ we define the chart $\phi_P : U_P \to \mathbb{C}$ similarly, except we inverse the roles of x and y in the above reasoning. Indeed, $\frac{\partial f}{\partial x}(P) \neq 0$, since E is smooth, hence we get the existence of $V_P \subset \mathbb{C}$ containing y_P and $h_P : V_P \mapsto \mathbb{C}$, such that $h_P(y_P) = x_P$ and $f(h_P(y), y) = 0$ for all $y \in V_P$. We set $U_P := (h_P \times \mathrm{id})(V_P)$ and $\phi_P : U_P \to \mathbb{C}, (x, y) \mapsto y$.

Finally, we have yet to define a chart whose domain covers the point at infinity $O = [0, 1, 0] \in E$. To do this, we can look at E in $\{[X, Y, Z] \in \mathbb{P}^2 \mid Y \neq 0\}$ instead. We get that in this copy of $\mathbb{A}^2$, E is given by the equation.

$$z - x^3 - axz^2 - bz^3 = \tilde{f}(x, z) = 0.$$

We have that $\frac{\partial \tilde{f}}{\partial z}(O) = 1 \neq 0$, hence we can again apply the reasoning from above. We obtain the chart $\phi_O : U_O \to \mathbb{C}, [x, 1, z] \mapsto x$ with inverse $\phi_0^{-1} : \phi_O(U_O) \to \mathbb{C}, x \mapsto [x, 1, \tilde{g}(x)]$.

Now let $P, Q \in E \setminus \{O\}$, with $y_P \neq 0$ and $y_Q = 0$. We have that

$$\begin{aligned}
&\phi_P \circ \phi_Q^{-1}(y) = \phi_P(h_Q(y), y) = h_Q(y) \\
&\phi_Q \circ \phi_P^{-1}(x) = \phi_Q(x, g_P(x)) = g_P(x) \\
&\phi_P \circ \phi_O^{-1}(x) = \phi_P([x, 1, \tilde{g}(x)]) = \phi_P\left(\frac{x}{\tilde{g}(x)}, \frac{1}{\tilde{g}(x)}\right) = \frac{x}{\tilde{g}(x)} \\
&\phi_O \circ \phi_P^{-1}(x) = \phi_O(x, g_P(x)) = \phi_O\left(\left[\frac{x}{g_P(x)}, 1, \frac{1}{g_P(x)}\right]\right) = \frac{x}{g_P(x)}
\end{aligned}$$

All of these transition maps are holomorphic and by transitivity so are $\phi_O \circ \phi_Q^{-1}$ and $\phi_Q \circ \phi_O^{-1}$. Hence the the atlas $\mathcal{A} = \{\phi_P \mid P \in E\}$ is holomorphic and so gives E the structure of a Riemann surface. □

4.2 Elliptic Functions

Let's introduce the definition and some basic properties of elliptic functions. For the rest of this section, let $\Lambda \subseteq \mathbb{C}$ be an arbitrary lattice.

Definition 4.3. An *elliptic function* (relative to the lattice Λ) is a meromorphic function f on $\mathbb{C}$, which satisfies

$$f(z + \lambda) = f(z) \qquad \text{for all } \lambda \in \Lambda, z \in \mathbb{C}$$

Notation. The set of elliptic functions relative to the lattice Λ is denoted $\mathbb{C}(\Lambda)$.

Remark. $\mathbb{C}(\Lambda)$ is a field with the usual operations of addition and multiplication of complex functions.

Definition 4.4. A *fundamental parallelogram* for Λ is a set of the form

$$D = \{a + r\lambda_1 + s\lambda_2 \mid r, s \in [0, 1)\},$$

where $a \in \mathbb{C}$ and λ_1, λ_2 is a basis for Λ.

Liouville's theorem tells us that a bounded entire function is constant. If an elliptic function is bounded on a fundamental parallelogram, then it is bounded everywhere by periodicity, so we get the following proposition.

Proposition 4.5. *An elliptic function with no poles (or no zeros) is constant.*

Proof. Suppose that $f(z) \in \mathbb{C}(\Lambda)$ is holomorphic (i.e. it has no poles). Let D be a fundamental parallelogram for Λ. Since f is periodic, we have that

$$\sup_{z \in \mathbb{C}} |f(z)| = \sup_{z \in \overline{D}} |f(z)|.$$

Since f is continous, it is bounded on the compact set $\overline{D}$. It follows that it is bounded on all of $\mathbb{C}$. By Liouville's theorem, f is constant. If f has no zeros, we can look at $1/f$. □

Notation. For $f \in \mathbb{C}(\Lambda), z \in \mathbb{C}/\Lambda$, we write $f(z), \mathrm{res}_z(f)$ and $\mathrm{ord}_z(f)$ for $f(\bar{z}), \mathrm{res}_{\bar{z}}(f)$ and $\mathrm{ord}_{\bar{z}}(f)$ respectively, for any one representative $\bar{z} \in \mathbb{C}$ of the coset z. This is well defined by the Λ-periodicity of f.

From periodicity of an elliptic function, we can deduce the following result from the residue theorem.

Proposition 4.6. *Let $f \in \mathbb{C}(\Lambda)$.*

(a) $\sum_{z \in \mathbb{C}/\Lambda} \mathrm{res}_z(f) = 0.$

(b) $\sum_{z \in \mathbb{C}/\Lambda} \mathrm{ord}_z(f) = 0.$

Proof. We can choose a fundamental parallelogram D for Λ, such that f has no zeroes or poles on the boundary ∂D.

(a) By the residue theorem,

$$\sum_{z \in \mathbb{C}\Lambda} \mathrm{res}_z(f) = \frac{1}{2\pi i} \int_{\partial D} f(z)\, dz.$$

By periodicity, the integrals along the opposite sides of ∂D cancel out, so the integral along the boundary of D is zero.

(b) Since f is periodic, so is f' and hence also f/f'. We have that $\mathrm{res}_z(f/f') = \mathrm{ord}_z(f)$ and hence this point follows from (a) applied to the elliptic function f/f'.

□

Next let us introduce the Weierstrass $\wp$-function, which will serve as a connecting link between elliptic curves and elliptic functions.

Definition 4.7. (a) The Weierstrass elliptic function ($\wp$-function), is defined by the series

$$\wp(z;\Lambda) = \frac{1}{z^2} + \sum_{\lambda \in \Lambda \setminus \{0\}} \left(\frac{1}{(z-\lambda)^2} - \frac{1}{\lambda^2} \right)$$

(b) The Eisenstein series (of Λ) of weight k, where $k \geq 2$ is an integer is the series

$$G_k(\Lambda) = \sum_{\lambda \in \Lambda \setminus \{0\}} \lambda^{-k}$$

Notation. If Λ is known from context, we write simply $\wp(z)$ and G_k for $\wp(z;\Lambda), G_k(\Lambda)$ respectively.

Of course, we have to show that the Eisenstein series converge and the Weierstrass $\wp$-function are well defined and elliptic.

Proposition 4.8. *(a) The Eisenstein series $G_k(\Lambda)$ is absolutely convergent for all $k \geq 3$.*

(b) The series defining the Weierstrass $\wp$-function converges absolutely and uniformly on every compact subset of $\mathbb{C} \setminus \Lambda$. It defines a meromorphic function on $\mathbb{C}$ with double poles of residue 0 at each lattice point.

(c) The Weierstrass $\wp$-function is an even elliptic function.

Proof. (a) Let λ_1, λ_2 be basis vectors of Λ. Let

$$A_N := \{n\lambda_1 + m\lambda_2 \in \Lambda \mid n, m \in \mathbb{Z}, \max(|n|, |m|) = N\}.$$

Let also

$$m = \min\{|a\lambda_1 + b\lambda_2| \mid a, b \in \mathbb{R}, \max(|a|, |b|) = 1\},$$

then m is well defined and strictly positive, as it's the minimum of a compact subset of $\mathbb{R}$, which does not contain zero. We have that

$$\#A_N = (2N+1)^2 - (2N-1)^2 = 8N.$$

Furthermore, $\min\{|\lambda|, \lambda \in A_N\} \geq Nm$, so we get

$$\sum_{\lambda \in \Lambda \setminus 0} \frac{1}{|\lambda|^k} \leq \sum_{N=1}^{\infty} \frac{\#A_N}{\min\{|\lambda|, \lambda \in A_N\}^k} = \sum_{N=1}^{\infty} \frac{8}{m^k N^{k-1}} < \infty.$$

(b) If $|\lambda| > 2|z|$, then we have that

$$|2\lambda - z| \leq 2|\lambda| + |z| \leq \frac{5}{2}|\lambda|$$

and

$$|z - \lambda| = |\lambda| \left|\frac{z}{\lambda} - 1\right| \geq \frac{1}{2}|\lambda|.$$

These imply that

$$\left|\frac{1}{(z-\lambda)^2} - \frac{1}{\lambda^2}\right| = \left|\frac{z(2\lambda - z)}{\lambda^2 (z-\lambda)^2}\right| \leq 10\frac{|z|}{|\lambda|^3}$$

Hence using (a) we see that the series for $\wp$ converges absolutely and uniformly on any compact subset of $\mathbb{C} \setminus \Lambda$. It follows that the series defines a holomorphic function on $\mathbb{C} \setminus \Lambda$, furthermore, it is clear from the series expansion that $\wp$ has a double pole with residue 0 at each point of Λ.

(c) It follows from the definition of $\wp$ that $\wp(z) = \wp(-z)$, since we can just replace λ by $-\lambda$ in the sum. Since the series converges uniformly, we can compute the derivative of $\wp$ by termwise differentiation. We obtain

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

It is clear from this expansion that $\wp'$ is an elliptic function, hence for all $\lambda \in \Lambda$,

$$\frac{\partial}{\partial z}(\wp(z) - \wp(z+\lambda)) = \wp'(z) - \wp'(z+\lambda) = 0$$

and hence $\wp(z) - \wp(z+\lambda)$ is the constant function. By setting $z = -\lambda/2$, and using the fact $\wp$ is even, we get that

$$\wp(z) - \wp(z+\lambda) = \wp(-\lambda/2) - \wp(\lambda/2) = 0$$

and hence $\wp$ is an elliptic function.

$\square$

As in the case of curves, we can define divisors for elliptic functions.

Definition 4.9. Let Λ be a lattice, the *divisor group* $\mathrm{Div}(\mathbb{C}/\Lambda)$ to be the free abelian group on the set $\mathbb{C}/\Lambda$. We write elements of $\mathrm{Div}(\mathbb{C}/\Lambda)$ as $\sum_{z\in\mathbb{C}/\Lambda} n_z(z)$ with $n_z \in \mathbb{Z}$ and $n_z = 0$ for all but finitely many z.

We define analogously to the case of elliptic curves,

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

and for any $f \in \mathbb{C}(\Lambda)^\times$ we define the divisor $\mathrm{div}(f) \in \mathrm{Div}^0(\mathbb{C}/\Lambda)$ by

$$\mathrm{div}(f) = \sum_{z\in\mathbb{C}/\Lambda} \mathrm{ord}_z(f)\cdot(z)$$

Divisors give us an useful way to compare elliptic functions, as if the divisors of two elliptic functions are equal, the functions have to be equal up to multiplication by a constant. In fact, we can use them to show the following powerful result.

Theorem 4.10. *We have that*

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

Proof. Let $f \in C(\Lambda)$. We can decompose f as

$$f(z) = \frac{1}{2}(f(z) + f(-z)) + \frac{1}{2}(f(z) - f(-z)),$$

hence we see that it suffices to prove the theorem for odd and even functions. If f is odd, then $\wp' f$ is even, so we can just consider the case that f is even.

If f is even, we have that

$$\operatorname{ord}_z f = \operatorname{ord}_{-z} f$$

for all $z \in \mathbb{C}$. Furthermore, if $2z \in \Lambda$, then $\operatorname{ord}_z f$ is even. By differentiating $f(z) = f(-z)$ repeatedly, we obtain

$$f^{(k)}(z) = (-1)^k f^{(k)}(-z)$$

so if $2z \in \Lambda$, $f^{(k)}(z) = f^{(k)}(-z)$, which implies $f^{(k)}(z) = 0$ for all odd k. Hence $\operatorname{ord}_z f$ must be even.

Let D be a fundamental parallelogram for Λ and let H be "half" of D in the sense that it is a fundamental domain for $(\mathbb{C}/\Lambda)/\{\pm 1\}$ in $\mathbb{C}$, i.e. $\mathbb{C} = (H + \Lambda) \cup (-H + \Lambda)$. Then the divisor of f has the form

$$\sum_{z \in D} n_z(z) = \sum_{z \in H} n'_z((z) + (-z)).$$

for certain integers n_z and

$$n'_z = \begin{cases} n_z & \text{if } 2z \notin \Lambda; \\ \frac{1}{2} n_z & \text{if } 2z \in \Lambda. \end{cases}$$

If $2z \in \Lambda$, then $n_z = \operatorname{ord}_z f$ is even, so this is well defined.

Now consider the function

$$g(z) = \prod_{w \in H \setminus 0} (\wp(z) - \wp(w))^{n_w}.$$

The divisor of $\wp(z) - \wp(w)$ is $(w) + (-w) - 2(0)$, so we see that f and g have exactly the same zeros and poles except possibly at 0. But then by 4.6 they also have the same order at 0. It follows that f/g is a holomorphic elliptic function and so is constant by 4.5. We conclude that $f = cg \in \mathbb{C}(\wp, \wp')$. $\square$

We would like to get a result similar to 2.7 for divisors of elliptic functions. In fact, such a result holds, and to show it, we will make use of the Weierstrass σ-function.

Definition 4.11. The *Weierstrass σ-function* (relative to Λ) is the function defined by

$$\sigma(z; \Lambda) = z \prod_{\lambda \in \Lambda \setminus 0} \left(1 - \frac{z}{\lambda}\right) \exp\left(\frac{z}{\lambda} + \frac{1}{2}\left(\frac{z}{\lambda}\right)^2\right)$$

Notation. As before, we write just $\sigma(z)$ for $\sigma(z;\Lambda)$ when Λ is clear from context.

The most useful property of the σ-function is that it holomorphic and has simple zeroes on the lattice points. This will allow us to take an appropriate product of σ translated to match the zeroes and poles of any given elliptic function. Furthermore, if certain criteria are met, this product will define an elliptic function.

Lemma 4.12. *(a) The infinite product for σ defines a holomorphic function on all of $\mathbb{C}$. It has simple zeros at each $z \in \Lambda$ and no other zeros.*

(b) For all $z \in \mathbb{C} \setminus \Lambda$

$$\frac{d^2}{dz^2} \log \sigma(z) = -\wp(z)$$

(c) For any $\lambda \in \Lambda$, there are constants $a, b \in \mathbb{C}$ such that for all $z \in \mathbb{C}$

$$\sigma(z+\lambda) = e^{az+b}\sigma(z)$$

Proof. (a) Let $K \subset \mathbb{C}$ be a compact set. Let $M > 0$ be such that $K \subset B(0,M)$. We have that for all $z \in K$ and $\lambda \in \Lambda \backslash 0$ such that $|\lambda| \geq \frac{3}{2}M$, using the Taylor expansion of $\log(1-x)$,

$$\begin{aligned}
\left|\log\left(1-\frac{z}{\lambda}\right)+\frac{z}{\lambda}+\frac{1}{2}\left(\frac{z}{\lambda}\right)^2\right| &\leq \sum_{k=3}^{\infty}\frac{1}{k}\left|\frac{z}{\lambda}\right|^k \\
\left(\text{since } \left|\frac{z}{\lambda}\right| \leq \frac{M}{|\lambda|}\right) \qquad &\leq \frac{1}{3}\left(\frac{M}{|\lambda|}\right)^3 \sum_{k=0}^{\infty}\left(\frac{M}{|\lambda|}\right)^k \\
&= \frac{1}{3}\left(\frac{M}{|\lambda|}\right)^3\left(1-\frac{M}{|\lambda|}\right)^{-1} \\
\left(\text{since } \frac{M}{|\lambda|} \leq \frac{2}{3}\right) \qquad &\leq \left(\frac{M}{|\lambda|}\right)^3
\end{aligned}$$

We deduce from 4.8(a) that the series

$$\sum_{\substack{\lambda\in\Lambda\backslash 0 \\ |\lambda|\geq\frac{3}{2}M}} \left|\log\left(1-\frac{z}{\lambda}\right)+\frac{z}{\lambda}+\frac{1}{2}\left(\frac{z}{\lambda}\right)^2\right|$$

converges uniformly on K and hence so does the product defining σ (since there is only a finite number of $\lambda \in \Lambda$ with $|\lambda| < \frac{3}{2}M$).

Hence the product defining σ converges on all compact subsets of $\mathbb{C}$ and so σ defines a holomorphic function on all of $\mathbb{C}$.

Since the series

$$\sum_{\lambda\in\Lambda\backslash 0}\left(\log\left(1-\frac{z}{\lambda}\right)+\frac{z}{\lambda}+\frac{1}{2}\left(\frac{z}{\lambda}\right)^2\right)$$

converges provided $z\notin\Lambda$, $\sigma(z)\neq 0$ for all $z\in\Lambda$. Clearly, $\sigma(\lambda)=0$ for all $\lambda\in\Lambda$ and $\frac{\sigma(z)}{z-\lambda}$ is non-zero for $z=\lambda$ by the same argument as above. Hence σ has simple zeros at each $z\in\Lambda$ and no other zeros.

(b) We have from (a) that we can differentiate

$$\log\sigma(z)=\log z+\sum_{\lambda\in\Lambda\backslash 0}\left(\log\left(1-\frac{z}{\lambda}\right)+\frac{z}{\lambda}+\frac{1}{2}\left(\frac{z}{\lambda}\right)^2\right)$$

term by term. We get

$$\begin{aligned}\frac{d}{dz}\log\sigma(z)&=\frac{1}{z}+\sum_{\lambda\in\Lambda\backslash 0}\left(\frac{1}{z-\lambda}+\frac{1}{\lambda}+\frac{z}{\lambda^2}\right)\\ \frac{d^2}{dz^2}\log\sigma(z)&=-\frac{1}{z^2}+\sum_{\lambda\in\Lambda\backslash 0}\left(\frac{-1}{(z-\lambda)^2}+\frac{1}{\lambda^2}\right)=-\wp(z)\end{aligned}$$

(c) Let $\lambda\in\Lambda$. Since $\wp$ is elliptic, for all $z\in\mathbb{C}$,

$$\frac{d^2}{dz^2}\log\sigma(z+\lambda)=-\wp(z+\lambda)=\wp(z)=\frac{d^2}{dz^2}\log\sigma(z).$$

By integrating twice, we obtain

$$\log\sigma(z+\lambda)=\log\sigma(z)+az+b$$

for some constants of integration $a,b\in\mathbb{C}$.

□

We will now see how we can use the σ-function to prove the desired property.

Proposition 4.13. *Let $n_1,\ldots,n_r\in\mathbb{Z}$ and $z_1,\ldots,z_n\in\mathbb{C}$, such that*

$$\sum n_i=0 \text{ and } \sum n_iz_i\in\Lambda.$$

Then there exists an elliptic function $f(z)\in\mathbb{C}(\Lambda)$ satisfying

$$\operatorname{div}(f)=\sum n_i(z_i).$$

Proof. Let $\lambda = \sum n_i z_i \in \Lambda$. Replacing $\sum n_i(z_i)$ by $\sum n_i(z_i) + (0) - (\lambda)$, we may assume that $\sum n_i z_i = 0$ (indeed these are two different writings for the same divisor as $0 \equiv \lambda \mod \Lambda$). Then from 4.12(a) we get that

$$f(z) = \prod \sigma(z - z_i)^{n_i}$$

has the correct zeros and poles. Furthermore, from 4.12(c), we get that

$$\begin{aligned} f(z+\lambda) &= \prod \sigma(z + \lambda - z_i)^{n_i} \\ &= \prod \left(\sigma(z - z_i)e^{a(z-z_i)+b}\right)^{n_i} \\ &= e^{\sum n_i(az+b) - a\sum n_i z_i} f(z) \\ &= f(z) \end{aligned}$$

and hence $f \in \mathbb{C}(\Lambda)$. $\square$

4.3 Constructing the Isomorphism

The Weierstrass $\wp$-function satisfies a differential equation, which we will be able exploit to exhibit an isomorphism between an elliptic curve and a torus.

Proposition 4.14. *For all $z \in \mathbb{C} \setminus \Lambda$, we have that*

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

In order to show that $\wp$ satisfies this differential equation, we will first calculate the Laurent series of $\wp$.

Proposition 4.15. *The Laurent series for $\wp(z)$ about $z = 0$ is given by*

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

Proof. For $|z| < |\lambda|$, we have that

$$\begin{aligned} \frac{1}{(z-\lambda)^2} - \frac{1}{\lambda^2} &= \frac{1}{\lambda^2}\left(\left(\frac{1}{1-\frac{z}{\lambda}}\right)^2 - 1\right) \\ &= \frac{1}{\lambda^2}\left(\left(\sum_{k=0}^{\infty}\left(\frac{z}{\lambda}\right)^k\right)^2 - 1\right) \\ &= \frac{1}{\lambda^2}\left(\sum_{k=0}^{\infty}(k+1)\left(\frac{z}{\lambda}\right)^k - 1\right) \\ &= \sum_{k=1}^{\infty}(k+1)\frac{z^k}{\lambda^{k+2}} \end{aligned}$$

where the third equality is obtained by grouping the terms $\left(\frac{z}{\lambda}\right)^k$ together in the double sum (the series is absolutely convergent). Hence we have that for all $|z| < \min\{|\lambda| : \lambda \in \Lambda \setminus 0\}$

$$\begin{aligned}\wp(z) &= z^{-2} + \sum_{\lambda \in \Lambda \setminus 0} \left((z-\lambda)^{-2} - \lambda^{-2}\right) \\ &= z^{-2} + \sum_{\lambda \in \Lambda \setminus 0} \sum_{k=1}^{\infty} (k+1) \frac{z^k}{\lambda^{k+2}} \\ &= z^{-2} + \sum_{k=1}^{\infty} (k+1) z^k G_{k+2}\end{aligned}$$

The result follows from the fact that $G_{k+2} = 0$ for k odd, since the terms $1/\lambda^{k+2}$ and $1/(-\lambda)^{k+2}$ cancel each other out. $\square$

We can now use the Laurent series to show that $\wp$ satisfies 4.14. Since an elliptic function with no poles is constant, it suffices to look at the first few terms of the Laurent series.

Proof of 4.14. We write the first few terms in various Laurent expansions:

$$\begin{aligned}\wp(z) &= z^{-2} + 3G_4 z^2 + 5G_6 z^4 + \dots \\ \wp(z)^3 &= z^{-6} + 9G_4 z^{-4} + 15G_6 + \dots \\ \wp'(z)^2 &= 4z^{-6} - 24G_4 z^{-2} - 80G_6 + \dots\end{aligned}$$

Comparing these, we see that the function

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

is holomorphic around $z = 0$, since the negative power terms cancel each other out. But since $\wp$ is elliptic and holomorphic on $\mathbb{C} \setminus \Lambda$, we get that f is elliptic and holomorphic everywhere, so constant. Since f vanishes at 0, we get $f \equiv 0$. $\square$

Remark. We write

$$g_2 = g_2(\Lambda) = 60G_4 \text{ and } g_3 = g_3(\Lambda) = 60G_3.$$

Then the equation in 4.14 becomes

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

The differential equation in 4.14 being the equation for an elliptic curve, we can finally exhibit an isomorphism between $\mathbb{C}/\Lambda$, which is the torus and the elliptic curve given by the corresponding equation.

Theorem 4.16. *Let g_2, g_3 be the quantities associated to Λ as in the above remark. Let $E/\mathbb{C}$ be the curve given by the equation*

$$E : y^2 = 4x^3 - g_2 x - g_3$$

then E is an elliptic curve and the map

$$\phi : \mathbb{C}/\Lambda \to E$$
$$z \mapsto \begin{cases} [\wp(z), \wp'(z), 1] & \text{if } z \notin \Lambda \\ [0, 1, 0] & \text{if } z \in \Lambda \end{cases}$$

is an isomorphism of complex Lie groups.

Proof. To show E is an elliptic curve, we have to show that it is non-singular. From 2.4 this is the case if and only if the determinant Δ of the polynomial $f(x) = 4x^3 - g_2 x - g_3$ is non-zero, in other words if and only if f has no repeated roots. Let $\{\lambda_1, \lambda_2\}$ be a basis of Λ, let $\lambda_3 = \lambda_1 + \lambda_2$. then since $\wp'$ is an odd elliptic function, we have that for $i \in \{1, 2, 3\}$

$$\wp'(\lambda_i/2) = -\wp'(-\lambda_i/2) = -\wp'(\lambda_i/2)$$

and hence $\wp'(\lambda_i/2) = 0$. It follows from 4.14 that $\wp(\lambda_i/2)$ is a root of f. So we need to show that the $\wp(\lambda_i/2)$ are all distinct. The function $\wp(z) - \wp(\lambda_i/2)$ has a double zero at $\lambda_i/2$, since its derivative is $\wp'(z)$ which vanishes at $\lambda_i/2$. Using 4.6 and 4.8, we deduce that these are the only zeroes and hence the $\wp(\lambda_i/2)$ are all distinct. Hence E is indeed an elliptic curve.

The image of ϕ is contained in $E(\mathbb{C})$ by 4.14. Let $[x, y, 1] \in E(\mathbb{C})$, then we have that $\wp(z) - x$ is a non-constant elliptic function, so by 4.5, it has a zero $a \in \mathbb{C}$. Hence $\wp(a) = x$ and hence by 4.14,

$$\wp'(a)^2 = f(\wp(a)) = f(x) = y^2.$$

It follows that $\wp'(a) = \pm y$, hence by replacing a with $-a$ in the case $\wp'(a) = -y$, we get that $\wp'(a) = y$. Hence $\phi(a) = [x, y, 1]$. This shows the surjectivity of ϕ.

Now to show injectivity, suppose $z_1, z_2 \in \mathbb{C}$ are such that $\phi(z_1) = \phi(z_2)$. Suppose $z_1 \not\equiv -z_1 \mod \Lambda$. The function $\wp(z) - \wp(z_1)$ admits the roots $z_1, -z_1, z_2$, but being of order 2, two of these values are congruent mod Λ. Hence $z_2 \equiv \pm z_1 \mod \Lambda$. But since $\wp'(z_1) = \wp'(z_2)$, we get necessarily $z_2 \equiv z_1 \mod \Lambda$.

Now, if $z_1 \equiv -z_1 \mod \Lambda$, then

$$\frac{\partial}{\partial z}(\wp(z) - \wp(z_1)) = \wp'(z)$$

and $\wp'(z_1) = \wp'(-z_1) = -\wp'(z_1)$ and hence $\wp'(z_1) = 0$. It follows that z_1 is a double root of $\wp(z) - \wp(z_1)$, which is of order 2. Hence z_2, being also a root of $\wp(z) - \wp(z_1)$, is necessarily congruent to z_1 mod Λ. This shows the injectivity of ϕ.

Now we will show ϕ is an isomorphism of Riemann surfaces. Denote by $\xi : \mathbb{C} \mapsto \mathbb{C}/\Lambda$, the quotient map. Then the charts of $\mathbb{C}/\Lambda$ are given by local sections of ξ. Let $z \in \mathbb{C}$ and $U \subseteq \mathbb{C}$ containing z an open set such that $\xi|_U$ is injective. Let ψ be a chart of E which we can suppose (up to shrinking U) to be defined on $\phi(\xi(U))$. Depending on the value of $P = \phi(\xi(z))$, ψ will be of one of the three forms as described in the proof of Proposition 4.2. We get that

$$\psi \circ \phi \circ \xi = \begin{cases} \wp & \text{if } P \neq O \text{ and } \wp'(z) \neq 0 \\ \wp' & \text{if } P \neq O \text{ and } \wp'(z) = 0 \\ \frac{\wp}{\wp'} & \text{if } P = O \end{cases}$$

and hence $\psi \circ \phi \circ \xi$ is holomorphic (and seen as a map to its image, it is bijective, and hence biholomorphic). Since ϕ is bijective and locally biholomorphic, it is biholomorphic and hence an isomorphism of Riemann surfaces.

Finally, we want to show that ϕ is a group homomorphism. Let $z_1, z_2 \in \mathbb{C}$, then from 4.13, there exists a function $f \in \mathbb{C}(\Lambda)$ with divisor

$$\operatorname{div}(f) = (z_1 + z_2) - (z_1) - (z_2) + (0)$$

Now, by 4.10, we can write $f(z) = F(\wp(z), \wp'(z))$ for some rational function $F(X, Y) \in \mathbb{C}(X, Y)$. We can see F in

$$\mathbb{C}(E) = \mathbb{C}(E \cap \mathbb{A}^2) = \operatorname{Frac}\left(\mathbb{C}[x, y]/(y^2 - 4x^3 + g_2 x + g_3)\right)$$

and hence $f = F \circ \phi$. It follows that

$$\operatorname{div}(F) = (\phi(z_1 + z_2)) - (\phi(z_1)) - (\phi(z_2)) + (0)$$

By Proposition 2.7, it follows that

$$\phi(z_1 + z_2) = \phi(z_1) + \phi(z_2)$$

□

The following theorem (which we will not prove) gives the converse to 4.16

Theorem 4.17. *Let $E/\mathbb{C}$ be a non-singular curve given by the equation*

$$E : y^2 = 4x^3 - ax - b.$$

Then there exists a lattice $\Lambda \subseteq \mathbb{C}$ unique up to homothety, such that $a = g_2(\Lambda)$ and $b = g_3(\Lambda)$

4.4 Homology Groups of Elliptic Curves

Since any elliptic curve is isomorphic to a curve given by an equation as in 4.17, we deduce that all curves are homeomorphic to a torus $\mathbb{T}^2$. This allows us to calculate its homology groups.

To calculate the homology groups of a torus, we will use simplicial homology, as in [Hat01, §2.1]. The torus can be given a Δ-complex structure as in Figure 2.

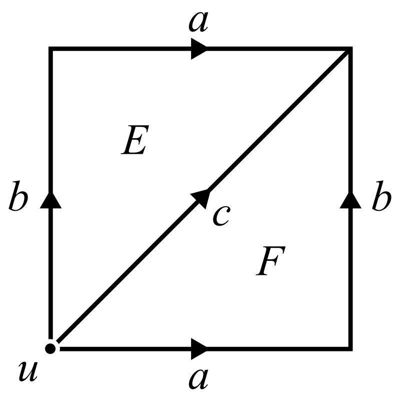

Figure 2: Δ-complex structure of a torus

The associated chain complex for taking simplicial homology is

$$\cdots \longrightarrow 0 \longrightarrow E\mathbb{Z} \oplus F\mathbb{Z} \xrightarrow{\partial_2} a\mathbb{Z} \oplus b\mathbb{Z} \oplus c\mathbb{Z} \xrightarrow{\partial_1} u\mathbb{Z} \longrightarrow 0$$

$$a, b, c \longmapsto 0$$

$$E, F \longmapsto a + b - c$$

Hence we get that

$$\begin{aligned}
&H_0(\mathbb{T}^2) \cong \mathbb{Z}, \\
&H_1(\mathbb{T}^2) = \ker \partial_1 / \operatorname{im} \partial_2 = a\mathbb{Z} \oplus b\mathbb{Z} \oplus c\mathbb{Z}/(a + b - c)\mathbb{Z} \cong \mathbb{Z}^2, \\
&H_2(\mathbb{T}^2) = \ker \partial_2 = (E - F)\mathbb{Z} \cong \mathbb{Z},
\end{aligned}$$

and $H_n(\mathbb{T}^2) = 0$ for $n \geq 3$. We deduce that the associated Betti numbers are

$$\begin{aligned}
b_0(\mathbb{T}^2) &= \operatorname{rk}(\mathbb{Z}) = 1, \\
b_1(\mathbb{T}^2) &= \operatorname{rk}(\mathbb{Z}^2) = 2, \\
b_2(\mathbb{T}^2) &= \operatorname{rk}(\mathbb{Z}) = 1,
\end{aligned}$$

and $b_n(\mathbb{T}^2) = 0$ for $n \geq 3$.

Now if E is given by a Weierstrass equation defined over a number field embedded in $\mathbb{C}$ and can be reduced modulo p such that the curve $C/\mathbb{F}_q$ obtained is a good reduction (i.e. an elliptic curve), these Betti numbers coincide with the degrees of the polynomials that appear in the decomposition of $Z(C/\mathbb{F}_q)$, which was calculated in Theorem 3.4. This shows that part (e) of the Weil Conjectures (3.2) holds for the case of elliptic curves given by a Weierstrass equation.

References

[AM69] M. F. Atiyah and I. G. MacDonald. *Introduction to Commutative Algebra*. Addison-Wesley Publishing Company, 1969.

[Har77] Robin Hartshorne. *Algebraic Geometry*. Springer Science+Business Media, Inc., 1977.

[Hat01] Allen Hatcher. *Algebraic Topology*. Cambridge University Press, 2001.

[Sil09] Joseph H. Silverman. *The Arithmetic of Elliptic Curves*. Springer, New York, NY, 2 edition, 2009.