Elliptic Curves

Yourong Zang

June 22, 2022

Contents

0 Introduction

The main reference of this note is Silverman's *Arithmetic in Elliptic Curves*, and sometimes with examples from *Rational Points on Elliptic Curves* by Silverman & Tate.

Lemma 0.0.1. *Suppose A is an abelian group and $d : A \to \mathbb{Z}$ a positive definite quadratic form. Then*

$$|d(a-b) - d(a) - d(b)| \leqslant 2\sqrt{d(a)d(b)}$$

for all $a, b \in A$.

Proof. If $a = 0$ then we are done. Suppose $a \neq 0$. Let $L(a,b) = d(a,b) - d(a) - d(b)$ which is a $\mathbb{Z}$-bilinear form. Then since d is positive definite, for all $m, n \in \mathbb{Z}$,

$$0 \leqslant d(ma - nb) = m^2 d(a) + mnL(a,b) + n^2 d(b)$$

Let $m = -L(a,b)$ and $n = 2d(a)$. We obtain

$$d(a)\left(4d(a)d(b) - L(a,b)\right) \geqslant 0$$

which gives the result as $a \neq 0$. □

1 More on Curves

1.1 Curves and rational points

We require all varieties in this report to be irreducible.

Definition 1.1.1. A *curve* is a projective variety of dimension 1.

Therefore, we are only interested in projective varieties and most of the objects will be constructed in them. In order to study the rational solutions of a certain type of equations (that is, on some curves), it is important to base all geometric constructions on some algebraically closed extension of the field we are interested in. Say k is a perfect field and K an algebraic closure of k, we denote by $\mathrm{Gal}(K/k)$ the Galois group of K/k (the fixed field of this group is k as K is an algebraic, separable and normal extension of k). We can define a natural group action of $\mathrm{Gal}(K/k)$ on the projective space $\mathbb{P}^n$ over K by $[x_0 : \cdots : x_n]^\sigma = [x_0^\sigma : \cdots : x_n^\sigma]$ for any σ in the Galois group. We introduce the following notations/definitions.

Definition 1.1.2. The *set of k-rational points* $\mathbb{P}^n(k)$ is the set $\{[x_0 : \cdots : x_n] : \forall i, x_i \in k\}$. Given a projective variety V, the *k-rational points of* V is the set $V(k) = V \cap \mathbb{P}^n(k)$.

Definition 1.1.3. A projective variety V is said to be *defined over* k, written as V/k, if $\mathbb{I}(V)$ can be generated by homogeneous polynomials with rational coefficients (i.e., in $k[x_0, \ldots, x_n]$).

Remark 1.1.1. We can also use Galois-theoretic languages:

$$\mathbb{P}^n(k) = \{P \in \mathbb{P}^n : P^\sigma = P, \forall \sigma \in \mathrm{Gal}(K/k)\},$$

and

$$V(k) = \{P \in V : P^\sigma = P, \forall \sigma \in \mathrm{Gal}(K/k)\}$$

as the fixed field of the Galois group is k.

Since we are working with low dimensional cases, it is convenient to define the function field of a projective variety using an affine chart. For any variety W we define

$$k[W] = k[x_0, \ldots, x_n]/\mathbb{I}(W/k)$$

where $\mathbb{I}(W/k) = \mathbb{I}(W) \cap k[x_0, \ldots, x_n]$.

Definition 1.1.4. Given a projective variety V/k, choose some $U_i = \{x_i \neq 0\} \subseteq \mathbb{P}^n$. Define the *function field of* V, $k(V)$, to be the quotient field of $k[V \cap U_i]$ and the *larger function field of* V to be the quotient field of $K[V \cap U_i]$.

Remark 1.1.2. The choice of the chart does not matter — the resulting fields are isomorphic. The elements in $K(V)$ are of the form f/g where f, g are homogeneous polynomials of the same degree in $n+1$ variables, $g \notin \mathbb{I}(V)$.

For some projective variety V, we can define a group action of $\mathrm{Gal}(K/k)$ on $K[V]$ sending $f = \sum a_I x^I$ to $f^\sigma = \sum \sigma(a_I) x^I$, that is, acting on the coefficients of f. We can further extend this group action to $K(V)$ by defining $(f/g)^\sigma = f^\sigma/g^\sigma$. It is easy to check that the invariant sets in $K[V]$ and $K(V)$ are $k[V]$ and $k(V)$ respectively.

Remark 1.1.3. Since $\mathrm{Gal}(K/k)$ consists of field endomorphisms, we have $(f(P))^\sigma = f^\sigma(P^\sigma)$ for all f and points P.

Suppose V_1, V_2 are two projective varieties. For any rational map $\varphi = [f_0 : \cdots : f_n] : V_1 \to V_2$ where $f_i \in K(V_1)$, we define a group action $\varphi^\sigma = [f_0^\sigma : \cdots : f_n^\sigma]$. And by Remark 1.1.3, we get $(\varphi(P))^\sigma = \varphi^\sigma(P^\sigma)$.

Definition 1.1.5. A rational map $\varphi = [f_0 : \cdots : f_n]$ on V is *defined over* k if there exists some nonzero $\lambda \in K$ such that $\lambda f_i \in k(V)$ for all i. Equivalently, $\varphi^\sigma = \varphi$ for all $\sigma \in \mathrm{Gal}(K/k)$.

Definition 1.1.6. For any projective variety V and a smooth point $P \in V$, the maximal ideal at P is $\mathfrak{m}_P = \{f \in K[V] : f(P) = 0\}$. The *local ring of* V *at* P, denoted by $K[V]_P$ is the localization $K[V]_{\mathfrak{m}_P}$ which is simply the local ring

$$K[V]_P = \{f/g : f, g \in K[V] \text{ and } g(P) \neq 0\}$$

A rational function $f \in K(V)$ is said to be regular at P if $f \in K[V]_P$.

These definitions are equivalent to the mostly seen ones, but it would require some nontrivial arguments to prove the equivalence. See [Har10] for instance. They also allow us to do most of our explicit computations on affine coordinate rings, while using the projective varieties to make certain huge theorems work.

Remark 1.1.4. Since for a projective variety V the closure of $V \cap \mathbb{A}^n$ in $\mathbb{P}^n$ is simply V, we will always use the affine variety to represent V and other objects on V.

1.2 Local rings at smooth points

We reproduce Definition 1.1.1 below.

Definition 1.2.1. A *curve* is a projective variety of dimension 1.

In our report, the term curve refers to **smooth** curves, which are curves with all points smooth. Standard algebraic geometry results show that if P is a smooth point of a projective variety V, then the dimension (over K) of $\mathfrak{m}_P/\mathfrak{m}_P^2$ ([Har10]) equals the dimension of V. Thus, given any curve C, we have $\dim_K \mathfrak{m}_P/\mathfrak{m}_P^2 = 1$, which gives us the following commutative algebra result:

Lemma 1.2.1. *For all points P in the curve C, the local ring $K[C]_P$ is a discrete valuation ring with a valuation defined by*

$$\mathrm{ord}_P(f) = \sup\{d \in \mathbb{N} : f \in \mathfrak{m}_P^d\}$$

which is a map $K[C]_P \to \mathbb{N} \cup \{\infty\}$. Furthermore, each valuation ord_P *can be extended to $K(C)$ by* $\mathrm{ord}_P(f/g) = \mathrm{ord}_P(f/1) - \mathrm{ord}_P(g/1)$. *This map is called* the order of f/g at P.

Proof. Prop. 9.2 in [AM94]. □

Remark 1.2.1. The fraction field of a localization of some ring is isomorphic to the fraction field of the original ring. Therefore, $K(C)$ is the fraction field of $K[C]_P$ for any P.

Definition 1.2.2. The *uniformizer for C at P* is some element $t \in K(C)$ such that $\operatorname{ord}_P(t) = 1$.

Remark 1.2.2. There certainly exists a uniformizer: since every discrete valuation ring is a principal ideal domain, $\mathfrak{m}_P = (t)$ for some t, which must be of order one as suggested by commutative algebra results.

If $t \in K(C)$ is of order one, then for any $g \in \mathfrak{m}_P$ (meaning $\operatorname{ord}_P(g) \geqslant 1$), we have

$$\operatorname{ord}_P(g/t) = \operatorname{ord}_P(g) - 1 \geqslant 0$$

so $g/t \in K[C]_P$, meaning there exists some $h \in K[C]_P$ such that $g = th$ and thus $\mathfrak{m}_P = (t)$.

To assist further understandings of this valuation, we present the following example.

Example 1.2.1. Consider the curve $y^2 = x^3 + 2x$ over a field K with characteristic not equal to 2, which is smooth. Let $P = (0,0)$ then $\mathfrak{m}_P = (x, y)$ and $\mathfrak{m}_P^2 = (x^2, xy, y^2)$. Since $x = \frac{1}{2}(y^2 - x^3) \in \mathfrak{m}_P^2$ (this also tells us $\operatorname{ord}_P(x) \geqslant 2$), $\mathfrak{m}_P = (x, y) = (y)$ (in the local ring at P). Thus, $\operatorname{ord}_P(y) = 1$. Now $y^2 = (x^2 + 2)x$ where $x^2 + 2 \neq 0$ at P which means it's a unit in the local ring, $x = (x^2 + 2)^{-1}y^2$ and thus

$$\operatorname{ord}_P(x) = \operatorname{ord}_P(\text{some unit}) + 2\operatorname{ord}_P(y) = 2$$

where the order of unit must be zero by definition (otherwise $\mathfrak{m}_P$ wouldn't be maximal). Finally for $2y^2 - 3x = 2x^3 + x = (2x^2 + 1)x$, we have

$$\operatorname{ord}_P(2y^2 - 3x) = \operatorname{ord}_P(\text{some unit}) + \operatorname{ord}_P(x) = 2$$

where the equality holds since $2x^2 + 1 \neq 0$ at $P = (0,0)$, i.e., $2x^2 + 1$ is a unit.

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

Lemma 1.2.2. *Given curve C/k and $t \in k(C)$ a uniformizer at a smooth $P \in C(k)$. Then $k(C)$ is a finite separable extension of $k(t)$.*

Proof. Since $k(C)$ is a finitely generated k-algebra, Zaraski's lemma ensures it's a finite extension of k. Clearly $k(t)$ has transcendence degree 1 ($t \notin k$ otherwise $\operatorname{ord}_P t = 0$ for all $P \in C$). Now as the transcendence degree of $k(C)/k$ is $\dim C = 1$, $\operatorname{trdeg} k(C)/k(t) = 0$, meaning $k(C)$ is an algebraic extension of $k(t)$.

Take any $x \in k(C)$ and we aim to show x is separable over $k(t)$. Since $k(C)$ is algebraic, there is some $\Phi(X,T) \in k[X,T]$ such that $\Phi(x,t) = 0$. Suppose further that Φ has minimal degree over $k(t)$.

If there is some term $a_{ij}T^iX^j$ in Φ where $p \nmid j$, then clearly $\partial\Phi(t,X)/\partial X$ is nonzero, meaning x is separable.

It remains to check when $\Phi(T,X) = \Psi(T,X^P)$ for some polynomial Ψ. Write

$$\Phi = \Psi(T,X^p) = \sum_{k=0}^{p-1}\left(\sum_{i,j} b_{ijk}T^{ip}X^{jp}\right)T^k$$

Since k is perfect of characteristic $p > 0$, every element of k is a pth power. Thus, define $c_{ijk}^p = b_{ijk}$ and thus

$$\sum_{i,j} b_{ijk}T^{ip}X^{jp} = \sum_{i,j}(c_{ijk}X^iT^j)^p = \left(\sum_{i,j} c_{ijk}X^iT^j\right)^p = \varphi_k(T,X)^p$$

Evaluate the order of each summand:

$$\operatorname{ord}_P(\varphi_k(t,x)^p t^k) = p\operatorname{ord}_P(\cdots) + k\operatorname{ord}_P(t) \equiv k \pmod p$$

which means they have different orders, and thus must all vanish as $\Phi(t,x) = 0$. There must exist some k such that φ_k contains X and $\varphi_k(t,x) = 0$. Yet $\Phi(t,X)$ is minimal and $\deg\varphi_k(t,X)^p \leqslant \deg\Phi(t,X)$ so we get a contradiction. □

Definition 1.2.3. For any point P on a curve C and any $f \in K(C)$, if $\operatorname{ord}_P(f) \geqslant 0$ then f is *regular at* P. If $\operatorname{ord}_P(f) > 0$ then f has *a zero of order* $\operatorname{ord}_P(f)$ *at* P; if $\operatorname{ord}_P(f) < 0$ then f has *a pole of order* $-\operatorname{ord}_P(f)$ *at* P

Remark 1.2.3. If $f = g/h$ is regular at P, then f corresponds to some element of $K[C]_P$, meaning there exist $g', h' \in K[C]$ such that $h' \neq 0$ near P and thus f is regular at P in the usual sense.

The order ord_P at any point P satisfies a very important property, which is an essential part of our algebraic geometry machine.

Theorem 1.2.1. *Let C be a curve and $f \in K(C)$. Then the set $\{P \in C : \operatorname{ord}_P(f) \neq 0\}$ is finite. Furthermore, if f has no poles on C, then $f \in K$.*

Proof. The proof of this theorem by elementary variety theory is rather long and complicated. A short proof using schemes is available in [Har10], II.6.1. □

1.3 Morphisms of curves

Let C_1, C_2 be two (smooth) curves. A rational map $\varphi : C_1 \to C_2$ is a morphism if it's regular at every point on C_1. We present a small lemma as an application of ord. The term regular

Lemma 1.3.1. *Any rational map $\varphi = [f_0 : \cdots : f_m] : C \to V$ from a (smooth) curve to a variety $V \subseteq \mathbb{P}^m$ is a morphism.*

Proof. It suffices to show that for all $P \in C$, there is some $g \in K(C)$ such that each gf_i is regular at P. Let $m = \min_i \operatorname{ord}_P(f_i)$. As Remark 1.2.2 suggests, there is a uniformizer at P, say t, such that $\operatorname{ord}_P(t) = 1$. Then $\operatorname{ord}_P(t^{-m} f_i) \geqslant 0$ for all i, completing the proof. □

If C_1/k and C_2/k, a nonconstant rational map $\varphi : C_1 \to C_2$ defined over k induces an injective pullback $\varphi^* : k(C_2) \to k(C_1)$ fixing k. We quote the following theorem:

Theorem 1.3.1. *Given curves C_1/k and C_2/k, the following statements hold:*

(i) *For any nonconstant rational map φ, $k(C_1)$ is a finite extension of the pullback of $k(C_2)$, that is, $[k(C_1) : \varphi^* k(C_2)] < \infty$.*

(ii) *For any injective field homomorphism $\psi : k(C_2) \to k(C_1)$ fixing k, there is a nonconstant rational map $\varphi : C_1 \to C_2$ such that $\varphi^* = \psi$.*

Proof. The proof is omitted. □

Definition 1.3.1. Suppose $\varphi : C_1 \to C_2$ is a rational map. If φ is constant we define the *degree of* φ, $\deg \varphi$, to be 0 and if φ is nonconstant, then we define

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

In particular, a rational map φ is *separable, inseparable or purely inseparable* if the extension $k(C_1)/\varphi^* k(C_2)$ is.

Definition 1.3.2. We define the *ramification index of φ at P* to be the order

$$e_\varphi(P) = \operatorname{ord}_P\left(\varphi^* t_{\varphi(P)}\right)$$

where $t_{\varphi(P)}$ is any uniformizer at $\varphi(P)$. Note: the choice of t does not matter.

Here are some general facts about the ramification index:

Lemma 1.3.2. *Suppose $\varphi : C_1 \to C_2$ is a nonconstant morphism, then*

(i) *For all* $Q \in C_2$,

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

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

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

where $\deg_s$ *is the separable degree*

$$[\varphi^* k(C_2)^{\text{sep}} : \varphi^* k(C_2)]$$

Furthermore, if $\psi : C_2 \to C_3$ *is another nonconstant map,*

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

Proof. The first two statements are nontrivial and can be found in [Har10].

For the last statement, let t_1, t_2 be uniformizers at at $\varphi(P)$ and $\psi(\varphi(P))$ respectively. Then by definition

$$\text{ord}_{\varphi(P)} \left(t_1^{e_\psi(\varphi(P))} \right) = e_\psi(\varphi(P)) = \text{ord}_{\varphi(P)}(\psi^* t_2)$$

and thus,

$$e_{\varphi \circ \varphi}(P) = \text{ord}_P((\psi \circ \varphi)^* t_2) = \text{ord}_{\varphi(P)}(\varphi^* t_1^{e_\psi(\varphi(P))}) = e_\psi(\varphi(P)) e_\varphi(P)$$

which completes the proof. □

1.4 The Frobenius map

On a field K of characteristic $p > 0$, we have an extremely important map — *the Frobenius endomorphism* $F : x \mapsto x^p$. It is clear that $F(x + y) = F(x) + F(y)$ since the prime p divides all $\binom{p}{k}$ with $0 < k < p$.

Remark 1.4.1. The invariant set of the nth iterate of the Frobenius endomorphism (that is, F^n) is simply $\mathbb{F}_{p^n}$. This property is one of the most essential "reasons" Weil conjectures holds.

Now for any curve C/k with $\text{char}\, k = p > 0$, we can define a new curve $C^{(q)}$ for any $q = p^m$ to be the zero locus of

$$I = \{f^{(q)} : f \in \mathbb{I}(C)\}$$

where $f^{(q)}$ is simply the polynomial resulting from raising the coefficients of f to the qth power.

Definition 1.4.1. Then the map $\varphi : C \to C^{(q)}$ defined by $\varphi = [F^m : \cdots : F^m]$ is called the *qth-power Frobenius map.*

It is easy to check that the image of φ is indeed inside $C^{(q)}$. Say $f(P) = 0$, then

$$f^{(q)}(\varphi(P)) = f^{(q)}(x_0^q, \ldots, x_n^q) = (f(P))^q = 0$$

as k is of characteristic p. The proof of the following theorem is omitted.

Theorem 1.4.1. *We have $\varphi^* k(C^{(q)}) = k(C)^q$ which means φ is purely inseparable. Furthermore,* $\deg \varphi = p$.

Corollary 1.4.1. *Let $\psi : C_1 \to C_2$ be a map between curves over a field of* char $= p > 0$. *Write $q = \deg_i \psi$. Then there exists separable $\lambda : C_1^{(q)} \to C_2$ such that*

$$\psi = \lambda \circ \varphi_q$$

where φ_q is the qth power Frobenius map.

Proof. Let k^{sep} be the separable closure of $\psi^* k(C_2)$ in $k(C_2)$. Then $k(C_1)/k^{\text{sep}}$ is purely inseparable of degree q which means $k(C_1)^q \subseteq k^{\text{sep}}$. But by Theorem 1.4.1,

$$\varphi_q^* k(C_1^{(q)}) = k(C_1)^q, \quad [k(C_1) : \varphi_q^* k(C_1^{(q)})] = q$$

so we must have $k^{\text{sep}} = \varphi_q^* k(C_1^{(q)})$, which means the extensions satisfy

$$k(C_1)/\varphi_q^* k(C_1^{(q)})/\psi^* k(C_2)$$

where $\varphi_q^* k(C_1^{(q)})/\psi^* k(C_2)$ is separable. From (ii) in Theorem 1.3.1, there is a λ separable such that $\lambda \circ \varphi_q = \psi$. □

1.5 Weil divisors and the Picard groups

In this section we introduce an extremely important algebro-geometric tool which would help us in defining and proving many important results. Let C be any curve.

Definition 1.5.1. A *Weil divisor D on C* is a formal sum

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

where only finitely many $n_P \in \mathbb{Z}$ are nonzero. The brackets around each point P only emphasizes that the point here is considered as a part of the formal sum, not an actual point.

The additive abelian group consisting of all Weil divisors on C is called the *divisor group of C*, denoted by $\text{Div}(C)$. The addition inside this group is just the coefficients-wise addition.

The Galois group $\mathrm{Gal}(K/k)$ acts on D by

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

We say that a divisor D is *defined over* k if $D^\sigma = D$ for all $\sigma \in \mathrm{Gal}(K/k)$ and such divisors form a subgroup $\mathrm{Div}_k(C)$.

Definition 1.5.2. We define the *degree of a divisor* D to be

$$\deg D = \sum_{p \in C} n_P$$

which makes sense since there are only finitely nonzero n_P. The subgroup formed by all divisors of degree 0 is denoted by $\mathrm{Div}^0(C)$.

Remark 1.5.1. By definition, $\deg(D_1 + D_2) = \deg D_1 + \deg D_2$ and $\deg(-D) = -\deg D$.

Example 1.5.1. Here we present a trivial example to assist understanding the idea of a formal sum. Say P, Q, S are three distinct points in C. Then let $D_1 = 2(P)+5(Q)$ and $D_2 = -(Q) - 7(S)$. Then $D_1 + D_2$ is nothing else but $2(P) + 4(Q) - (S)$. They do not need to have a specific meaning now. The degree of D_1 is $2 + 5 = 7$.

In the following sections we will refer to Weil divisors as divisors. Given some $f \in K(C)$, we see in Theorem 1.2.1, there are only finitely many points $P \in C$ such $\mathrm{ord}_P(f) \neq 0$. Therefore, the order valuation can be used to define a special type of divisors:

Definition 1.5.3. For any $f \neq 0 \in K(C)$, the *divisor associated to* f is

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

A divisor D on C is a *principal divisor* if there is some $f \neq 0 \in K(C)$ such that $D = \mathrm{div}(f)$.

Remark 1.5.2. Obviously for all $\sigma \in \mathrm{Gal}(K/k)$, we have

$$\begin{aligned}(\mathrm{div}(f))^\sigma &= \sum \mathrm{ord}_P(f)(P^\sigma) \\ &= \sum \mathrm{ord}_{P^\sigma}(f^\sigma)(P^\sigma) \\ &= \sum \mathrm{ord}_P(f^s)(P) = \mathrm{div}(f^\sigma)\end{aligned}$$

where the second equality comes from the fact that $f^\sigma(Q^\sigma) = (f(Q))^\sigma$ for all $Q \in C$ so the order is invariant under σ.

Clearly if $f \in k(C)$, $f = f^\sigma$ so $\operatorname{div}(f) \in \operatorname{Div}_k(C)$.

Lemma 1.5.1. *For any $f \neq 0 \in K(C)$,*

(i) $\operatorname{div} f = 0$ *if and only if* $f \in K^\times$.

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

Two divisors D_1, D_2 are equivalent $D_1 \sim D_2$ if and only if $D_1 - D_2$ is a principal divisor. This equivalence relation gives us a quotient $\operatorname{Div}(C)/\sim$. We denote this group by $\operatorname{Pic}(C)$ and call it the *Picard group of* C. Similarly we denote by $\operatorname{Pic}^0(C)$ the *degree-0 part of the Picard group of* C, that is, $\operatorname{Div}^0(C)/\sim$.

Given a nonconstant map $\varphi : C_1 \to C_2$, we can define the pullback and pushforward map of φ between the divisor groups of C_i as

$$\varphi^* : \operatorname{Div}(C_2) \to \operatorname{Div}(C_2), \quad \varphi^*(Q) = \sum_{P \in \varphi^{-1}(Q)} e_\varphi(P)(P)$$

and

$$\varphi_* : \operatorname{Div}(C_1) \to \operatorname{Div}(C_2), \quad \varphi_*(P) \mapsto (\varphi(P)),$$

and extend them linearly.

Lemma 1.5.2. *The pushforward map φ_* preserves principal divisors and divisors of degree 0. Therefore it defines a homomorphism $\varphi_* : \operatorname{Pic}^0(C_1) \to \operatorname{Pic}^0(C_2)$.*

1.6 Differentials and canonical divisors

The definition we present for differential forms is extremely simple, but it will do the job for us.

Let C be a curve defined on K/k. The *space of differential forms on* C Ω_C is defined to be the $K(C)$-vector space generated by all elements satisfying the following definition:

Definition 1.6.1. A *differential form on* C is an element generated by symbols dx where $x \in K(C)$ such that

(i) $d(x + y) = dx + dy$.

(ii) $d(xy) = xdy + ydx$.

(iii) $dr = 0$ for all $r \in K$.

Remark 1.6.1. Silverman's text contains a typo — Ω_C is not only a K-vector space but also a $K(C)$-vector space.

Every morphism $\varphi : C_1 \to C_2$ induces a pullback of differential forms $\varphi^* : \Omega_2 \to \Omega_1$ defined by

$$\sum f_i dx_i \mapsto \sum \varphi^* f_i d\left(\varphi^* x_i\right)$$

which gives a separability test of φ (which we won't prove):

Lemma 1.6.1. (i) *The space Ω_C is one-dimensional over $K(C)$ for any curve C.*

(ii) *A form dx is a basis of Ω_C if and only if $K(C)/K(x)$ is separable.*

(iii) *Suppose $\varphi : C_1 \to C_2$ is nonconstant, then φ is separable if and only if $\varphi^* : \Omega_2 \to \Omega_1$ is an injective map.*

Suppose $\operatorname{char} k > 0$. Then we have the following theorem.

Theorem 1.6.1. *Let C be a curve, $P \in C$ and $t \in K(C)$ a uniformizer at P. Then for every $\omega \in \Omega_C$, there is a unique $g \in K(C)$, denoted by ω/dt, such that $\omega = g dt$. Furthermore, $\operatorname{ord}_P(g)$ is independent of the choice of t and we denote this quantity by $\operatorname{ord}_P(\omega)$. In particular, $\operatorname{ord}_P(\omega) = 0$ for all but finitely many $P \in C$.*

Proof. The proof of the first statement is easy. By Lemma 1.2.2, $K(C)/K(t)$ is separable so by (ii) in Lemma 1.6.1, dt generates Ω_C and the statement follows. The proofs of the other two statements are omitted. □

Definition 1.6.2. For any $\omega \neq 0 \in \Omega_C$, the divisor associated to ω/dt is called a *canonical divisor*, denoted by $\operatorname{div}(\omega)$. As for rational functions, if $\operatorname{ord}_P(\omega) \geqslant 0$ for all $P \in C$ then we say ω is *holomorphic* and we say it's nonvanishing if $\operatorname{ord}_P(\omega)$ for all $P \in C$.

Remark 1.6.2. All canonical divisors are equivalent in $\operatorname{Pic}(C)$. Take nonzero $\omega_1, \omega_2 \in \Omega_C$, since the latter space is one-dimensional, we have some $f \in K(C)$ such that $\omega_1 = f\omega_2$. In this case $\operatorname{ord}_P(\omega_1) = \operatorname{ord}_P(f) + \operatorname{ord}_P(\omega_2)$ and thus by definition $\operatorname{div}(\omega_1) = \operatorname{div}(f) + \operatorname{div}(\omega_2)$.

1.7 The Riemann-Roch theorem for curves

In this section, we will state the superbly powerful Riemann-Roch theorem without introducing the concept of differentials. This means some objects associated to a curve will not be defined but some of their special properties will be provided.

Given a curve C and a divisor D on C, we say D is *positive* if all $n_P \geqslant 0$. We denote this by $D \geqslant 0$. Given two divisors we write $D_1 \geqslant D_2$ if $D_1 - D_2 \geqslant 0$.

Remark 1.7.1. The definition above might not be so trivial as they seem to be. Given any $f \neq 0 \in K(C)$, if it is regular everywhere except at finitely many points $P_1, \ldots, P_n$ with poles of order less than or equal to $a_1, \ldots, a_n$ (which means $\mathrm{ord}_P(f) \geqslant 0$ for $P \neq P_i$ and $\mathrm{ord}_{P_i}(f) \geqslant -a_i$), we can write

$$\mathrm{div}(f) \geqslant \sum_{i \leqslant n} -a_i(P_i)$$

Similarly, if f has a zero at Q, then one may write $\mathrm{div}(f) \geqslant (Q)$, which is quite convenient.

Also, it is clear that if $D_1 \geqslant D_2$, then $\deg D_1 \geqslant \deg D_2$.

Definition 1.7.1. For a divisor D, define a K-vector space:

$$\mathcal{L}(D) = \{f \neq 0 \in K(C) : \mathrm{div}(f) \geqslant -D\} \cup \{0\}$$

This vector space is actually finite-dimensional (nontrivial result; proof omitted), and we write

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

Lemma 1.7.1. *For any $D \in \mathrm{Div}(C)$,*

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

(ii) *For another $D' \in \mathrm{Div}(C)$, if $D \equiv D'$ in $\mathrm{Pic}(C)$, then $\mathcal{L}(D) \cong \mathcal{L}(D')$ and as a consequence $l(D) = l(D')$.*

Proof. For (i) we quote Lemma 1.5.1. Since $\deg D < 0$ and for any nonzero $f \in K(C)$, $f \in \mathcal{L}(C)$ if $\deg \mathrm{div}(f) \geqslant -\deg D > 0$. Yet the LHS is zero, so $\mathcal{L}(C) = 0$.

For (ii), suppose $D - D' = \mathrm{div}(g)$. We have an isomorphism

$$\alpha : \mathcal{L}(D) \to \mathcal{L}(D')$$

defined by $f \mapsto fg$ (one only needs to check that this map and its inverse $f \mapsto f/g$ are both well-defined, which is an easy argument on orders). □

Let K_C be a canonical divisor. By Remark 1.6.2, when dealing with the $\mathcal{L}$ space of these divisors, we can always use the notation K_C to represent any canonical divisor on C as $l(K_C)$ are always the same.

Theorem 1.7.1 (Riemann-Roch)**.** *Let C be a curve and K_C the canonical divisor on C. There is an integer $g \geqslant 0$ called the* genus of C *such that for any $D \in \mathrm{Div}(C)$,*

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

Proof. Proof omitted. See [Har10] for example. □

Remark 1.7.2. The term $l(K_C - D)$ is sometimes called the correction term. Since $l(K_C - D) \geqslant 0$ for any D, we have

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

which is called Riemann's inequality.

Corollary 1.7.1. *The followings hold:*

(i) $l(K_C) = g$.

(ii) $\deg K_C = 2g - 2$ *(which is $-\chi$ where χ is the Euler characteristic of C).*

(iii) *If* $\deg D > 2g - 2$*, then* $l(D) = \deg D - g + 1$

Proof. For (i) take $D = 0$ then by Remark 1.7.1 any $f \in \mathcal{L}(D)$ has no poles, i.e., they are just constants by Theorem 1.2.1. Thus, $\mathcal{L}(D) = K$ and therefore $l(D) = \dim_K K = 1$. Plugging this into Riemann-Roch we get the result.

For (ii) take $D = K_C$. Then $l(D) = g$ and thus $l(D) - l(0) = \deg K_C - g + 1$. Since $l(0) = 1$ we get $\deg K_C = 2g - 2$.

For (iii), $\deg D > 2g - 2$ together with (ii) suggests $\deg(K_C - D) < 0$. Thus, $\mathcal{L}(K_C - D) = 0$ by Lemma 1.7.1. This means $l(D) = \deg D - g + 1$. □

2 More on Elliptic Curves

2.1 Curves of genus one

In this section we present a more abstract definition of elliptic curves, and show that this definition is equivalent to the one using Weierstrass normal forms.

Definition 2.1.1. An *elliptic curve* is a pair $(E, \mathcal{O})$ where E is a (smooth) curve of genus 1 and $\mathcal{O} \in E$. We say that E *is defined over* k if E/k and $\mathcal{O} \in E(k)$.

Remark 2.1.1. The selected k-rational base point $\mathcal{O}$ is extremely important in the definition of elliptic curves. There are several reasons for taking it: first, many smooth projective curves of genus one does NOT have rational points. For example, the curve $y^2 = 1 - 17x^4$ has no rational points (and it violates the Hasse principle) over $\mathbb{Q}$ [Poo99]. Second, we need the rationality of this base point to generate the $\mathcal{L}$-space of $n(\mathcal{O})$ with elements in $k(C)$, see the proof of (i) in Theorem 2.1.1; we want that, for all elliptic curves defined above, there is some Weierstrass equation with k-rational coefficients.

Theorem 2.1.1. *Suppose E/k is an elliptic curve with a base point $\mathcal{O}$, then*

(i) *There exists $f, g \in k(E)$ such that the map*

$$\varphi : E \to \mathbb{P}^2, \quad P \mapsto [f(P) : g(P) : 1]$$

is an isomorphism onto a curve given by some Weierstrass equation

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

with k-rational coefficients and $\varphi(\mathcal{O}) = [0 : 1 : 0]$. In this case, f, g are called the Weierstrass coordinate of E.

(ii) *Any two Weierstrass equations of E are related by a linear change of variables.*

(iii) *All curves defined by Weierstrass equations with k-rational coefficients are elliptic curves with the base point $[0 : 1 : 0]$.*

Proof. We only prove (i) partially and omit the remaining.

(i) For E, $2g - 2 = 0$ so $\deg n(\mathcal{O}) = n > 2g - 2$ for all $n \geqslant 1$. Then by Corollary 1.7.1 (iii), $l(n(\mathcal{O})) = n$. Let $\{1, f\} \subseteq k(E)$ (we can take the fact that if $D \in \mathrm{Div}_k(C)$ then $\mathcal{L}(D)$ has a basis of elements in $k(C)$) be a basis of $\mathcal{L}(2(\mathcal{O}))$, and extending it to a basis $\{1, f, g\}$ of $\mathcal{L}(3(\mathcal{O}))$. Here $\mathrm{ord}_{\mathcal{O}}(f) = -2$ and $\mathrm{ord}_{\mathcal{O}}(g) = -3$ (proof omitted). Now f^2, f^3, fg, g^2 all have order $\geqslant -6$ at $\mathcal{O}$, so they are all in $\mathcal{L}(6(\mathcal{O}))$. But then we would have seven functions $\{1, f, g, f^2, f^3, fg, g^2\}$ in a K-vector space of dimension 6 (so its dimension over k must be at most 6). Thus, there are $A_1, \ldots, A_7 \in k$ such that

$$A_1 + A_2f + A_3g + A_4f^2 + A_5fg + A_6g^2 + A_7f^3 = 0$$

where $A_6, A_7 \neq 0$ or else all elements remaining will have different orders at $\mathcal{O}$. Replace f, g by $-A_6A_7f$ and $A_6A_7^2g$,

$$A_1 - A_2A_6A_7f + A_3A_6A_7^2g - A_4A_6^2A_7^2f^2 - A_5A_6^2A_7^3fg + A_6^3A_7^4g^2 - A_6^3A_7^4f^3 = 0$$

and rescaling gives us the map

$$\varphi : P \mapsto [f(P) : g(P) : 1]$$

under which $\operatorname{im}\varphi$ is contained in some zero locus V of an Weierstrass equation. However since φ is nonconstant and it's a morphism as E is smooth, it must be surjective (standard algebraic geometry result). Thus, $\operatorname{im}\varphi = V$ is defined by an Weierstrass equation.

By definition, the pullback of $k(C)$ under φ is just $k(f, g)$. We claim that $[k(E) : k(x, y)] = \deg\varphi = 1$. Since the orders of f, g at $\mathcal{O}$ are $-2, -3$ respectively, $[k(E) : k(f)] = 2$, $[k(E) : k(g)] = 3$. This means $\deg\varphi$ must divide two coprime numbers and thus it's one. We will take for granted that $\operatorname{im}\varphi$ is smooth, and morphisms between smooth curves of degree 1 are isomorphism. Thus, φ is an isomorphism.

(ii) Suppose $\{f, g\}, \{f', g'\}$ are two sets of Weierstrass coordinates, then $\{1, f\}$, $\{1, f'\}$ ($\{1, f, g\}$,$\{1, f', g'\}$) are both bases of $\mathcal{L}(2(\mathcal{O}))$ ($\mathcal{L}(3(\mathcal{O}))$). We therefore have $u_1, u_2 \in k^\times$ and $r, t, s_2 \in k$ such that

$$x = u_1x' + r, \quad y = u_2y' + s_2x' + t.$$

Yet, x, y satisfy the Weierstrass equation so $u_1^3 = u_2^2$ and after a change of variables, we get the result.

(iii) Recall that every curve defined by a Weierstrass equation we have a nonzero, regular, nonvanishing differential form called the invariant differential:

$$\omega = \frac{dx}{2y - a_1x + a_3}$$

Since we know that it's regular and nonvanishing, we get a canonical divisor $K_E = \operatorname{div}(\omega) = 0$. Thus, by (ii) in Corollary 1.7.1, we get

$$0 = \deg K_E = 2g - 2$$

which means the curve E has genus one, completing the proof. □

2.2 The algebraic group law

Recall in Section 1.5, we defined something call the Picard group of a curve, by modding out principal divisors from the group of divisors. In this section we use the subgroup $\mathrm{Pic}^0(E)$ to derive a group structure on E. To prepare for the main construction, we start with an easy lemma

Lemma 2.2.1. *Suppose E is an elliptic curve. Then for any two points $P, Q \in E$, $(P) \sim (Q)$ if and only if $P = Q$.*

Proof. Let $f \neq 0 \in K(C)$ such that $\mathrm{div}(f) = (P) - (Q)$. Clearly $\mathrm{div}(f) \geqslant -(Q)$ so $\mathrm{div}(f) \in \mathcal{L}((Q))$. But since the genus of E is $g = 1$, $\deg(Q) = 1 > 2g - 2$. Thus, by Corollary 1.7.1 (iii), $l((Q)) = \deg(Q) = 1$. Therefore, as $1 \in \mathcal{L}((Q))$, $f \in K$ and $\mathrm{div}(f) = 0$. This means $P = Q$ (otherwise the formal sum cannot cancel). □

Consider any divisor $D \in \mathrm{Div}^0(E)$ of degree 0. We have $l(D + (\mathcal{O})) = \deg(D + (\mathcal{O})) = 1$ by Corollary 1.7.1 (iii). Let f be a nonzero element of $K(E)$ that spans $\mathcal{L}(D+(\mathcal{O}))$. Then we have $\mathrm{div}(f) \geqslant -D-(\mathcal{O})$. But by Lemma 1.5.1, $\deg \mathrm{div}(f) = 0$, we have some $P \in E$ such that $\mathrm{div}(f) = -D - (\mathcal{O}) + (P)$ To deduce the last statement, We must think about the formal sum. The inequality above tells us that the coefficients in $\mathrm{div}\, f$ before (Q) and each term in D must be larger than -1 and the coefficient of each term in $-D$; but the coefficient before $\mathcal{O}$ in $\mathrm{div}(f)$ cannot be positive, otherwise we cannot cancel it in the degree, as the other coefficients must be nonnegative. Thus the degree of $\mathrm{div}(f) = 0$ suggests that there is one single point (or else the degree of the part other than $-D - (\mathcal{O})$ would be ¿1, which is impossible to cancel in $\deg \mathrm{div}(f)$) such that $\mathrm{div}(f) = -D - (\mathcal{O}) + (P)$ (it could be $\mathcal{O}$ of course). Then if P' is another such point, we have $(P') \sim D + (\mathcal{O}) \sim (P)$ which by Lemma 2.2.1 gives $P = P'$.

Let $\sigma : \mathrm{Div}^0(E) \to E$ be the map sending D to the unique point P found above.

Theorem 2.2.1. *The map σ induces a bijection $\sigma : \mathrm{Pic}^0(E) \to E$, with its inverse being $\kappa : E \to \mathrm{Pic}^0(E)$ defined by $P \mapsto [(P) - (\mathcal{O})]$. Therefore we can impose E with a group structure by defining*

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

Proof. For any point $P \in E$, the divisor $(P) - (\mathcal{O})$ has degree 0. Therefore by construction $\sigma((P) - (\mathcal{O})) = P$, which means σ is surjective.

We now prove that $\sigma(D_1) = \sigma(D_2)$ if and only if $D_1 \sim D_2$. Suppose $P = \sigma(D_1) = \sigma(D_2)$. Then $D_i \sim (P) - (\mathcal{O})$ imply $D_1 - D_2 \sim (P) - (P) = 0$ and

thus $D_1 \sim D_2$. Conversely if $D_1 \sim D_2 \sim (P) - (\mathcal{O})$ for a unique P, by definition, $\sigma(D_1) = \sigma(D_2) = P$. Thus, we have a bijection:

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

and the inverse map is deduced when we proved σ's surjectivity. □

Theorem 2.2.2. *The algebraic group law and the geometric group law defined on an elliptic curve are the same thing.*

Proof. It suffices to show that $\kappa(P+Q) = \kappa(P) + \kappa(Q)$ (where the first addition is the addition from the geometric group law). Let $L = \mathbb{V}(f)$ be the line passing through P, Q; let R be the third point of intersection of this line and E; let $L' = \mathbb{V}(f')$ be the line passing through $R, \mathcal{O}$. Then since $Z = 0$ intersects with E at $\mathcal{O}$ with multiplicity 3 (so that $\mathrm{ord}_{\mathcal{O}}(Z) = 3$), we have

$$\mathrm{div}(f/Z) = (P) + (Q) + (R) - 3(\mathcal{O}), \quad \mathrm{div}(f'/Z) = (R) + (P+Q) + (\mathcal{O}) - 3(\mathcal{O})$$

where we know for example $\mathrm{ord}_P(f) = 1$ since f is a polynomial of degree 1 and the maximal ideal $\mathfrak{m}_P$ is generated by some nonconstant polynomial so we cannot have $f \in \mathfrak{m}_P^d$ for any $d > 1$. This means

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

which is principal so equivalent to 0. But in $\mathrm{Pic}^0(E)$,

$$\kappa(P+Q) - \kappa(P) - \kappa(Q) = (P+Q) - (\mathcal{O}) - (P) + (\mathcal{O}) - (Q) + (\mathcal{O}) \equiv 0$$

which completes the proof. □

Corollary 2.2.1. *Given a divisor $D \in \mathrm{Div}(E)$, it is principal if and only if*

$$\deg D = 0, \quad \sum [n_p]P = 0$$

where we write $D = \sum n_P(P)$.

Proof. If D is principal then by Lemma 1.5.1, $\deg D = 0$. Also, using the σ map defined in Theorem 2.2.1, we have $D \sim 0$ implies $\sigma([D]) = \mathcal{O}$ which means

$$\sum [n_P]\sigma[(P) - (\mathcal{O})] = \sum [n_P]P = \mathcal{O}$$

where we used the definition that $\sigma[(P) - (\mathcal{O})] = P$.

Now if $D \in \mathrm{Div}^0(E)$ and $\sum [n_P]P = \mathcal{O}$, then $\sigma(D) = \mathcal{O}$ and thus $D \sim 0$. □

Lemma 2.2.2. *The addition and negation map on an elliptic curve are morphisms of elliptic curves.*

Proof. Simply use the explicit formulas. □

3 Constructions on Elliptic Curves

In this section we talk about several important objects on elliptic curves.

3.1 Isogenies

Definition 3.1.1. Given two elliptic curves E_1, E_2, a morphism $\varphi : E_1 \to E_2$ is an *isogeny* if it preserves the base point, that is, $\varphi(\mathcal{O}) = \mathcal{O}$. Two elliptic curves are called *isogenous* if there is a nonconstant isogeny from E_1 to E_2.

Remark 3.1.1. If $\varphi \neq [0]$ (where $[0]$ is the trivial isogeny sending everything to $\mathcal{O}$) is an isogeny, then φ is surjective. We define the degrees of φ as before. We define $\deg[0] = 0$ so that we would have $\deg(\psi \circ \varphi) = \deg\psi \deg\varphi$.

Let the Hom-space of elliptic curves to be $\mathrm{Hom}(E_1, E_2) = \{\text{isogeny } : E_1 \to E_2\}$ and $\mathrm{End}(E) = \mathrm{Hom}(E_1, E_2)$.

Definition 3.1.2. The *multiplication-by-m isogeny* $[m]$ is the map sending P to the sum of $|m|$ numbers of $\mathrm{sgn}(m)P$.

The proof of the following lemma is tedious so it is omitted.

Lemma 3.1.1. *The map* $[m]$ *is nonconstant for* $m > 0$.

The abelian group $\mathrm{Hom}(E_1, E_2)$ forms a $\mathbb{Z}$-module by defining $m\varphi = [m] \circ \varphi$. Then if $m\varphi = 0$, $0 = \deg m\varphi = \deg[m] \deg\varphi$. Now if $\deg\varphi \neq 0$ (which means $\varphi = [0]$) then $\deg[m] = 0$ which implies $m = 0$ as $[m]$ is nonconstant for $m > 0$. Thus, $\mathrm{Hom}(E_1, E_2)$ is torsion free. Using the same argument we can show that $\mathrm{End}(E)$ is an integral domain of characteristic 0.

Definition 3.1.3. The *m-torsion subgroup* of E is denoted by $E[m]$. The *torsion subgroup of* E is the union

$$E_{\mathrm{tor}} = \bigcup_{m \geqslant 1} E[m]$$

We use the notation $E[m](k)$ and $E_{\mathrm{tor}}(k)$ to denote the corresponding rational torsion points.

Remark 3.1.2. If a point $P \neq \mathcal{O}$ has order 2, then $[2]P = \mathcal{O}$, which is equivalent to $P = -P$, so $(x, y) = -(x, y) = (x, -y)$, indicating $y = 0$. This shows that the rational points of order 2 are given by $y = 0$, namely $\{\mathcal{O}, (x_1, 0), (x_2, 0), (x_3, 0)\}$, where $x_i \in K$ are (distinct) solutions to the elliptic curve's Weierstrass equation.

If a point $P \neq \mathcal{O}$ has order 3, then $[3]P = \mathcal{O}$, which is equivalent to $[2]P = [-1]P$. This happens if and only if the x-coordinate of P satisfies $x(P) = x([2]P)$. Using the explicit duplication formula, it can be shown that every elliptic curve has exactly nine points of order dividing three, forming a group isomorphic to $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$.

Remark 3.1.3. If $k = \mathbb{F}_q$ and E/k, then the Frobenius map defined in Definition 1.4.1 is an endomorphism since $E^{(q)} = E$ for all $q = p^r$, so it's now called the *Frobenius endomorphism* and denoted by φ_q. The fixed points of this endomorphism are precisely $E(\mathbb{F}_q)$.

Lemma 3.1.2. *Every isogeny $\varphi : E_1 \to E_2$ is a homomorphism of groups.*

Proof. If $\varphi = [0]$ then we are done. Suppose $\varphi \neq [0]$. Then by Lemma 1.5.2, there is a homomorphism $\varphi_* : \mathrm{Pic}^0(E_1) \to \mathrm{Pic}^0(E_2)$ defined by

$$\left[\sum n_P(P)\right] \mapsto \left[\sum n_P(\varphi(P))\right]$$

Recall the isomorphisms $\kappa_i : E_i \to \mathrm{Pic}^0(E_i)$ defined by $P \mapsto [(P) - (\mathcal{O})]$. They satisfy

$$\varphi_*\kappa_1(P) = [(\varphi(P)) - (\varphi(\mathcal{O}))] = [(\varphi(P)) - (\mathcal{O})] = \kappa_2(\varphi(P))$$

since $\varphi(\mathcal{O}) = \mathcal{O}$. Therefore $\varphi = \kappa_2^{-1} \circ \varphi_* \circ \kappa_1$ is a group homomorphism. □

The kernel $\ker \varphi = \varphi^{-1}(\mathcal{O})$ is therefore a subgroup of E_1 and finite by Lemma 1.3.2.

There are two important results on the size of kernel stated below. The proofs of these two results require some complicated constructions that we do not want to know in this report. Therefore, we will take the theorems for granted.

Theorem 3.1.1. *Let $\varphi : E_1 \to E_2$ be an isogeny. Then for all $Q \in E_2$, $\#\varphi^{-1}(Q) = \deg_s \varphi$ and for all $P \in E_1$, $e_\varphi(P) = \deg_i \varphi$. In particular, if φ is separable, $\#\ker \varphi = \deg \varphi$.*

Theorem 3.1.2. *If φ_q is the qth-power Frobenius map on some elliptic curve $E/\mathbb{F}_q$ of characteristic $p > 0$, then all maps $m + n\varphi_q : E \to E$ where $p \nmid m$ are separable.*

Remark 3.1.4. By Theorem 3.1.2, $1 - \varphi_q$ is always separable. Therefore, the fixed points of φ_q, $\{P \in E : (1 - \varphi_q)(P) = \mathcal{O}\}$, has size $\deg(1 - \varphi_q)$.

Remark 3.1.5. For a fixed point $Q \in E$, we define the map $\tau_Q : P \mapsto P + Q$ to be the *translation by Q* morphism. For any morphism $F : E_1 \to E_2$ of elliptic curves, we have

$$\varphi = \tau_{-F(\mathcal{O})} \circ F \in \mathrm{Hom}(E_1, E_2)$$

as $\varphi(\mathcal{O}) = F(\mathcal{O}) - F(\mathcal{O}) = \mathcal{O}$. Therefore, every morphism can be expressed as a composition of a translation and an isogeny.

Still without a proof, we have the following decomposition theorem:

Theorem 3.1.3. *Suppose $\varphi : E_1 \to E_2$ and $\psi : E_1 \to E_3$ are nonconstant isogenies. Further assume that φ is separable and $\ker \varphi \subseteq \ker \psi$. Then there exits a unique $\pi : E_2 \to E_3$ such that $\psi = \pi \circ \varphi$.*

3.2 Dual isogenies

In this section we introduce another important object on elliptic curves. The construction of dual isogenies is not that obvious from a geometric point of view. Consider two elliptic curves E_1, E_2 and a nonconstant isogeny (thus surjective) $\varphi : E_1 \to E_2$. Recall that the isogeny induces an homomorphism $\varphi^* : \mathrm{Pic}^0(E_2) \to \mathrm{Pic}^0(E_1)$ defined by

$$[(Q)] \mapsto \left[\sum_{P \in \varphi^{-1}(Q)} e_\varphi(P)(P) \right]$$

where e_φ is φ's ramification index at P. Now if $\kappa_i : E_i \to \mathrm{Pic}^0(E_i)$ be the bijection we constructed in Section 2.2. Then let's investigate the composition $\kappa_1^{-1} \circ \varphi^* \circ \kappa_2$. Take some $Q \in E_2$ and some P such that $\varphi(P) = Q$. Then

$$\begin{aligned}
\left(\kappa_1^{-1} \circ \varphi^* \circ \kappa_2\right)(Q) &= \left(\kappa_1^{-1} \circ \varphi^*\right)[(Q) - (\mathcal{O})] \\
&= \kappa_1^{-1}\left[\sum [e_\varphi(P')(P')] - \sum [e_\varphi(T)(T)]\right] \\
&= \sum_{P' \in \varphi^{-1}(Q)} [e_\varphi(P')]P' - \sum_{T \in \varphi^{-1}(\mathcal{O})} [e_\varphi(T)]T \\
&= [\deg_i \varphi] \left(\sum_{P' \in \varphi^{-1}(Q)} P' - \sum_{T \in \varphi^{-1}(\mathcal{O})} T \right) \qquad \text{by Theorem 3.1.1} \\
&= [\deg_i \varphi \cdot \# \ker \varphi]P \\
&= [\deg_i \varphi \cdot \deg_s \varphi]P = [\deg \varphi]P \qquad \text{by Theorem 3.1.1}
\end{aligned}$$

where the second last equality holds since all $P' \in \varphi^{-1}(Q)$ are of the form $P + T$ for a distinct $T \in \ker \varphi^{-1}(Q)$. However, we do not know if this composition is an isogeny. Therefore, it is reasonable to construct the following object:

Theorem 3.2.1. *Let $\varphi : E_1 \to E_2$ be an isogeny and $\deg \varphi = m$. Then there exists a unique isogeny $\hat{\varphi} : E_2 \to E_1$, called* the dual isogeny of φ, *such that $\hat{\varphi} \circ \varphi = [m]$.*

Proof. We first prove uniqueness. Suppose $\hat{\varphi}, \hat{\varphi}'$ are two dual isogenies, then

$$(\hat{\varphi} - \hat{\varphi}') \circ \varphi = [m] - [m] = [0].$$

This means $\hat{\varphi} - \hat{\varphi}'$ must be a constant, namely $\hat{\varphi} = \hat{\varphi}'$.

To simplify the proof of existence, we use Corollary 1.4.1. Say $\varphi = \psi \circ \varphi_q$ where φ_q is a Frobenius map of degree q and ψ separable. Suppose φ and ψ are two maps of degree m, n respectively whose dual isogenies exist. Then

$$(\hat{\varphi} \circ \hat{\psi}) \circ (\psi \circ \varphi) = \hat{\varphi} \circ [n] \circ \varphi = [n] \circ \hat{\varphi} \circ \varphi = [nm]$$

where the third equality holds since φ is a homomorphism. By uniqueness, $\widehat{\psi \circ \varphi} = \hat{\varphi} \circ \hat{\psi}$. This means if we can prove that the two maps from the Frobenius decomposition have dual isogeny, then the composition of their dual isogeny is the dual isogeny of the original map.

Case 1: φ is separable. Since φ has degree m, we have $\#\ker\varphi = \deg_s \varphi = \deg\varphi = m$. This suggests the extremely crucial conclusion that every element of $\ker\varphi$ has order dividing $[m]$. Thus, $\ker\varphi \subseteq \ker[m]$. By Theorem 3.1.3, there is a unique $\hat{\varphi}$ such that $[m] = \hat{\varphi} \circ \varphi$.

Case 2: φ is the qth power Frobenius map φ_q with $q = p^e$, then $\varphi_q = \varphi_p^e$. Thus it suffices to reduce to the case pth power Frobenius map. We use the fact that if ω is an invariant differential, then $[m]^*\omega = m\omega$, which means $[p]^*\omega = p\omega = 0$. This means the map $[p]$ is not separable, otherwise it violates (iii) in Lemma 1.6.1. Thus we can decompose $[p] = \psi \circ \varphi_p^d$ for some integer $d \geqslant 1$ (otherwise $[p]$ would be separable!). Then taking $\hat{\varphi} = \psi \circ \varphi_p^{d-1}$, one gets the dual isogeny. □

Lemma 3.2.1. *Suppose $\varphi : E_1 \to E_2$ is an isogeny. Then*

(i) $\varphi \circ \hat{\varphi} = [m]$.

(ii) *If $\psi : E_1 \to E_2$ is another isogeny. Then $\widehat{\varphi + \psi} = \hat{\varphi} + \hat{\psi}$.*

(iii) *For all $m \in \mathbb{Z}$, $\widehat{[m]} = [m]$ which suggests* $\deg[m] = m^2$.

(iv) $\deg\hat{\varphi} = \deg\varphi$ *and* $\hat{\hat{\varphi}} = \varphi$.

Proof. (i) We have $(\varphi \circ \hat{\varphi}) \circ \varphi = \varphi \circ [m] = [m] \circ \varphi$. But since φ is nonconstant, $\varphi \circ \hat{\varphi} = [m]$

(ii) The proof of this part is lengthy and difficult, so we omit it.

(iii) Using (ii), $\widehat{[m+1]} = \widehat{[m]} + \widehat{[1]}$. Yet $[0] \circ [0] = [0] = [\deg[0]]$ so $\widehat{[0]} = [0]$, which gives the base case of the induction. Let $d = \deg[m]$, then $[d] = [m^2]$, which means $d = m^2$ as $\mathrm{End}(E)$ is torsion-free.

(iv), (v) are easy using (iii). □

Remark 3.2.1. Suppose $\operatorname{char} k = p > 0$. We have collected all necessary properties of the isogeny $[m]$. Thus, we could investigate the structure of $E[m]$, which is the kernel of $[m]$. Taking $n = 0$ in Theorem 3.1.2, if $p \nmid m$, then $[m]$ is separable. Thus, by Theorem 3.1.1, $\#E[m] = \#\ker[m] = \deg\,[m] = m^2$. And since p is prime, for every $d \mid m$, we have $p \nmid d$. Thus, $\#E[d] = d^2$. By looking at the classification of $E[m]$ as a finitely generated group, it must follow that $E[m] \cong \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$.

Now consider the case where $m = p^e$ for some $e \geqslant 1$. Then

$$\#E[p^e] = \#\ker[p^e] = \deg_s[p^e] = (\deg_s(\hat{\varphi}_p \circ \varphi_p))^e$$

But since φ_p, the pth power Frobenius map is purely inseparable by Theorem 1.4.1, the RHS equals $(\deg_s(\hat{\varphi}_p)^e$. If $\hat{\varphi}_p$ is inseparable, then $\#E[p^e] = 1$ which implies $E[p^e] = \{\mathcal{O}\} = 0$. If $\hat{\varphi}_p$ is separable, then $\#E[p^e] = p^e$ and writing out $E[p^e]$'s decomposition as a finite group, we get $E[p^e] \cong \mathbb{Z}/p^e\mathbb{Z}$.

Corollary 3.2.1. *For elliptic curves E_1, E_2, the function*

$$\deg : \operatorname{Hom}(E_1, E_2) \to \mathbb{Z}$$

is a positive definite quadratic form.

Proof. By definition $\deg \varphi = 0$ if and only if $\varphi = [0]$ so it is positive definite. Also, we have $\deg(m\varphi) = \deg[m] \cdot \deg \varphi = m^2 \deg \varphi$ for all $m \in \mathbb{Z}$. So it remains to prove that the polar form of deg:

$$\langle \varphi, \psi \rangle = \deg(\varphi + \psi) - \deg \varphi - \deg \psi$$

is $\mathbb{Z}$-bilinear.

Note the map $[] : \mathbb{Z} \to \operatorname{End}(E_1)$ is an injection, so

$$\begin{aligned}
[\langle \varphi, \psi \rangle] &= [\deg(\varphi + \psi)] - [\deg \varphi] - [\deg \psi] \\
&= (\hat{\varphi} + \hat{\psi}) \circ (\varphi + \psi) - \hat{\varphi} \circ \varphi - \hat{\psi} \circ \psi \\
&= \hat{\varphi} \circ \psi + \hat{\psi} \circ \varphi
\end{aligned}$$

Since $\hat{\varphi} \circ \psi$ and $\hat{\psi} \circ \varphi$ are both $\mathbb{Z}$-linear (easy to check) in φ and ψ and [] is an injection, the polar form is $\mathbb{Z}$-bilinear. Thus, deg is a positive definite quadratic form. □

3.3 Tate modules

In this section, we get a little bit more "Galois", and see what we can do with the group action $\mathrm{Gal}(K/k)$ on the elliptic curve. Let E be an elliptic curve over K/k. Recall that the explicit formula for $[2]$ shows that if E/k then $[2]$ is also defined over k, meaning for all $\sigma \in \mathrm{Gal}(K/k)$, $[2]^\sigma = [2]$. Thus we know, for any $P \in E$

$$[m]P^\sigma = [m]^\sigma P^\sigma = ([m]P)^\sigma$$

which means $\mathrm{Gal}(K/k)$ acts on each $E[m]$!

Therefore, the group action induces a representation (or in certain texts the group action is itself a representation):

$$\rho : \mathrm{Gal}(K/k) \to \mathrm{Aut}(E[m]) = \mathrm{GL}_2(\mathbb{Z}/m\mathbb{Z})$$

But the ring $\mathbb{Z}/m\mathbb{Z}$ has characteristic > 0, which is hard to work with. Thus, we want some ring of characteristic 0 where the representation would live.

Note that $\mathbb{Z}_l$, the ring of l-adic numbers, is the completion of $\mathbb{Z}_{(p)}$, meaning

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

where the obvious inverse system is given by maps of the form $\mathbb{Z}/l^{n+m}\mathbb{Z} \xrightarrow{\cdot l^m} \mathbb{Z}/l^n\mathbb{Z}$. Indeed, this ring has characteristic zero, and it relates very closely to the quotients $\mathbb{Z}/l^n\mathbb{Z}$. So it is ideal to make our representations live on this ring. Meanwhile, note that we also have an inverse system of l^n-torsion subgroups of an elliptic curves, namely

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

We can take

Definition 3.3.1. The inverse limit of all l^n-torsion subgroups:

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

to be the *l-adic Tate module of E*.

Remark 3.3.1. Note that if l is a prime number different from the characteristic of p, then $E[l^n] \cong \mathbb{Z}/l^n\mathbb{Z} \times \mathbb{Z}/l^n\mathbb{Z}$ (Remark 3.2.1), which is a free $\mathbb{Z}/l^n\mathbb{Z}$-module of rank 2. Thus,

$$T_l(E) \cong \mathbb{Z}_l \times \mathbb{Z}_l$$

which is a $\mathbb{Z}_l$-module, with the canonical Krull topology.

Similarly, if $l = p = \mathrm{char}\, k$, then $T_l(E) = 0$ or $\mathbb{Z}_p$.

Remark 3.3.2. The Galois group also acts on $T_l(E)$. To see this, take some element $(,,,,a_2,a_1) \in T_l(E)$. Then we want to show $(...,a_2^\sigma,a_1^\sigma)$ is also in $T_l(E)$ for all $\sigma \in \mathrm{Gal}(K/k)$. This is clear since $a_j = [l]^{j-i}a_i$ suggests

$$a_j^\sigma = ([l]^{j-i}a_i)^\sigma = [l]^{j-1}a_i^\sigma$$

so the property is still preserved.

Thus we have a group representation:

Definition 3.3.2. The representation induced by the group action

$$\rho : \mathrm{Gal}(K/k) \to \mathrm{Aut}(T_l(E))$$

is the *l-adic Galois representation attached to E*.

Remark 3.3.3. For any isogeny $\varphi : E_1 \to E_2$ between elliptic curves (which are homomorphisms so they preserve the torsion subgroups), we have induced maps $\varphi : E_1[l^n] \to E_2[l^n]$ which induce a map

$$\varphi_l : T_l(E_1) \to T_l(E_2)$$

If $E_1 = E_2 = E$, the map $\varphi \mapsto \varphi_l$ is a homomorphism of rings

$$\rho : \mathrm{End}(E) \to \mathrm{End}(T_l(E))$$

The following lemma is an exercise in [Sil09]. We reproduce and solve it here.

Lemma 3.3.1. *The map $\rho : \mathrm{End}(E) \to \mathrm{End}(T_l(E))$ defined by $\varphi \mapsto \varphi_l$ is injective.*

Proof. Suppose $\varphi \in \ker \rho$. Then $\varphi|_{E[l^n]} = 0$ for all n by the construction of φ_l, which means $\#\ker\varphi \geqslant \#E[l^n] = l^{2n}$ for all n. But note that $\#\ker\varphi = \deg_s\varphi$ which is finite if φ is nonconstant. Thus, $\varphi \equiv \mathcal{O}$, suggesting ρ is injective. □

3.4 Weil pairings

Selecting a basis of $E[m]$, which is a $\mathbb{Z}/m\mathbb{Z}$-module, we could define a determinant map $\det : E[m] \times E[m] \to \mathbb{Z}/m\mathbb{Z}$ by selecting a basis $\{T_1, T_2\}$ and letting

$$\det(aT_1 + bT_2, cT_2 + dT_2) = ad - bc.$$

But this determinant might not be Galois invariant. So we define a pairing that's more complicated but nicer.

Take some $T \in E[m]$. Then there is some $f \in K(E)$ such that $\operatorname{div}(f) = m(T) - m(O)$ (since $\kappa([m]T) = m\kappa(T) \equiv \mathcal{O}$ in the Picard group). Take T' such that $[m]T' = T$. Then there is some $g \in K(E)$ such that

$$\operatorname{div}(g) = m^*(T) - m^*(O) = \sum_{R \in E[m]} (T' + R) - (R)$$

It can be checked that $f \circ [m] = g^m$ after multiplying f with a constant. Now fix any $S \in E[m]$. We observe that for all $X \in E$,

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

which means for each X the function $g(X+S)/g(X)$ only takes finitely many values which are all mth roots of unity. Also, the rational function $\varphi : E \to \mathbb{P}^1$ defined by $S \mapsto [g(X+S)/g(X) : 1]$ is not surjective, meaning it's a constant. Therefore, we can define the pairing

Definition 3.4.1.

$$e_m(S,T) = \frac{g(X+S)}{g(X)}$$

called the *Weil e_m-pairing*.

We will only state the following properties of e_m and will omit the proof as it is superbly lengthy but there is not enough space for it.

Lemma 3.4.1. *The Weil e_m-pairing satisfies:*

(i) *The paring is bilinear: $e_m(S_1 + S_2, T) = e_m(S_1, T)e_m(S_2, T)$ and similarly for the other entry.*

(ii) *The pairing is alternating: $e_m(T,T) = 1$ and thus $e_m(S,T) = e_m(T,S)^{-1}$.*

(iii) *The pairing is Galois invariant: $e_m(S,T)^\sigma = e_m(S^\sigma, T^\sigma)$.*

(iv) *The pairing is nondegenerate: if $e_m(S,T) = 1$ for all $S \in E[m]$ then $T = \mathcal{O}$.*

(v) *For all $S \in E[mm'], T \in E[m]$, $e_{mm'}(S,T) = e_m([m']S, T)$.*

(vi) *There exist $S, T \in E[m]$ such that $e_m(S,T)$ is a primitive mth root of unity, namely if $E[m] \subseteq E(k)$ then $\boldsymbol{\mu}_m \subseteq k^\times$ where $\boldsymbol{\mu}_m$ is the set of mth roots of unity in K.*

(vii) *The adjointness of $\hat{\varphi}$: $e_m(S, \hat{\varphi}(T)) = e_m(\varphi(S), T)$.*

We want to create a pairing on $T_l(E)$ too. This would be a map from $T_l(E)\times T_l(E)$ to $T_l(\boldsymbol{\mu}) = \varinjlim \boldsymbol{\mu}_{l^n}$. Note that the map $\boldsymbol{\mu}_{l^{n+1}} \xrightarrow{z\mapsto z^l} \boldsymbol{\mu}_{l^n}$ form the inverse system of the latter inverse limit. By bilinearity and (v) in Lemma 3.4.1,

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

So we have

Definition 3.4.2. The map induced by e_m

$$e : T_l(E) \times T_l(E) \to T_l(\boldsymbol{\mu})$$

is called the *l-adic Weil pairing*.

Remark 3.4.1. Suppose we select a $\mathbb{Z}_l$-basis of $T_l(E)$. Then we can compute the trace and determinant of φ_l for each $\varphi \in \mathrm{End}(E)$. These functions take values in $\mathbb{Z}_l$ and they are independent of the choice of basis.

And finally we use the l-adic Weil pairing to deduce the most important formula in this report:

Theorem 3.4.1. *Let $\varphi \in \mathrm{End}(E)$ and $\varphi_l = \rho(\varphi) \in \mathrm{End}(T_l(E))$. Then*

$$\det(\varphi_l) = \deg\varphi, \quad \mathrm{tr}(\varphi_l) = 1 + \deg\varphi - \deg(1-\varphi)$$

Proof. The latter formula is immediate from the first formula ($a+d = 1+ad-bc-(1-a)(1-d)+bc$). So it suffices to prove the first formula.

Let $\{v_1, v_2\}$ be a $\mathbb{Z}_l$-basis of $T_l(E)$ and write

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

Then

$$\begin{aligned}
e(v_1,v_2)^{\deg\varphi} &= e([\deg\varphi]v_1, v_2) && \text{by bilinearity} \\
&= e(\hat{\varphi}\varphi v_1, v_2) && \text{by construction} \\
&= e(\varphi v_1, \varphi v_2) && \text{by adjointness} \\
&= e(v_1,v_2)^{ad-bc} && \text{by bilinearity and the alternating property} \\
&= e(v_1,v_2)^{\det(\varphi_l)}
\end{aligned}$$

and since $e(v_1,v_2)$ is nondegenerate, $e(v_1,v_2) \neq 1$ so $\deg\varphi = \det(\varphi_l)$. □

4 The p-Riemann Hypothesis

The prominent and difficult Riemann Hypothesis was first presented by Riemann himself in 1859 [Rie59], concerning the real part of the nontrivial zeros of the analytic continuation of the zeta function

$$\zeta(s) = \sum_{n \geqslant 1} \frac{1}{n^s}$$

The mathematical genius Euler proved that

$$\zeta(s) = \prod_{p \text{ prime}} \frac{1}{1 - p^{-s}}$$

in 1740.

While people had no idea about how one might prove or disprove the Riemann Hypothesis, Emil Artin studied a generalized version of this zeta function. Let R be an algebra of finite type over $\mathbb{Z}$ (we don't care what this means). Then for any maximal ideal ideal $\mathfrak{m} \lhd R$, the residue field $R/\mathfrak{m}$ is finite. Artin then defined a generalized zeta function by

$$\zeta_R(s) = \prod_{\mathfrak{m} \text{ maximal}} \frac{1}{1 - \#(R/\mathfrak{m})^{-s}}$$

Note that if $R = \mathbb{Z}$ then the maximal ideals are of the form $p\mathbb{Z}$ and then $\zeta_{\mathbb{Z}}(s)$ is just the regular Riemann zeta function. Unfortunately this definition did not provide the mathematicians with anything special or useful for Riemann Hypothesis [Oor14]. In his Ph.D. thesis, Emil Artin presented an analogous definition of the zeta function $Z(V;T)$ on algebraic curves V over finite fields [Art24]. This zeta function is also called the Hasse–Weil zeta function. This new zeta function then proved to be fruitful, and led to some fruitful developments in geometry and number theory.

With this new zeta function on algebraic curves over a finite field $\mathbb{F}_q$ of characteristic $p > 0$, German mathematicians were able to produce a similar version of Riemann Hypothesis, called the *p-Riemann Hypothesis*, on the properties of $Z(V;T)$. The zeta function $Z(V;T)$ is essentially a generating function of the sizes of the sets $V(\mathbb{F}_{q^n})$ representing the $\mathbb{F}_{q^n}$-rational points in V.

4.1 The Hasse bound

Suppose $E/\mathbb{F}_q$ is an elliptic curve and q is a power of some prime p.

Theorem 4.1.1 (Hasse bound)**.** *Let $E/\mathbb{F}_q$. Then*

$$|\#E(\mathbb{F}_q) - q - 1| \leqslant 2\sqrt{q}$$

Proof. Let $\varphi_q : E \to E$ be the qth Frobenius map. Since the Galois group $\mathrm{Gal}(\overline{\mathbb{F}_q}/\mathbb{F}_q)$ is topologically generated by the Frobenius endomorphism $F : x \mapsto x^q$ (that the cyclic group $\langle F \rangle$ is dense in $\mathrm{Gal}(\overline{\mathbb{F}_q}/\mathbb{F}_q)$ with respect to its Krull topology).; equivalently, the restriction of every $\sigma \in \mathrm{Gal}(\overline{\mathbb{F}_q}/\mathbb{F}_q)$ to $\mathbb{F}_{q^n}$ is a power of F. Thus,

$$P \in E(\mathbb{F}_q) = E^{\mathrm{Gal}(\overline{\mathbb{F}_q}/\mathbb{F}_q)} \text{ if and only if } \varphi_q(P) = \varphi$$

which means $E(\mathbb{F}_q) = \ker(1 - \varphi_q)$. By Theorem 3.1.2 and Theorem 3.1.1, $\#E(\mathbb{F}_q) = \deg(1 - \varphi_q)$. Since $\deg[1] = 1^2 = 1$ and $\deg \varphi_q = q$, by Corollary 3.2.1 and Lemma 0.0.1,

$$|\#E(\mathbb{F}_q) - q - 1| = |\deg(1 - \varphi_q) - \deg[1] - \deg \varphi_q| \leqslant 2\sqrt{\deg[1] \cdot \deg \varphi_q} = 2\sqrt{q}$$

which completes the proof. □

Example 4.1.1. Let $f(x) = ax^3 + bx^2 + cx + d$ be a cubic with distinct roots in $\mathbb{F}_q[x]$. Let $\chi : \mathbb{F}_q^\times \to \{\pm 1\}$ be the character which determines if an element is a square in $\mathbb{F}_q$. One immediately sees that the number of solutions to $E : y^2 = f(x)$ is (with the point at infinity)

$$\#E(\mathbb{F}_q) = 1 + \sum_{x \in \mathbb{F}_q} [1 + \chi(f(x))] = 1 + q + \sum_{x \in \mathbb{F}_q} \chi(f(x))$$

which suggests

$$\left| \sum_{x \in \mathbb{F}_q} \chi(f(x)) \right| \leqslant 2\sqrt{q}$$

by Theorem 4.1.1.

4.2 Weil conjectures

The Weil conjectures consist of several conjectures concerning the properties of the zeta function defined on algebraic varieties (which was primarily defined by Emil Artin in his Ph.D. thesis, mentioned in section 0). Given a smooth projective variety $V/\mathbb{F}_q$, we define similarly the set of $\mathbb{F}_{q^r}$-rational points on V, denoted by $N_r = \#V(\mathbb{F}_{q^r})$.

Definition 4.2.1. The *zeta function of* $V/\mathbb{F}_q$ is the power series

$$Z(V/\mathbb{F}_q;T) = \exp\left(\sum_{r=1}^{\infty} \frac{N_r}{r} T^r\right)$$

where the exponential of a power series with no constant term is defined by

$$\exp(F(T)) = \sum_{k=0}^{\infty} \frac{F(T)^k}{k!}$$

Remark 4.2.1. If we know the zeta function, we could recover each N_r from it:

$$N_r = \frac{1}{(r-1)!} \frac{d^r}{dT^r} \log Z(V/\mathbb{F}_q;T)\Big|_{T=0}$$

Example 4.2.1. Let's try an easy example. Consider the projective space $V = \mathbb{P}^n$. Then the number of points in $V(\mathbb{F}_{q^r})$ is simply $N_r = \frac{q^{r(n+1)}-1}{q^r-1} = \sum_{i=0}^{n} q^{ir}$ (discard the zero tuple and dividing out the equivalence classes). Thus, we have

$$\log Z(V/\mathbb{F}_q;T) = \sum_{r=1}^{\infty}\sum_{i=0}^{n} \frac{(q^iT)^r}{n} = \sum_{i=0}^{n} -\log(1-q^iT)$$

where the second equality holds by exchanging the summation. Thus,

$$Z(V/\mathbb{F}_q;T) = \frac{1}{(1-T)\cdots(1-q^nT)}$$

Remark 4.2.2. What is the set $E(\mathbb{F}_{q^n})$ essentially? Similar to what was argued in Theorem 4.1.1, $E(\mathbb{F}_{q^n})$ is the set of fixed points of the nth iterate of the qth power Frobenius map φ_q. Therefore, we have $\#E(\mathbb{F}_{q^n}) = \ker(1-\varphi_q^n)$, which opens a path way to proving a particular case of the Weil conjectures Hasse used in 1936 [Has36].

The history of the Weil conjectures is also quite interesting. Hasse solved the p-Riemann Hypothesis for curves of genus one, i.e., elliptic curves, and proved Theorem 4.1.1. Weil was aware of this result, and announced an outline of the proof for curves of genus g in 1940, when he was a prisoner "in a French military prison for failing to report for duty" [Bae19]! In 1941 Weil published a proof of a generalization of the Hasse bound. Weil then studied equations of the form

$$a_0x_0^{m_0} + \cdots + a_rx_r^{m_r} = b$$

over some finite fields, and when $b = 0$, Weil found that

$$\sum_{n=1}^{\infty} N_n T^{n-1} = \frac{d}{dT} \log \left(\frac{1}{(1-T)\cdots(1-q^r T)} \right) + (-1)^r \frac{d}{dT} \log P(T)$$

for some polynomial P [Mil16]. Weil then wrote, in [Wei49], that his observation of the homogeneous equations over finite fields might lead to some "conjectural statements", which are rephrased and restate below. These famous statements are the so-called "Weil conjectures". A brief remark on the name of the last statement is in Remark 4.3.1.

Theorem 4.2.1 (Weil conjectures)**.** *Let $V/\mathbb{F}_q$ be a smooth projective variety of dimension N. Then*

(i) *Rationality: $Z(V/\mathbb{F}_q; T) \in \mathbb{Q}(T)$.*

(ii) *Functional equation: there is an integer ε — the Euler characteristic of V — such that $Z(V/\mathbb{F}_q; 1/q^N T) = \pm q^{N\varepsilon/2} T^{\varepsilon} Z(V/\mathbb{F}_q; T)$.*

(iii) *p-Riemann Hypothesis:*

$$Z(V/\mathbb{F}_q; T) = \frac{P_1(T) P_3(T) \cdots P_{2N-1}(T)}{P_0(T) P_2(T) \cdots P_{2N}(T)}$$

where $P_i \in \mathbb{Z}[T]$, $P_0(T) = 1 - T$ and $P_{2N} = 1 - q^N T$. Furthermore, each P_i factors over $\mathbb{C}$ with roots α_{ij} satisfying $|\alpha_{ij}| = q^{1/2}$ for all i, j. The degree of P_i, b_i, is the ith Betti number of V.

As noted before, a baby version of these "conjectures" was proved by Hasse in 1930s. In 1950s, Weil proved these statements for abelian varieties — varieties with an abelian structures but, unlike elliptic curves, are of arbitrary genus and dimension. Grothendieck proved the first two statements for general projective varieties using his theory of étale cohomology, but was unable to prove the p-Riemann Hypothesis. In 1973, Deligne presented his first proof of Weil conjectures [Del74]; in 1980, Deligne presented another proof [Del80]. Deligne's proof was described by Gowers as a "surprise" from Weil's belief of the need of "standard conjectures". Deligne took a "different route", in spite of using Grothendieck's cohomology theory [Gow13].

4.3 Hasse's proof for elliptic curves

Due to the extreme difficulty of the Weil conjectures for general varieties and the level of knowledge required to understand them, we only present the proof of Weil conjectures for elliptic curves — smooth projective varieties of genus one and dimension one. This proof is due to Hasse and was done years before Weil conjectures.

Lemma 4.3.1. *Let $E/\mathbb{F}_q$ be an elliptic curve. Let φ_q be the qth power Frobenius map and suppose*

$$a = q + 1 - \#E(\mathbb{F}_q)$$

Then

(i) *Let $\alpha, \beta \in \mathbb{C}$ be roots of $T^2 - aT + q$. Then $\beta = \bar{\alpha}$ and $|l\alpha| = |\beta| = \sqrt{q}$ and for all $n \geqslant 1$,*

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

(ii) *The characteristic polynomial of φ is $T^2 - aT + q$.*

Proof. By Theorem 3.1.2, $1 - \varphi_q$ is separable and by Theorem 3.1.1,

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

By Theorem 3.4.1, for any prime $l \neq p$

$$\det(\varphi_{q,l}) = \deg \varphi_q = q, \quad \operatorname{tr}(\varphi_{q,l}) = 1 + \deg \varphi_q - \deg(1 - \varphi_q) = 1 + q - \#E(\mathbb{F}_q) = a$$

Thus by the degree-trace formula, $\varphi_{p,l}$ has characteristic polynomial $\det(T - \varphi_{p,l}) = T^2 - aT + q$, which factors over $\mathbb{C}$ as $(T - \alpha)(T - \beta)$.

(i) Since for all $m/n \in \mathbb{Q}$, if $T = m/n$ then by Theorem 3.4.1,

$$\det(T - \varphi_{p,l}) = \frac{\det(m - n\varphi_{p,l})}{n^2} = \frac{\deg(m - n\varphi_{p,l})}{n^2} \geqslant 0,$$

the quadratic function is also nonnegative for all reals. Thus, the roots must be the same or they must be two complex conjugates. In either case, we have $|\alpha| = |\beta|$. But since $\alpha\beta = \det(\varphi_{p,l}) = q$, we get $|\alpha| = |\beta| = \sqrt{q}$.

Similarly, $E(\mathbb{F}_{q^n})$ is the fixed field of φ_q^n. Then as $\varphi_{p,l}$ is equivalent to $\operatorname{diag}(\alpha, \beta)$ or $J_2(\alpha)$, the Jordan canonical normal form of $\varphi_{p,l}^n$ is always $\operatorname{diag}(\alpha^n, \beta^n)$ or $J_2(\alpha^n)$. Thus,

$$\#E(\mathbb{F}_{q^n}) = \deg(1 - \varphi_q^n) = \det(1 - \varphi_{q,l}^n) = 1 - \alpha^n + \beta^n + q^n$$

(ii) We have by Cayley–Hamilton,

$$\deg(\varphi_q^2 - a\varphi_q + q) = \det(\varphi_{q,l}^2 - a\varphi_{q,l} + q) = 0$$

which by the positive definiteness of the quadratic form deg, $\varphi_q^2 - a\varphi_q + q$=0. □

Theorem 4.3.1 (Weil conjectures for elliptic curves)**.** *Let $E/\mathbb{F}_q$ be an elliptic curve. Then there is an $a \in \mathbb{Z}$ such that*

$$Z(E/\mathbb{F}_q; T) = \frac{1 - aT + qT^2}{(1-T)(1-qT)}$$

and (the Euler characteristic is zero; which is already known since $2 - 2g = 0$)

$$Z(E/\mathbb{F}_q; 1/qT) = Z(E/\mathbb{F}_q; T)$$

and finally

$$1 - aT + qT^2 = (1 - \alpha T)(1 - \beta T), \quad |\alpha| = |\beta| = \sqrt{q}$$

Proof. With all our works, the proof is surprisingly easy.

$$\begin{aligned}
\log Z(E/\mathbb{F}_q; T) &= \sum_{n=1}^{\infty} \frac{N_n T^n}{n} && \text{by definition} \\
&= \sum_{n=1}^{\infty} \frac{(1 - \alpha^n - \beta^n + q^n)T^n}{n} && \text{by Lemma 4.3.1} \\
&= -\log(1-T) + \log(1-\alpha T) \\
&\quad + \log(1-\beta T) - \log(1-qT)
\end{aligned}$$

Thus,

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

and the other results are then obvious. □

Remark 4.3.1. Define a function $\zeta_{E/\mathbb{F}_q}(s)$ on $\mathbb{C}$ to be

$$\zeta_{E/\mathbb{F}_q}(s) = Z(E/\mathbb{F}_q; q^{-s}) = \frac{1 - aq^{-s} + q^{1-s}}{(1-q^{-s})(1-q^{1-s})}$$

Then we have $\zeta_{E/\mathbb{F}_q}(s) = \zeta_{E/\mathbb{F}_q}(1-s)$, which is derived from the functional equation. Furthermore, $\zeta_{E/\mathbb{F}_q}(s) = 0$ if and only if $q^{-s} = \alpha$ or β. This means $|q^s| = q^{\mathrm{Re}(s)} = \sqrt{q}$ or $\mathrm{Re}(s) = \frac{1}{2}$. This why the last statement is called the p-Riemann Hypothesis!

5 References

[AM94] M.F. Atiyah and I.G. MacDonald. *Introduction To Commutative Algebra*. Addison-Wesley series in mathematics. Avalon Publishing, 1994. ISBN: 9780813345444. URL: https://books.google.co.uk/books?id=HOASFid4x18C.

[Art24] E. Artin. "Quadratische Körper im Gebiete der höheren Kongruenzen. I." In: *Mathematische Zeitschrift* 19.1 (Dec. 1924), pp. 153–206. ISSN: 1432-1823. DOI: 10.1007/BF01181074. URL: https://doi.org/10.1007/BF01181074.

[Bae19] John Baez. *The Riemann Hypothesis (Part 3)*. The n-Category Café, 2019. URL: https://golem.ph.utexas.edu/category/2019/09/the_riemann_hypothesis_part_3.html (visited on 06/20/2022).

[Del74] Pierre Deligne. "La conjecture de Weil : I". fr. In: *Publications Mathématiques de l'IHÉS* 43 (1974), pp. 273–307. URL: http://www.numdam.org/item/PMIHES_1974__43__273_0/.

[Del80] Pierre Deligne. "La conjecture de Weil : II". fr. In: *Publications Mathématiques de l'IHÉS* 52 (1980), pp. 137–252. URL: http://www.numdam.org/item/PMIHES_1980__52__137_0/.

[Gow13] W. T. Gowers. *The Work of Pierre Deligne*. 2013. URL: https://gowers.files.wordpress.com/2013/03/peterd.pdf.

[Har10] Robin Hartshorne. *Algebraic Geometry*. Springer, 2010.

[Has36] Helmut Hasse. "Zur Theorie der abstrakten elliptischen Funktionenkörper III. Die Struktur des Meromorphismenrings. Die Riemannsche Vermutung." In: *Journal für die reine und angewandte Mathematik* 175 (1936), pp. 193–208. URL: http://eudml.org/doc/149968.

[Mil16] J. S. Milne. "The Riemann Hypothesis over Finite Fields: From Weil to the Present Day". In: ed. by Lizhen Ji, Frans Oort, and Shing-Tung Yau. The Legacy of Bernhard Riemann after One Hundred and Fifty Years. International Press of Boston, Inc., 2016, pp. 487–566.

[Oor14] Frans Oort. "Wei Conjectures". In: *Nieuw Archief Voor Wiskunde* 1 (2014), p. 211. URL: http://www.nieuwarchief.nl/serie5/pdf/naw5-2014-15-3-211.pdf (visited on 06/20/2022).

[Poo99] Bjorn Poonen. "An explicit algebraic family of genus-one curves violating the Hasse principle". In: (1999). DOI: 10.48550/ARXIV.MATH/9910124. URL: https://arxiv.org/abs/math/9910124.

[Rie59] Bernard Riemann. “Ueber die Anzahl der Primzahlen unter einer gegebenen Grösse”. In: *Monatsberichte der Königlich Preußischen Akademie der Wissenschaften zu Berlin* (1859).

[Sil09] Joseph H Silverman. *The Arithmetic of Elliptic Curves*. Springer-Verlag, 2009.

[Wei49] André Weil. “Numbers of Solutions of Equations in Finite Fields”. In: *Bulletin of the American Mathematical Society* 55 (1949), pp. 497–508. DOI: 10.1090/s0002-9904-1949-09219-4. (Visited on 06/20/2022).