Elliptic Curves over $\mathbb{C}$ and over Finite Fields

Matthew Dupraz

May 12, 2022

Contents

Introduction

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 algebraically closed, unless stated otherwise.

1 Algebraic Varieties

The 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

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

Notation. Thanks to the above isomorphism, we can see $\mathbb{A}^n$ as a chosen $U_i \subset \mathbb{P}^n$. Hence we can see any affine variety $V \subseteq \mathbb{A}^n$ as a subset of $\mathbb{P}^n$. Similarly, if $V \subseteq \mathbb{P}^n$ is a projective variety, then for a chosen $\mathbb{A}^n \subseteq \mathbb{P}^n$, $V \cap \mathbb{A}^n$ is an affine variety.

Definition 1.1. For $V \subseteq \mathbb{P}^n$ a subset, we define $\overline{V}$ the (Zariski) *closure*, the closure of V in the Zariski topology of $\mathbb{P}^n$.

Proposition 1.1. *1. For V an affine variety, $\overline{V}$ is a projective variety, and*

$$V = \overline{V} \cap \mathbb{A}^n.$$

2. Let V be a projective variety. Then $V \cap \mathbb{A}^n$ is an affine variety, and either

$$V \cap \mathbb{A}^n = \emptyset \text{ or } V = \overline{V \cap \mathbb{A}^n}$$

Proof. 1. Follows from Lemma 3.5 from the course "Algebraic curves".

2. Suppose $V \cap \mathbb{A}^n \neq \emptyset$. We have that $V \supseteq V \cap \mathbb{A}^n$ and V is closed, hence $V \supseteq \overline{V \cap \mathbb{A}^n}$. $V \setminus \mathbb{A}^n$ is closed, and

$$V = \overline{V \cap \mathbb{A}^n} \cup (V \setminus \mathbb{A}^n).$$

By irreducibility of V and the fact $V \cap \mathbb{A}^n \neq \emptyset$ and so $V \neq (V \setminus \mathbb{A}^n)$, we get $V = \overline{V \cap \mathbb{A}^n}$.

□

Definition 1.2. 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 $n - \dim(V)$. If V is non-singular at every point, then V is *non-singular*, or *smooth*.

Definition 1.3. Let $V \subseteq \mathbb{P}^n$ be a projective variety, $P \in V$ and choose $\mathbb{A}^n \subseteq \mathbb{P}^n$ such that $P \in \mathbb{A}^n$. Then V is *non-singular*, or *smooth* at P if $V \cap \mathbb{A}^n$ is smooth at P (as an affine variety).

Proposition 1.2. *Let $V \subseteq \mathbb{P}^n$ be a projective variety, for any $\mathbb{A}^n \subseteq \mathbb{P}^n$, $K(V) = K(V \cap \mathbb{A}^n)$.*

Proof. Follows from Proposition 3.11 from the course "Algebraic curves". □

Definition 1.4. 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

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

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

Definition 1.5. 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

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

Proposition 1.3. *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, $q(gf_0, \dots, gf_m)(P) = q(\phi(P)) \neq 0$ and hence we deduce that $f \circ \phi$ is regular. This implies that ϕ is a morphism. □

2 Algebraic Curves

2.1 Basic properties

By a *curve* we always mean a projective variety of dimension one.

Proposition 2.1. *Let C be a curve and $P \in C$ a smooth point. Then $K[C]_P$ is a discrete valuation ring.*

Definition 2.1. Let C be a curve and $P \in C$ a smooth point. The *valuation* on $K[C]_P$ is given by

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

We extend this definition to $K(C)$ using

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

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 $\mathfrak{m}_P$)

Proposition 2.2. *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.*

Theorem 2.3. *Let $\phi : C_1 \to C_2$ be a morphism of curves. Then ϕ is either constant or surjective.*

Definition 2.2. 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*

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

Definition 2.3. 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.

Definition 2.4. 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 $I(C^{(q)})$,

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

2.2 Divisors

Definition 2.5. 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

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

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

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

Definition 2.6. Let C be a smooth curve and $f \in K(C) \setminus \{0\}$. We associate to f the divisor $\mathrm{div}(f)$ given by

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

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.

Definition 2.7. 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.

Definition 2.8. The *divisor class group* of a curve C, denoted $\mathrm{Cl}(C)$, is the quotient $\mathrm{Div}(C)/\mathrm{PDiv}(C)$. Principal divisors have degree 0 and hence it makes sense to speak about the degree of elements in $\mathrm{Cl}(C)$. The sugroup of elements of $\mathrm{Cl}(C)$ of degree 0 is denoted $\mathrm{Cl}^0(C)$.

Definition 2.9. A divisor $D = \sum n_P(P) \in \mathrm{Div}(C)$ is *positive* (or *effective*), denoted by $D \geq 0$, if $n_P \geq 0$ for all $P \in C$. For two divisors $D_1, D_2 \in \mathrm{Div}(C)$, we write $D_1 \geq D_2$ to indicate that $D_1 - D_2$ is positive.

Definition 2.10. 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 finite-dimensional. We denote its dimension by

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

We now state (without proof) a corrolary of the Riemann-Roch theorem, which will be useful in the following chapters.

Theorem 2.4 (Riemann-Roch)**.** *Let C be a smooth curve of genus g. Let $D \in \mathrm{Div}(C)$, then if $\deg(D) > 2g - 2$, we have that*

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

3 Basic Definitions and Facts

3.1 Weierstrass Equation

Our main interest are *elliptic curves*, which are curves in $\mathbb{P}^2$ of genus 1. These are characterized by the homogeneous equation

$$Y^2Z + aXYZ + bYZ^2 = X^3 + cX^2Z + dXZ^2 + eZ^3 \tag{1}$$

for some $a, b, c, d, e \in \mathbb{F}$. Setting $U_Z = \{[X, Y, Z] \in \mathbb{P}^2 \mid Z \neq 0\}$, we can study the solutions of (1) on U_Z using the change of coordinates $x = X/Z$ and $y = Y/Z$. We obtain the following equation

$$y^2 + axy + by = x^3 + cx^2 + dx + e \tag{2}$$

We can further simplify this equation with linear changes of variables. First notice that if $\mathrm{char}(\mathbb{F}) \neq 2$, the left hand side can be written as

$$\begin{aligned} y(y + ax + b) &= (y + \frac{1}{2}(ax + b) - \frac{1}{2}(ax + b))(y + \frac{1}{2}(ax + b) + \frac{1}{2}(ax + b)) \\ &= (y + \frac{1}{2}(ax + b))^2 - \frac{1}{4}(ax + b)^2 \end{aligned}$$

Hence by replacing y with $y + \frac{1}{2}(ax + b)$ and collecting the terms in each monomial, we get an equation of the form

$$y^2 = x^3 + \alpha x^2 + \beta x + \gamma \tag{3}$$

If $\mathrm{char}(\mathbb{F}) \neq 3$, we can also get rid of the term in x^2 with a linear change of variables. replacing x with $x - \frac{1}{3}\alpha$ yields

$$\begin{aligned} y^2 &= (x - \frac{1}{3}\alpha)^3 + \alpha(x - \frac{1}{3}\alpha)^2 + \beta(x - \frac{1}{3}\alpha) + \gamma \\ &= x^3 - \alpha x^2 + \frac{1}{3}\alpha^2 x - \frac{1}{27}\alpha^3 + \alpha x^2 - \frac{2}{3}\alpha^2 x + \frac{1}{9}\alpha^3 + \beta x - \frac{1}{3}\alpha\beta + \gamma \end{aligned}$$

Collecting the terms in each monomial, we get an equation of the form

$$y^2 = x^3 + Ax + B \tag{4}$$

with $A, B \in \mathbb{F}$. Plugging back the substitutions $x = X/Z$ and $y = Y/Z$, we obtain the homogeneous equation

$$Y^2Z = X^3 + AXZ^2 + BZ^3 \tag{5}$$

3.2 Singularities

We suppose $\mathbb{F}$ is algebraically closed.

We have that an elliptic curve $V \subset \mathbb{P}_2(\mathbb{F})$ is the projective variety

$$V = V(X^3 + AXZ^2 + BZ^3 - Y^2Z) = V(F) \tag{6}$$

We are interested in the case where the curve is smooth. By the regular preimage theorem, V is smooth if all its points are non-singular, i.e. if for all $P = [x, y, z] \in V$,

$$\nabla F(P) = \begin{bmatrix} 3x^2 + Az^2 \\ -2yz \\ 2Axz + 3Bz^2 - y^2 \end{bmatrix} \neq 0$$

If $P = [0, 1, 0]$, then

$$\nabla F(P) = \begin{bmatrix} 0 \\ 0 \\ -1 \end{bmatrix} \neq 0$$

hence the point at infinity is never singular. It follows that when looking for singularities, we can consider just the case where $z \neq 0$, since else we have necessarily $x = 0$ and so $P = [0, 1, 0]$. So if there are any singularities of V, they are on $V \cap U_Z$. So V is non-singular precisely when $V \cap U_Z$ is non-singular. Using the isomorphism $V \cap U_Z \to W, [X, Y, Z] \mapsto (\frac{X}{Z}, \frac{Y}{Z})$ it suffices to study singularities on $W = V(x^3 + Ax + B - y^2) = V(f)$

Let $\Delta = 4A^3 + 27B^2$ be the discriminant of the polynomial $g(x) = x^3 + Ax + B$, we have the following criteria for the existence of singularities of V.

Proposition 3.1. *W (and equivalently V) is non-singular if and only if $\Delta \neq 0$.*

Proof. Suppose there is a point $P = (x_0, y_0) \in W$ that is singular, then we have

$$\begin{bmatrix} 3x_0^2 + A \\ -2y_0 \end{bmatrix} = 0$$

Hence we have that $g'(x_0) = 3x_0^2 + A = 0$ and $y_0 = 0$. In particular, since $P \in W$, also $g(x_0) = 0$, and hence since $g(x_0) = g'(x_0) = 0$, x_0 is a double root of g and so the discriminant $\Delta = 4A^3 + 27B^2$ of g is zero.

Suppose instead that $\Delta = 0$, then g admits a double root $x_0 \in \mathbb{F}$ (since we supposed $\mathbb{F}$ algebraically closed) which is unique since g is a cubic polynomial. Then $P = (x_0, 0) \in V$. Furthermore,

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

We have that $3x^2 + A = g'(x) = 0$, hence $\nabla f(P) = 0$ and so W is singular at P. $\square$

3.3 Group Law

Let E be an elliptic curve. 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 $+$ on E as follows.

Definition 3.1. 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 $P + Q$ be the third point of intersection of L' with 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 $m < 0$.

As we have seen, any elliptic curve can be written up to isomorphism under the form

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

Since this isomorphism is induced by linear changes of variables, it sends lines to lines and hence this preserves the group structure on E induced by $+$. Hence in what follows, we consider simply elliptic curves of the above form. Let $F(x, y) = y^2 - x^3 - ax - b$, so that E is given by the equation $F(x, y) = 0$.

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

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

which is clear by inspection of the composition law.

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

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

If $y_P = 0$, L is the line $x = x_P$ 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

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

Finally, we obtain $P + Q = (x_R, -y_R)$.

This can be summarized in the following proposition:

Proposition 3.2. *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*

$$\begin{aligned} x_{[2]P} &= \left(\frac{3x^2 + a}{2y} \right)^2 - 2x \\ &= \frac{x^4 - 2ax^2 - 8bx + a^2}{4(x^3 + ax + b)} \\ y_{[2]P} &= -\frac{3x^2 + a}{2y} x_{[2]P} + \frac{-x^3 + ax + 2b}{2y} \end{aligned}$$

Lemma 3.3. *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 (2.4), 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 $P = Q$. $\square$

Proposition 3.4. *Let E be an elliptic curve. Then E equipped with the group law from 3.1 and $\mathrm{Cl}^0(E)$ are isomorphic. The isomorphism is given by the map*

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

Proof. Let $D \in Div^0(E)$ be a divisor. Since E has genus 1, by the Riemann-Roch theorem (2.4), we have that

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

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

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

we have necessarily that

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

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 3.3.

This allows us to define

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

which sends a divisor $D \in \operatorname{Div}^0(E)$ 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

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

and hence $\sigma(D_1) = \sigma(D_2)$ by 3.3. 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 $\overline{\sigma} : \operatorname{Cl}^0(E) \to E$. Furthermore, clearly $\overline{\sigma} = \kappa^{-1}$.

It remains to show that κ is a group homomorphism. Clearly, $\kappa(O) = 0$, so we have to show that for $P, Q \in E$, $\kappa(P + Q) = \kappa(P) + \kappa(Q)$.

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. We then have that $f/Z \in K(E)$ and since Z intersects E at O with multiplicity 3, we have

$$\operatorname{div}(f/Z) = \sum_{P \in E} \operatorname{ord}_P(f)(P) - \operatorname{ord}_P(Z)(P) = (P) + (Q) + (R) - 3(O).$$

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 addition on E, we have that the third point of intersection of L' with E is $P+Q$. As above, $f'/Z \in K(E)$ and we have

$$\operatorname{div}(f'/Z) = (R) + (O) + (P+Q) - 3(O) = (R) + (P+Q) - 2(O).$$

It follows that

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

And hence

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

□

Corollary 3.4.1. *Let E be an elliptic curve and $D = \sum n_P(P) \in \operatorname{Div}(E)$. 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

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

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,

$$[D] = \left[\sum n_P(P)\right] = \kappa\left(\sum [n_P]P\right) = 0$$

and so $D \sim 0$. □

3.4 Isogenies

Definition 3.2. Let E_1 and E_2 be elliptic curves. An *isogeny* between E_1 and E_2 is a 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.

Definition 3.3. 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.

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

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

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

3.5 The Dual Isogeny

3.6 The Tate Module

3.7 The Weil Pairing

4 Elliptic Curves over $\mathbb{C}$

The goal of this section is to show an elliptic curve is isomorphic to a torus as a Riemann surface.

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

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 $E(\mathbb{C}) \subset \mathbb{P}^2$ will be equipped with the subspace topology.

Proposition 4.1. *Let $E(\mathbb{C}) \subset \mathbb{P}^2$ be an elliptic curve, then $E(\mathbb{C})$ admits the structure of a Riemann surface.*

Proof. Let $y^2 - x^3 - ax - b = f(x, y) = 0$ be the equation defining $E(\mathbb{C})$. So for all $P = (x_P, y_P) \in E(\mathbb{C})$ 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 $U_P = (\mathrm{id} \times g_P)(V_P) \subset E(\mathbb{C})$, is an open subset of $E(\mathbb{C})$. Indeed, $U_P = \pi_x^{-1}(V_P)$, where $\pi_x : E(\mathbb{C}) \setminus \{O\} \to \mathbb{C}, (x, y) \mapsto x$. 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 $P = (x_P, 0) \in E(\mathbb{C})$ 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 $E(\mathbb{C})$ 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 $O = [0, 1, 0] \in E(\mathbb{C})$. To do this, we can look at $E(\mathbb{C})$ in $\{[X, Y, Z] \in \mathbb{P}^2 \mid Y \neq 0\}$ instead. We get that in this copy of $\mathbb{A}^2$, $E(\mathbb{C})$ 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 $P, Q \in E(\mathbb{C}) \setminus \{O\}$, 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 $\mathcal{A} = \{\phi_P \mid P \in E(\mathbb{C})\}$ is holomorphic and so gives $E(\mathbb{C})$ the structure of a Riemann surface. □

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 4.2. 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 4.3. 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.

Proposition 4.2. *An elliptic function with no poles (or no zeros) is constant.*

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.

Proposition 4.3. *Let $f \in \mathbb{C}(\Lambda)$.*

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

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

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

Definition 4.4. (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.

Proposition 4.4. *(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 for $z \in \mathbb{C} \setminus \Lambda$, the series for $\wp(z)$ 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) TO BE ADDED

$\square$

Theorem 4.5. *We have that*

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

Definition 4.5. 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.

Proposition 4.6. *Let $n_1, \ldots, n_r \in \mathbb{Z}$ and $z_1, \ldots, z_n \in \mathbb{C}$, such that*

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

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

$$\operatorname{div}(f) = \sum n_i(z_i).$$

Proposition 4.7. *For all $z \in \mathbb{C} \setminus \Lambda$, we have that*

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

Remark. We write

$$g_2 = g_2(\Lambda) = 60G_4 \text{ and } g_3 = g_3(\Lambda) = 60G_3.$$

Then the equation in 4.7 becomes

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

Theorem 4.8. *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*

$$E : y^2 = 4x^3 - g_2x - g_3$$

then E is an elliptic curve and the map

$$\begin{aligned} \phi : \mathbb{C}/\Lambda &\to E \\ z &\mapsto \begin{cases} [\wp(z), \wp'(z), 1] & \text{if } z \notin \Lambda \\ [0, 1, 0] & \text{if } z \in \Lambda \end{cases} \end{aligned}$$

is a complex analytic isomorphism of complex Lie groups.

Proof. To show E is an elliptic curve, we have to show that it is non-singular. From 3.1 this is the case if and only if the determinant Δ of the polynomial $f(x) = 4x^3 - g_2x - g_3$ 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 4.7 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 4.3 and 4.4, 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 4.7. Let $[x, y, 1] \in E(\mathbb{C})$, then we have that $\wp(z) - x$ is a non-constant elliptic function, so by 4.2, it has a zero $a \in \mathbb{C}$. Hence $\wp(a) = x$ and hence by 4.7,

$$\wp'(a)^2 = f(\wp(a)) = f(x) = y^2.$$

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 Λ. 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 $E(\mathbb{C})$ 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 4.1. 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 4.6, 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 4.5, 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

$$\mathbb{C}(E) = \mathbb{C}(E \cap \mathbb{A}^2) = \mathrm{Frac}\left(\mathbb{C}[x,y]/(y^2 - 4x^3 + g_2 x + g_3)\right)$$

and hence $f = F \circ \phi$. It follows that

$$\mathrm{div}(F) = (\phi(z_1 + z_2)) - (\phi(z_1)) - (\phi(z_2)) + (0)$$

By Proposition **??**, 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 4.8

Theorem 4.9. *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 $b = g_3(\Lambda)$

Since any elliptic curve is isomorphic to a curve given by an equation as in 4.9, 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 1. The associated chain complex for taking simplicial homology is

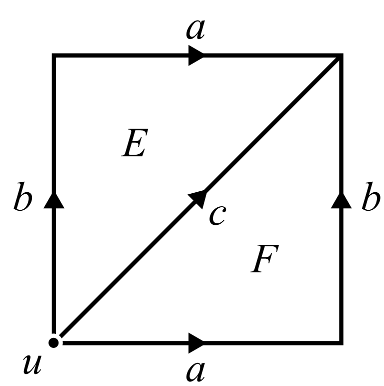

Figure 1: Δ-complex structure of a torus

$$\begin{array}{ccccccccccc} \cdots \longrightarrow 0 \longrightarrow & E\mathbb{Z} \oplus F\mathbb{Z} & \xrightarrow{\partial_2} & a\mathbb{Z} \oplus b\mathbb{Z} \oplus c\mathbb{Z} & \xrightarrow{\partial_1} & u\mathbb{Z} & \longrightarrow 0 \\ & & & a, b, c & \longmapsto & 0 & \\ & E, F & \longmapsto & a + b - c & & & \end{array}$$

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 $n \geq 3$.

5 Elliptic Curves over Finite Fields

For this section we fix a prime p and q a power of p.

Definition 5.1. 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 5.1 (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 $P_0(T) = 1 - T, P_{2n}(T) = 1 - q^n T$ and for each $1 \le i \le 2n-1$, $P_i(T)$ factors (over $\mathbb{C}$) as

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

(b) Functional Equation: The zeta function satisfies

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

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

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

(d) Betti Numbers: If $V/\mathbb{F}_q$ is a 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 of the space of complex points of W.

We will now verify Weil's conjecture for elliptic curves. For this we will make use of the homomorphism $\mathrm{End}(E) \to \mathrm{End}(T_l(E)), \psi \mapsto \psi_l$, where l is a prime different from p. If we fix a $\mathbb{Z}_l$-basis of $T_l(E)$, we can write ψ_l as a 2×2 matrix and so we can compute $\det(\psi_l), \mathrm{tr}(\psi_l) \in \mathbb{Z}_l$.

The following proposition tells us that these quantities are not only independent of the choice of basis, but also of the choice of l.

Proposition 5.2. *Let $\psi \in \mathrm{End}(E)$. Then*

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

In particular, $\det(\psi_l), \mathrm{tr}(\psi_l) \in \mathbb{Z}$

Proposition 5.3. *Let $E/\mathbb{F}_q$ be an elliptic curve, and*

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

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

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

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. Fix v_1, v_2 a $\mathbb{Z}_l$-basis for $T_l(E)$, and write the matrix of ψ_l for this basis as

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

We have the non-degenerate, bilinear, alternating pairing

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

□

Theorem 5.4. *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

$$\begin{aligned} \log Z(E/\mathbb{F}_q; T) &= \sum_{n=1}^{\infty} (\#E(\mathbb{F}_{q^n})) \frac{T^n}{n} \\ &= \sum_{n=1}^{\infty} (q^n + 1 - \alpha^n - \beta^n) \frac{T^n}{n} \qquad (5.3) \\ &= -\log(1 - qT) - \log(1 - T) + \log(1 - \alpha T) + \log(1 - \beta T) \end{aligned}$$

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 (5.3), $|\alpha| = |\beta| = \sqrt{q}$, and

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

$\square$

Hence the Weil conjectures are verified for elliptic curves. Notice that using the notation from theorem 5.1, $\deg P_0 = 1$, $\deg P_1 = 2$, $\deg P_2 = 1$, hence we would expect the Betti numbers of $E/\mathbb{C}$ to coincide with these values, and indeed, these are exactly the Betti numbers we calculated in Section 4.

References

[Hat01] Allen Hatcher. *Algebraic Topology*. Cambridge University Press, 2001.