Contents

Chapter 1

Introduction to Field Theory

We put together some facts from field theory that we frequently call upon. Proofs can be found in all standard textbooks on algebra, e.g. [3], [4], [5], [6].

1.0.1 Algebraic Field Extensions

Let L be a field that contains K as a subfield. Then L/K is called a *field extension*. Considering L as a vector space over K, its dimension is called the degree of L/K and denoted by $[L : K]$.

L/K is said to be a *finite extension* if $[L : K] = n < \infty$. Then, there exists a *basis* $\{\alpha_1, \ldots, \alpha_n\}$ of L/K, i.e. every $\gamma \in L$ has a unique representation $\gamma = \sum_{i=1}^{n} c_i \alpha_i$ with $c_i \in K$. If L/K and M/L are finite extensions, then M/K is finite as well, and the degree is $[M : K] = [M : L] = [L : K]$.

An element $\alpha \in L$ is *algebraic over* K if there is a non–zero polynomial $f(X) \in K[X]$ (the polynomial ring over K) such that $f(\alpha) = 0$. Among all such polynomials, there is a unique polynomial of smallest degree that is monic (i.e., its leading coefficient is 1); this is called the *minimal polynomial* of α over K. The minimal polynomial is irreducible in the ring $K[X]$, hence it is often called the *irreducible polynomial* of α over K.

The field extension L/K is called an *algebraic extension* if all elements $\alpha \in L$ are algebraic over K.

Let $\gamma_1, \ldots, \gamma_r \in L$. The smallest subfield of L that contains K and all elements $\gamma_1, \ldots, \gamma_r$ is denoted by $K(\gamma_1, \ldots, \gamma_r)$. The extension $K(\gamma_1, \ldots, \gamma_r)/K$ is finite if and only if all γ_i are algebraic over K.

In particular, $\alpha \in L$ is algebraic over K if and only if $[K(\alpha) : K] < \infty$. Let $p(X) \in K[X]$ be the minimal polynomial of α over K and $r = deg\, p(X)$. Then $[K(\alpha) : K] = r$, and the elements $1, \alpha, \alpha^2, \ldots, \alpha^{r-1}$ form a basis of $K(\alpha)/K$.

1.0.2 Embeddings and K-Isomorphisms

Consider field extensions L_1/K and L_2/K. A field homomorphism $\sigma : L_1 \to L_2$ is called an *embedding* of L_1 into L_2 over K, if $\sigma(a) = a$ for all $a \in K$. It follows that σ is injective and yields an isomorphism of L_1 onto the subfield $\sigma(L_1) \subseteq L_2$. A surjective (hence bijective) embedding of L_1 into L_2 over K is a K-*isomorphism*.

1.0.3 Adjoining Roots of Polynomials

Given a field K and a non–constant polynomial $f(X) \in K[X]$, there exists an algebraic extension field $L = K(\alpha)$ with $f(\alpha) = 0$. If $f(X)$ is irreducible, this extension field is unique up to $f(\alpha') = 0$, then there exists a K-isomorphism $\sigma : L \to L'$ with $\sigma(\alpha) = \alpha'$. We say that $L = K(\alpha)$ is obtained by *adjoining a root* of $p(X)$ to K.

If $f_1(X), \ldots, f_r(X) \in K[X]$ are monic polynomials of degree $d_i \geq 1$, there exists an extension field $Z \supseteq K$ such that all $f_i(X)$ split into linear factors $f_i(X) = \prod_{j=1}^{d_i}(X - \alpha_{ij})$ with $\alpha_{ij} \in Z$, and $Z = K(\{\alpha_{ij} \mid 1 \leq i \leq r \text{ and } 1 \leq j \leq d_i\})$. The field Z is unique up to K-isomorphism; it is called the *splitting field* of $f_1, \ldots, f_r$ over K.

1.0.4 Algebraic Closure

A field M is called *algebraically closed* if every polynomial $f(X) \in M[X]$ of degree ≥ 1 has a root in M.

For any field K, there exists an algebraic extension $\bar{K}/K$ with an algebraically closed field $\bar{K}$. The field $\bar{K}$ is unique up to K-isomorphism; it is called the *algebraic closure* of K.

Given an algebraic field extension L/K, there exists an embedding $\sigma : L \to \bar{K}$ over K. If $[L : K] < \infty$, the number of distinct embeddings of L to $\bar{K}$ over K is at most $[L : K]$.

1.0.5 The Characteristic of a Field

Let K be a field and $1 \in K$ be the neutral element with respect to multiplication. For any integer $m > 0$, let $\underline{m} = 1 + 1 + \cdots + 1 \in K$ (m summands). If $\underline{m} \neq 0$ (the zero element of K) for all $m > 0$, we say that K has characteristic zero.

Otherwise, there exists a unique prime number $p \in \mathbb{N}$ such that $p = 0$, and K is said to have characteristic p. We use the abbreviation *char* K.

If *char* $K = 0$, then K contains the field $\mathbb{Q}$ of rational numbers (up to isomorphism), In case *char* $K = p > 0$, K contains the field $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$.

In a field of characteristic $p > 0$, we have $(a+b)^q = a^q + b^q$ for all $a, b \in K$ and $q = p^j$, $j \geq 0$.

1.0.6 Separable Polynomials

Let $f(X) \in K[X]$ be a monic polynomial of degree $d \geq 1$. In some extension field $L \supseteq K$, $f(X)$ splits into linear factors $f(X) = \prod_{i=1}^{d}(X - \alpha_i)$. The polynomial $f(X)$ is called *separable* if $\alpha_i \neq \alpha_j$ for all $i \neq j$; otherwise, f is an *inseparable* polynomial.

If *char* $K = 0$, all irreducible polynomials are separable. In case *char* $K = p > 0$, an irreducible polynomial $f(X) = \sum a_i X^i \in K[X]$ is separable if and only if $a_i \neq 0$ for some $i \not\equiv 0$ *mod* p.

The *derivative* of $f(X) = \sum a_i X^i \in K[X]$ is defined in the usual manner by $f'(X) = \sum i a_i X^{i-1}$ (where $i \in \mathbb{N}$ is considered as an element of K as in 1.0.5). An irreducible polynomial $f(X) \in K[X]$ is separable iff $f'(X) \neq 0$.

1.0.7 Separable Field Extensions

Let L/K be an algebraic field extension. An element $\alpha \in L$ is called *separable* over K if its minimal polynomial $p(X) \in K[X]$ is a separable polynomial. L/K is a *separable extension* if all $\alpha \in L$ are separable over K. If *char* $K = 0$, then all algebraic extensions L/K are separable.

Let Φ be an algebraically closed field, $\Phi \supseteq K$, and suppose that L/K is a finite extension of degree $[L : K] = n$. Then, L/K is separable if and only if there exists n distinct embeddings $\sigma_1, \ldots, \sigma_n : L \to \Phi$ over K (cf. 1.0.4). In this case, an element $\gamma \in L$ is in K iff $\sigma_i(\gamma) = \gamma$ for $i = 1, \ldots, n$.

Given a tower $M \supseteq L \supseteq K$ of algebraic field extensions, the extension M/K is separable if and only if both extensions M/L and L/K are separable.

1.0.8 Purely Inseparable Extensions

Consider an algebraic extension L/K where *char* $K = p > 0$. An element $\gamma \in L$ is called *purely inseparable* over K if $\gamma^{p^r} \in K$ for some $r \geq 0$. In this case, the minimal polynomial of γ over K has the form $f(X) = X^{p^e} - \mathrm{c}$ with $c \in K$ (and

$e \leq r$). The extension L/K is *purely inseparable* if all elements $\gamma \in L$ are purely inseparable over K.

Given an arbitrary algebraic extension L/K, there exists a unique intermediate field S, $K \subseteq S \subseteq L$, such that S/K is separable and L/S is purely inseparable.

1.0.9 Perfect Fields

A field K is called *perfect* if all algebraic extensions L/K are separable. Fields of characteristic 0 are always perfect. A field K of characteristic $p > 0$ is perfect if and only if every $\alpha \in K$ can be written as $\alpha = \beta^p$, for some $\beta \in K$. All finite fields are perfect (cf. 1.0.15).

1.0.10 Simple Algebraic Extensions

An algebraic extension L/K is called *simple* if $L = K(\alpha)$ for some $\alpha \in L$. The element α is called a *primitive element* for L/K.

Every finite separable algebraic field extension is simple.

Suppose that $L = K(\alpha_1, \ldots, \alpha_r)$ is a finite separable extension and $K_0 \subseteq K$ is an infinite subset of K. Then there exists a primitive element α of the form $\alpha = \sum_{i=1}^{n} c_i \alpha_i$ with $c_i \in K_0$.

1.0.11 Galois Extensions

For a field extension L/K, we denote the group of automorphisms of L over K by $Aut(L/K)$. That is, an element $\sigma \in Aut(L/K)$ is a K-isomorphism of L into L. If $[L : K] < \infty$, the order of $Aut(L/K)$ is always $\leq [L : K]$. The extension L/K is said to be *Galois* [1] if the order of $Aut(L/K)$ is $[L : K]$. In this case, we call $Gal(L/K) := Aut(L/K)$ the *Galois group* of L/K. The following conditions are equivalent, for a field extension L/K of finite degree:

(1) L/K is Galois.

(2) L is the splitting field of separable polynomials $f_1(X), \ldots, f_r(X) \in K[X]$ over K.

(3) L/K is separable, and any irreducible polynomial $p(X) \in K[X]$ that has a root in L, splits into linear factors in $L[X]$.

Given a finite separable extension L/K and an algebraically closed field $\Phi \supseteq L$, there exists a unique field M, $L \subseteq M \subseteq \Phi$, with the following properties:

[1] We consider here only Galois extensions of finite degree.

(a) M/K is Galois, and

(b) if $L \subseteq N \subseteq \phi$ and N/K is Galois, then $M \subseteq N$.

This field M is called the *Galois closure* of L/K.

1.0.12 Galois Theory

We consider a Galois extension L/K with Galois group $G = Gal(L/K)$. Let

$$\mathcal{U} := \{U \subseteq G \,|\, U \text{ is a subgroup of } G\} \tag{1.1}$$

and

$$\mathcal{F} := \{N \,|\, N \text{ is an intermediate field of } L/K\}. \tag{1.2}$$

For any intermediate field N of L/K, the extension L/N is Galois, thus we have a mapping

$$\begin{array}{rcl} \mathcal{F} & \longrightarrow & \mathcal{U}\,, \\ N & \longmapsto & Gal(L/N)\,. \end{array} \tag{1.3}$$

On the other hand, given a subgroup $U \subseteq G$ we define the *fixed field* of U by

$$L^U := \{c \in L \,|\, \sigma(c) = c \text{ for all } \sigma \in U\}\,. \tag{1.4}$$

In this manner, we obtain a mapping

$$\begin{array}{rcl} \mathcal{U} & \longrightarrow & \mathcal{F}\,, \\ U & \longmapsto & L^U\,. \end{array} \tag{1.5}$$

Now we can formulate the main results of Galois theory:

(1) The mappings (1.3) and (1.5) are inverse to each other. They yield a 1-1 correspondence between $\mathcal{U}$ and $\mathcal{F}$ (*Galois correspondence*).

(2) For $U \in \mathcal{U}$, we have

$$[L : L^U] = ord\, U \quad \text{and} \quad [L^U : K] = (G : U)\,. \tag{1.6}$$

(3) If $U \subseteq G$ is a subgroup, then $U = Gal(L/L^U)$.

(4) If N is an intermediate field of L/K, then $N = L^U$ with $U = Gal(L/N)$.

(5) For subgroups $U,\ V \subseteq G$, we have $\quad U \subseteq V \Longleftrightarrow L^U \supseteq L^V$.

(6) Let N_1 and N_2 be intermediate fields of L/K and $N = N_1N_2$ be the compositum of N_1 and N_2. Then $Gal(L/N) = Gal(L/N_1) \cap Gal\,(L/N_2)$.

(7) If N_1 and N_2 are intermediate fields of L/K, then the Galois group of $L/N_1 \cap N_2$ is the subgroup of G that is generated by $Gal(L/N_1)$ and $Gal(L/N_2)$.

(8) A subgroup $U \subseteq G$ is a normal subgroup of G if and only if the extension L^U/K is Galois. In this case, $Gal(L^U/K)$ is isomorphic to the factor group G/U.

1.0.13 Cyclic Extensions

A Galois extension L/K is said to be *cyclic* if $Gal(L/K)$ is a cyclic group. Two special cases are of particular interest: Kummer extensions and Artin-Schreier extensions.

(1) (*Kummer Extensions.*) Suppose that L/K is a cyclic extension of degree $[L : K] = n$, where n is relatively prime to the characteristic of K, and K contains all n-th roots of unity (i.e., the polynomial $X^n - 1$ splits into linear factors in $K[X]$). Then there exists an element $\gamma \in L$ such that $L = K(\gamma)$ with

$$\gamma^n = c \in K, \quad \text{and } c \neq w^d \text{ for all } w \in K \text{ and } d \,|\, n,\ d > 1. \tag{1.7}$$

Such a field extension is called a *Kummer Extensions*. The automorphisms $\sigma \in Gal(L/K)$ are given by $\sigma(\gamma) = \zeta \cdot \gamma$, where $\zeta \in K$ is an n-th root of unity.

Conversely, if K contains all n-th roots of unity (n relatively prime to *char* K), and $L = K(\gamma)$ where γ satisfies the conditions (1.7), then L/K is a cyclic extension of degree n.

(2) (*Artin-Schreier Extensions.*) Let L/K be a cyclic extension of degree $[L : K] = p = char\ K$. Then there exists an element $\gamma \in L$ such that $L = K(\gamma)$,

$$\gamma^p - \gamma = c \in K, \quad \text{and } c \neq \alpha^p - \alpha \text{ for all } \alpha \in K\,. \tag{1.8}$$

Such a field extension is called an *Artin-Schreier Extension* of degree p. The automorphisms of L/K are given by $\sigma(\gamma) = \gamma + \nu$ with $\nu \in \mathbb{Z}/p\mathbb{Z} \subseteq K$.

Any element $\gamma_1 \in L$ such that $L = K(\gamma_1)$ and $\gamma_1^p - \gamma_1 \in K$, is called an *Artin-Schreier generator* for L/K. Any two Artin-Schreier generators γ and γ_1 of L/K are related as follows: $\gamma_1 = \mu \cdot \gamma + (b^p - b)$ with $0 \neq \mu \in \mathbb{Z}/p\mathbb{Z}$ and $b \in K$.

Conversely, if we have a field extension $L = K(\gamma)$ where γ satisfies (1.8) (and *char* $K = p$), then L/K is cyclic of degree p.

1.0.14 Norm and Trace

Let L/K be a field extension of degree $[L : K] = n < \infty$. Any element $\alpha \in L$ yields a K-linear map $\mu_\alpha : L \to L$, defined by $\mu_\alpha(z) := \alpha \cdot z$ for $z \in L$. We define the *norm* (resp. the *trace*) of α with respect to the extension L/K by

$$N_{L/K}(\alpha) := det(\mu_\alpha) \quad \text{resp.} \quad Tr_{L/K}(\alpha) := Trace(\mu_\alpha)\,. \tag{1.9}$$

This means: if $\{\alpha_1, \dots, \alpha_n\}$ is a basis of L/K and

$$\alpha \cdot \alpha_i = \sum_{j=1}^{n} a_{ij}\alpha_j \quad \text{with} \quad a_{ij} \in K\,, \tag{1.10}$$

then

$$N_{L/K}(\alpha) = det(a_{ij})_{1\le i,j\le n} \quad \text{and} \quad Tr_{L/K}(\alpha) = \sum_{i=1}^{n} a_{ii}. \tag{1.11}$$

We note some properties of norms and traces.

(1) The norm map is multiplicative, i.e. $N_{L/K}(\alpha \cdot \beta) = N_{L/K}(\alpha) \cdot N_{L/K}(\beta)$ for all $\alpha, \beta \in L$. Moreover, $N_{L/K}(\alpha) = 0 \iff \alpha = 0$, and for $a \in K$ we have $N_{L/K}(a) = a^n$, with $n = [L : K]$.

(2) For $\alpha, \beta \in L$ and $a \in K$, the following holds:

$$\begin{aligned} &Tr_{L/K}(\alpha + \beta) = Tr_{L/K}(\alpha) + Tr_{L/K}(\beta)\,,\\ &Tr_{L/K}(a \cdot \alpha) = a \cdot Tr_{L/K}(\alpha)\,, \text{ and}\\ &Tr_{L/K}(a) = n \cdot a, \quad \text{with } n = [L : K]\,. \end{aligned} \tag{1.12}$$

In particular, $Tr_{L/K}$ is a K-linear map.

(3) If L/K and M/L are finite extensions, then

$$\begin{aligned} &Tr_{M/K}(\alpha) = Tr_{L/K}(Tr_{M/L}(\alpha)) \quad \text{and}\\ &N_{M/K}(\alpha) = N_{L/K}(N_{M/L}(\alpha)) \end{aligned} \tag{1.13}$$

for all $\alpha \in M$.

(4) A finite field extension L/K is separable if and only if there exists an element $\gamma \in L$ such that $Tr_{L/K}(\gamma) \neq 0$ (since the trace map is K-linear, it follows then that $Tr_{L/K} : L \to K$ is surjective).

(5) Let $f(X) = X^r + a_{r-1}X^{r-1} + \cdots + a_0 \in K[X]$ be the minimal polynomial of α over K, and $[L : K] = n = rs$ (with $s = [L : K(\alpha)]$). Then

$$N_{L/K}(\alpha) = (-1)^n a_0^s \quad \text{and} \quad Tr_{L/K}(\alpha) = -sa_{r-1}\,. \tag{1.14}$$

(6) Suppose now that L/K is separable of degree n. Consider the n distinct embeddings $\sigma_1, \dots, \sigma_n : L \to \Phi$ of L over K into an algebraically closed field $\Phi \supseteq K$. Then,

$$N_{L/K}(\alpha) = \prod_{i=1}^{n} \sigma_i(\alpha) \quad \text{and} \quad Tr_{L/K}(\alpha) = \sum_{i=1}^{n} \sigma_i(\alpha) \tag{1.15}$$

for all $\alpha \in L$.

(7) In particular, if L/K is Galois with Galois group $G = Gal(L/K)$, then

$$N_{L/K}(\alpha) = \prod_{\sigma\in G} \sigma(\alpha) \quad \text{and} \quad Tr_{L/K}(\alpha) = \sum_{\sigma\in G} \sigma(\alpha) \tag{1.16}$$

for $\alpha \in L$.

1.0.15 Finite Fields

Let $p > 0$ be a prime number and $q = p^n$ be a power of p. Then $\mathbb{F}_q$ is the splitting field of the polynomial $X^q - X$ over the field $\mathbb{F}_p := \mathbb{Z}/p\mathbb{Z}$. In this manner, we obtain *all* finite fields of characteristic p.

The multiplicative group of $\mathbb{F}_q$ is a cyclic group of order $q-1$, i.e.

$$\mathbb{F}_q = \{0, \beta, \beta^2, \ldots, \beta^{q-1} = 1\}, \tag{1.17}$$

where β is a generator of the multiplicative group.

Let $m \geq 1$. Then $\mathbb{F}_q \subseteq \mathbb{F}_{q^m}$, and the extension $\mathbb{F}_{q^m}/\mathbb{F}_q$ is a Galois extension of degree m. The Galois group $Gal\,(\mathbb{F}_{q^m}/\mathbb{F}_q)$ is a cyclic; it is generated by the *Frobenius automorphism*

$$\varphi : \begin{cases} \mathbb{F}_{q^m} & \longrightarrow & \mathbb{F}_{q^m} \ , \\ \alpha & \longmapsto & \alpha^q \ . \end{cases} \tag{1.18}$$

In particular, all finite fields are perfect.

The norm and trace map from $\mathbb{F}_{q^m}$ to $\mathbb{F}_q$ are given by

$$N_{\mathbb{F}_{q^m}/\mathbb{F}_q}(\alpha) \ = \ \alpha^{1+q+q^2+\cdots+q^{m-1}} \ , \tag{1.19}$$

$$Tr_{\mathbb{F}_{q^m}/\mathbb{F}_q}(\alpha) \ = \ \alpha + \alpha^q + \cdots + \alpha^{q^{m-1}} \ . \tag{1.20}$$

Hilbert's Theorem 90 states, for $\alpha \in \mathbb{F}_{q^m}$,

$$Tr_{\mathbb{F}_{q^m}/\mathbb{F}_q}(\alpha) = 0 \iff \alpha = \beta^q - \beta \quad \text{for some} \quad \beta \in \mathbb{F}_{q^m}. \tag{1.21}$$

1.0.16 Transcendental Extensions

Let L/K be a field extension. An element $x \in L$ that is not algebraic over K is called *transcendental* over K. A finite subset $\{x_1, \ldots, x_n\} \subseteq L$ is *algebraically independent* over K if there does not exist a non–zero polynomial $f(X_1, \ldots, X_n) \in K[X_1, \ldots, X_n]$ with $f(x_1, \ldots, x_n) = 0$. An arbitrary subset $S \subseteq L$ is algebraically independent over K if all finite subsets of S are algebraically independent over K.

A *transcendence basis* of L/K is a maximal algebraically independent subset of L. Any two transcendence bases of L/K have the same cardinality, the *transcendence degree* of L/K.

If L/K has finite transcendence degree n and $\{x_1, \ldots, x_n\}$ is a transcendence basis if L/K, the field $K(x_1, \ldots, x_n) \subseteq L$ is K-isomorphic to $K(X_1, \ldots, X_n)$, the quotient field of the polynomial ring $K[X_1, \ldots, X_n]$ in n variables over K. The extension $L/K(x_1, \ldots, x_n)$ is algebraic.

Chapter 2

Examples of Algebraic Function Fields - Elliptic Function Fields

We shall restrict to the perfect field K. In particular, the results hold if K is an algebraically closed field, a field of characteristic zero or a finite field.

Definition 1. *An algebraic function field F/K is said to be an elliptic function field if the following conditions hold:*

1. *the genus of F/K is* 1,
2. *there exists a divisor $A \in D_F$ with $deg\, A = 1$.*

Lemma 1. *Let F/K be an elliptic function field.*

1. *If $char(K) \neq 2$, there exists $x, y \in F$ such that $F = K(x, y)$ and*
$$y^2 = f(x) \in K[x] \text{ with a square-free polynomial } f(x) \in K[x], \tag{2.1}$$
$deg(f) = 3$.
2. *If char $(K) = 2$, there exist $x, y \in F$ such that $F = K(x, y)$ and*
$$y^2 + y = f(x) \in K[x], \qquad deg(f) = 3 \tag{2.2}$$
or
$$y^2 + y = x + \frac{1}{ax + b}, \qquad 0 \neq a, b \in K. \tag{2.3}$$

Proof:

Choose $A \in D_F,\ \deg(A) = 1$. By the Riemann-Roch Theorem [2], $\dim A = \deg A - g + 1 = 1$ (note $\deg A > 2g - 2$). Hence A is equivalent to a positive divisor $A_1,\ A_1 \sim A$. As $\deg A_1 = 1$ we conclude that A_1 a prime divisor $A_1 = P \in \mathbb{P}_F$.
Let us consider the spaces $K = \mathcal{L}(0) \subseteq \mathcal{L}(P) \subseteq \ldots \subseteq \mathcal{L}(nP) \subseteq \ldots$ Because $2g - 2 = 0$, the Riemann-Roch Theorem [2] gives $\dim \mathcal{L}(iP) = i\ \forall i > 0$, hence $\mathcal{L}(P) = K$ and $\mathcal{L}((i+1)P) \supsetneq \mathcal{L}(iP)$ for $i > 0$. We choose $x_1 \in \mathcal{L}(2P) \setminus K$, $y_1 \in \mathcal{L}(3P) \setminus \mathcal{L}(2P)$.
Then $[F : K(x_1)] = (x_1)_\infty = 2,\ [F : K(y_1)] = (y_1)_\infty = 3$, and so due to the $K-$independents of x_1 and y_1 we have $F = K(x_1, y_1)$.
The seven elements $\{1, x_1, y_1, {x_1}^2, x_1y_1, {x_1}^3, {y_1}^2\} \in \mathcal{L}(6P)$. Since $\mathcal{L}(6P) = 6$ there is a non-trivial relation

$$\alpha_1 {y_1}^2 + \beta_1 x_1 y_1 + \gamma_1 y_1 = \delta_1 {x_1}^3 + \epsilon_1 {x_1}^2 + \lambda_1 x_1 + \mu_1 \tag{2.4}$$

with $\alpha_1,\ \beta_1, \ldots \in K$. The coefficient $\alpha_1 \neq 0$; otherwise Equation (2.4) would reduce to an equation for y_1 over $K(x_1)$ of degree one, which is impossible as $F = K(x_1, y_1)$ and $[F : K(x_1)] = 2$. In the same manner, we see that $\delta_1 \neq 0$. Multiply Equation (2.4) by $\alpha_1^3\delta_1^2$; then

$$\alpha_1^4\delta_1^2 y_1^2 + \cdots = \alpha_1^3\delta_1^3 x_1^3 + \cdots$$

Setting $y_2 := \alpha_1^2\delta_1 y_1,\ x_2 := \alpha_1\delta_1 x_1$, we obtain $F = K(x_2, y_2)$ and

$$y_2^2 + (\beta_2 x_2 + \gamma_2)y_2 = x_2^3 + \epsilon_2 x_2^2 + \lambda_2 x_2 + \mu_2$$

with $\beta_2,\ \gamma_2, \ldots \in K$. We must distinguish two cases:

1. *char*$(K) \neq 2$
   We set $y := y_2 + \frac{1}{2}(\beta_2 x_2 + \gamma_2)$, $x := x_2$; then $F = K(x, y)$ and

   $$y^2 = x^3 + \epsilon x^2 + \lambda x + \mu = f(x) \in K[x], \qquad \epsilon,\ \lambda,\ \mu \in K.$$

   It remains to show that $f(x)$ is square-free. Suppose the contrary, i.e. $f(x) = (x - \xi)^2(x - \eta)$ for $\xi,\ \eta \in K$. Consider the element $z := \frac{y}{(x-\xi)}$. Then $z^2 = x - \eta$ and so $F = K(x, y) = K(x, z) = K(z)$. This implies that F is rational, a contradiction.

2. *char*$(K) = 2$ We have already shown that $F = K(x_2, y_2)$ with

   $$y_2^2 + (\beta_2 x_2 + \gamma_2)y_2 = x_2^3 + \epsilon_2 x_2^2 + \lambda_2 x_2 + \mu_2.$$

   We claim $\beta_2 x_2 + \gamma_2 \neq 0$. If $\beta_2 x_2 + \gamma_2 = 0$ then $y_2^2 \in K(x_2)$, i.e. the extension $F/K(x_2)$ is purely inseparable of degree $p = 2$. It is well-known that the only intermediate field $K \subseteq F_0 \subseteq F$ such that F/F_0 is purely inseparable of degree p is the field $F_0 = F^P$, so $K(x_2) = F^P$. However, the genus of $K(x_2)/K$ is zero and the genus of F^P/K is one. This proves

the claim.
We set $y_3 := (\beta_2 x_2 + \gamma_2)^{-1} y_2$, then $F = K(x_2, y_3)$ and

$$y_3^2 + y_3 = (\beta_2 x_2 + \gamma_2)^{-2}(x_2^3 + \epsilon_2 x_2^2 + \lambda_2 x_2 + \mu_2). \tag{2.5}$$

If $\beta_2 = 0$, the RHS of Equation (2.5) is a polynomial $f(x_2) \in K[x_2]$ of degree 3, which is the promised result. If $\beta_2 \neq 0$ the RHS of Equation (2.5) can be rewritten in the form

$$\nu x_2 + \varrho + \frac{\sigma}{(\beta_2 x_2 + \gamma_2)^2} + \frac{\tau}{\beta_2 x_2 + \gamma_2}, \qquad 0 \neq \nu,\ \varrho,\ \sigma,\ \tau \in K.$$

As K is a perfect field, $\sigma = \sigma_1^2$ for some $\sigma_1 \in K$, and the element $y_4 := y_3 + \sigma_1(\beta_2 x_2 + \gamma_2)$ satisfies an equation

$$y_4^2 + y_4 = \nu_2 x_2 + \varrho_2 + \frac{\tau_2}{\beta_2 x_2 + \gamma_2}, \qquad 0 \neq \nu_2,\ \varrho_2,\ \tau_2 \in K.$$

We have $\tau_2 \neq 0$; otherwise $F = K(x_2, y_4)$ would be rational, $F = K(x_2, y_4) = K(y_4)$. Set $y := y_4$ and $x := \nu_2 x_2 + \varrho_2$ and obtain $F = K(x, y)$ with

$$y^2 + y = x + \frac{1}{ax + b}, \qquad 0 \neq a,\ b \in K.$$

■

We shall list, without proof, a few basic results related to elliptic function fields given by Equation (2.1), (2.2), (2.3).

Lemma 2.

1. *char*$(K) \neq 2$
   suppose that $F = K(x,y)$ with $y^2 = f(x) \in K[x]$, where $f(x)$ is a square-free polynomial, $\deg f = 3$. Consider the decomposition $f(x) = c\prod_{i=1}^r p_i(x)$ into irreducible monic polynomials $p_i(x) \in K[x]\ \forall\, i = 1, \ldots, r$, $0 \neq c \in K$. Denote by $P_i \in \mathbb{P}_{K(x)}$ the place of $K(x)$ corresponding to $p_i(x)$, and by $P_\infty \in \mathbb{P}_{K(x)}$ the pole of x. Then
   (a) *$K \subseteq F$ is the full constant field of F and F/K is an elliptic function field*
   (b) *The extension $F/K(x)$ is cyclic of degree 2. The places $P_1, \ldots, P_r$ are ramified in $F/K(x)$; each of them has exactly one extension in F, say $Q_1, \ldots, Q_r$ and Q_∞, and we have $e(Q_j,\ P_j) = e(Q_\infty,\ P_\infty) = 2 (\forall j)$, $\deg Q_j = \deg P_j$ and $\deg Q_\infty = 1$.*
   (c) *$P_1, \ldots, P_r, P_\infty$ are the only places ramified in $F/K(x)$.*
2. *char*$(K) = 2$
   Suppose that $F = K(x,y)$ with $y^2 + y = f(x) \in K[x]$, deg$(f) = 3$ or $y^2 + y = x + \frac{1}{ax+b}$ with $0 \neq a,\ b \in K$. Denote by $P_\infty \in \mathbb{P}_{K(x)}$ the pole of x in $K(x)$ and by $P' \in \mathbb{P}_{K(x)}$ the zero of $(ax + b) \in K(x)$.

(a) K is the full constant field of F, and F/K is an elliptic function field.

(b) The extension $F/K(x)$ is cyclic of degree 2. The only places of $K(x)$ which ramify in $F/K(x)$ are P_∞ in the case of Equation (2.1) and P', P_∞ in the case of Equation (2.2). Let Q_∞ (resp. Q' in the case of Equation (2.2)) be the place(s) of F/K lying over P_∞ (resp. P'). Then $deg\, Q_\infty = deg\, Q' = 1$.

Ex. 1. *Let us describe the classical example of an elliptic function field. Consider the lattice $\Gamma \subseteq \mathbb{C}$, i.e. $\Gamma = \mathbb{Z}\gamma_1 \oplus \mathbb{Z}\gamma_2$, $\gamma_1,\ \gamma_2 \in \mathbb{C} \setminus \{0\}$, $\frac{\gamma_1}{\gamma_2} \notin \mathbb{R}$. An elliptic function $f : \mathbb{C} \to \mathbb{C}$ w. r. to lattice Γ is a meromorphic function satisfying $f(z+\gamma) = f(z)\ \forall \gamma \in \Gamma,\ z \in \mathbb{C}$. The elliptic function field $\mathcal{U}(\Gamma)$ forms a subfield of the field $\mathcal{U}(\mathbb{C})$ of meromorphic functions on the complex plane. The set $\mathbb{C} \subset \mathcal{U}(\Gamma) \subset \mathcal{U}(\mathbb{C})$ is the full subfield of constants. Two specific non-constant elliptic functions are Weierstrass $\mathcal{P}$-function*

$$\mathcal{P}(z) := \frac{1}{z^2} + \sum_{0 \neq \gamma \in \Gamma} \left(\frac{1}{(z-\gamma)^2} - \frac{1}{\gamma^2} \right)$$

and its derivative $\mathcal{P}'(z)$. These functions fulfill

1. $\mathcal{U}(\Gamma) = \mathbb{C}\left(\mathcal{P}(z), \mathcal{P}'(z)\right)$,

2. $\left(\mathcal{P}'(z)\right)^2 = 4\mathcal{P}^3(z) - g_2\mathcal{P}(z) - g_3$

with constants $g_2, g_3 \in \mathbb{C}$ and square-free polynomial $f(\mathcal{T}) = 4\mathcal{T}^3 - g_2\mathcal{T} - g_3 \in \mathbb{C}[\mathcal{T}]$. Hence $\mathcal{U}(\Gamma)/\mathbb{C}$ is an elliptic function field by Lemma 2.
For $\alpha \in \mathbb{C}$, any function $0 \neq f \in \mathcal{U}(\Gamma)$ has a Laurent series expansion

$$f(z) = \sum_{i=i_0}^{\infty} a_i (z-\alpha)^i, \qquad a_i \in \mathbb{C},\ i_0 \in \mathbb{Z},\ q_{i_0} \neq 0.$$

Let $v_\alpha : f \to v_\alpha(f) := i_0$ be a discrete valuation corresponding to $\alpha \in \mathbb{C}$, i.e. to the place $P_\alpha \in \mathbb{P}_{\mathcal{U}(\Gamma)/\mathbb{C}}$. It is obvious that $P_\alpha = P_\beta$ iff $\alpha \equiv \beta \mod \Gamma$. All places of the elliptic function field $\mathcal{U}(\Gamma)/\mathbb{C}$ are obtained in this manner.

Lemma 3. *Let F/K be an elliptic function field. Define*

$$\mathbb{P}_F^{(1)} := \{P \in \mathbb{P}_F \mid\ deg\, P = 1\}.$$

Then

1. *For any divisor $A \in D_F$ $deg\, A = 1$, there exists a unique place $P \in \mathbb{P}_F^{(1)}$ with $A \sim P$. In particular, $\mathbb{P}_F^{(1)} \neq 0$.*

2. *Fix a place $P_0 \in \mathbb{P}_F^{(1)}$. Then the map*

$$\begin{array}{rccc} \varphi : & \mathbb{P}_F^{(1)} & \longrightarrow & C_F^0, \\ & P & \longrightarrow & [P - P_0] \end{array}$$

is bijective.

Proof:

1. Let $A \in D_F$, $\deg A = 1$. Since $\dim A = \deg A - g + 1 > 0$, there is a divisor $A_1 \in D_F$, $A_1 \sim A$, $A_1 \geq 0$ ($\deg A_1 = \deg A = 1$, $\dim A_1 = \dim A > 0$) and it follows $A_1 \in \mathbb{P}_F^{(1)}$. This proves the existence.
   Suppose that $A \sim P$ and $A \sim Q$ for $P,\ Q \in \mathbb{P}_F^{(1)}$ and $P \neq Q$. Then $P \sim Q$, i.e. $\exists\ 0 \neq x \in F$ such that $P - Q = (x)$. It follows $(x)_0 = P,\ (x)_\infty = Q$ and so
   $$[F : K(x)] = \deg(x)_\infty = \deg(x)_0 = \deg P = \deg Q = 1,$$
   hence $F = K(x)$. This is in contradiction with the fact that F is an elliptic function field, i.e. $[F : K(x)] > 1$. This proves the uniqueness.

2. φ is surjective:
   Let $[B] \in C_F^0$. The divisor $B + P_0$ has degree one. By 1. there is a place $P \in \mathbb{P}_F^{(1)}$ with $B + P_0 \sim P$. Then $[B] = [P - P_0] = \varphi(P)$, and φ is surjective.
   φ is injective:
   Suppose $\varphi(P) = \varphi(Q)$ for $P,\ Q \in \mathbb{P}_F^{(1)}$. Then $P - P_0 \sim Q - P_0$, hence $P \sim Q$. By the uniqueness assertion in 1., it follows that $P = Q$.

■

The bijection φ of the foregoing proposition can be used to transport the group structure of C_F^0 to the set $\mathbb{P}_F^{(1)}$. This means that, for $P,\ Q \in \mathbb{P}_F^{(1)}$, we define

$$P \boxplus Q := \varphi^{-1}(\varphi(P) + \varphi(Q)). \tag{2.6}$$

Theorem 1. *Let F/K be an elliptic function field. Then*

1. *$\mathbb{P}_F^{(1)}$ is an abelian group w. r. to the operation $\boxplus$ defined in Equation (2.6).*

2. *The place P_0 is the neutral element of the group $\left(\mathbb{P}_F^{(1)}, \boxplus\right)$.*

3. *For $P,\ Q,\ R \in \mathbb{P}_F^{(1)}$, The following holds:*
   $$P \boxplus Q = R \Longleftrightarrow P + Q \sim R + P_0([P + Q] = [R + P_0]).$$

4. *The map $\varphi : \mathbb{P}_F^{(1)} \to C_F^0$ is isomorphism of abelian groups.*

Proof:

1., 2., 4. are trivial.
3. By Equation (2.6):

$$\begin{aligned} P \boxplus Q = R \Longleftrightarrow \varphi(R) = \varphi(P) + \varphi(Q) \quad &\Longleftrightarrow R - P_0 \sim (P - P_0) + (Q - P_0) \\ &\Longleftrightarrow P + Q \sim R + P_0 \end{aligned}$$

■

Remark 1. *The abelian group law on* $\mathbb{P}_F^{(1)}$ *is not completely canonical. The reason is that the isomorphism* φ *depends on the choice* $P_0 \in \mathbb{P}_F^{(1)}$. *If* F *is represented in the form* $F = K(x, y)$, *the usual choice is* $P_0 := Q_\infty$, *the pole of* $0 \neq x \in F$.

Chapter 3

Introduction

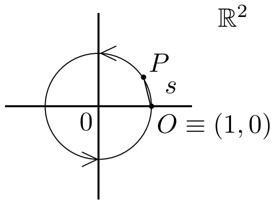
3.1 Comparison

Elementary theory (quadratic, rational, ...)		Elliptic curves
1. Arithmetic		
Pythagorean triples $a^2 + b^2 = c^2 \quad a, b, c \in \mathbb{N}$ gcd(a,b,c)=1	$\longleftrightarrow$	Rational solutions of $g(x, y) = 0,\ deg(g) = 3$
Roots of unity, division of circle, cyclotomic fields, 1-dimensional Galois representations	$\longleftrightarrow$	Points of finite order on elliptic curve, 2-dimensional Galois representations
2. Function theory		
arcsin, arccos $\int R(x, \sqrt{f(x)})\mathrm{d}x,\ deg(f) = 2$	$\longleftrightarrow$	Elliptic integrals $\int R(x, \sqrt{f(x)})\mathrm{d}x,\ deg(f) = 3, 4$
sin, cos (periods=2π)	$\longleftrightarrow$	Elliptic functions (periods= $\omega_1,\ \omega_2$) (($\omega_1,\ \omega_2$) are $\mathbb{R}$-independent)
$\big(R(x, y)$= a rational function of $x, y\big)$		
3. Geometry		
Conics (e.g. circles, parabolas, hyperbolas, ...) $g(x, y) = 0,\ deg(g) = 2$	$\longleftrightarrow$	Elliptic curves $g(x, y) = 0,\ deg(g) = 3$ (e.g. $y^2 = f(x),\ deg(f) = 3$)
Projective equivalence of conics	$\longleftrightarrow$	Families of (non-equivalent) elliptic curves (with levels), parameterized by modular curves

3.2 Elementary Theory (Motivation)

We shall present several motivating examples closely connected with the emergence of the theory of elliptic curves. This list is, of course, by no means complete, and could be hardly exhausted during any reasonable course.

3.2.1 Geometry and Topology of Complex Circles



Consider the (real) unit circle $C(\mathbb{R}) := \{(x,y) \in \mathbb{R}^2 \,|\, x^2 + y^2 = 1\}$ with a distinguished point $O \equiv (1,0) \in C(\mathbb{R})$. Let $s = s(x,y) = s(x,y(x))$ denotes the arclength $|OP|$. In the space of quadratic differentials holds $(\mathrm{d}s(x,y(x)))^2 = (\mathrm{d}x)^2 + (\mathrm{d}y(x))^2$, and because the function $\begin{array}{llll} f: & \mathbb{R}^2 & \longrightarrow & \mathbb{R} \\ & (x,y) & \longrightarrow & x^2+y^2-1 \end{array}$ is trivial on $C(\mathbb{R})$, we get (on $C(\mathbb{R})$)

$$0 = \mathrm{d}f = \mathrm{d}(x^2 - y^2 - 1) = 2x\mathrm{d}x + 2y\mathrm{d}y.$$

Combining these two results implies

$$\begin{aligned} \mathrm{d}x &= -\frac{y}{x}\mathrm{d}y, \\ (\mathrm{d}s)^2 &= \frac{(\mathrm{d}y)^2}{x^2} \Rightarrow \mathrm{d}s(x,y(x)) = \frac{\mathrm{d}y(x)}{x} = -\frac{\mathrm{d}x}{y(x)} \end{aligned}$$

and so the arclength $s = |OP|$ ($P \equiv (x,y) \in C(\mathbb{R})$) is

$$s = \int_0^y \frac{\mathrm{d}t}{\sqrt{1-t^2}} = \arcsin(y),$$

i.e. the inverse of the function

$$y \longrightarrow s(y(x)) = \int_0^y \frac{\mathrm{d}t}{\sqrt{1-t^2}} = \arcsin(y(x))$$

is

$$\begin{aligned} s(y(x)) &\longrightarrow y(s) = \sin(s), \\ s(x) &\longrightarrow x(s) = \frac{\mathrm{d}y(s)}{\mathrm{d}s} = \cos(s). \end{aligned}$$

The conclusion is that the **circle is transcendentally parametrized** by $(x(s), y(s)) = (\cos(s), \sin(s))$.

Addition of points on $\mathbf{C}(\mathbb{R})$, abelian group law on $\mathbf{C}(\mathbb{R})$

Let $P_i = (x_i, y_i) = (\cos(s_i), \sin(s_i))$, $i = 1, 2$ be a two points on $C(\mathbb{R})$. Let $(C(\mathbb{R}), \boxtimes, O)$ be abelian group defined by

$$(P_1, P_2) \longmapsto P := P_1 \boxtimes P_1 = (cos(s_1 + s_2), sin(s_1 + s_2)),$$

where $P \in C(\mathbb{R})$ is the point corresponding to the arclength $s = |OP| = s_1 + s_2$. The addition formulas for transcendental functions sin, cos

$$\cos(s_1 + s_2) = \cos(s_1)\cos(s_2) - \sin(s_1)\sin(s_2),$$

$$\sin(s_1 + s_2) = \cos(s_1)\sin(s_2) + \cos(s_2)\sin(s_1)$$

become algebraic when written in terms of coordinates (i.e. regular functions on $C(\mathbb{R})$) of the points of $C(\mathbb{R})$:

$$\begin{array}{rl} \text{(addition)} & (x_1, y_1) \boxtimes (x_2, y_2) = (x_1x_2 - y_1y_2, x_1y_2 + x_2y_1) \equiv (x_3, y_3), \\ \text{(inverse)} & (x_1, y_1) \boxtimes -(x_1, y_1) = (x_1, y_1) \boxtimes (x_1, -y_1) = (1, 0) = O. \end{array}$$

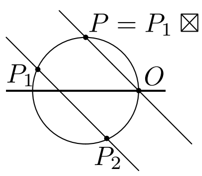
If $y \to s(y) = \int_0^y \frac{\mathrm{d}t}{\sqrt{1-t^2}}$ is the definition of the inverse of $s \mapsto y(s) = \sin(s)$, the abelian group structure reduces to

$$\int_0^{y_1} \frac{\mathrm{d}t}{\sqrt{1-t^2}} + \int_0^{y_2} \frac{\mathrm{d}t}{\sqrt{1-t^2}} = \int_0^{y_3} \frac{\mathrm{d}t}{\sqrt{1-t^2}}$$

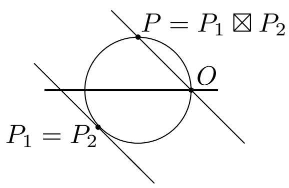
The key motive is that the addition formula for the transcendental function $\arcsin(y)$ on $C(\mathbb{R})$ is controlled by the algebraic rule.

Geometry of the group law on $\mathbf{C}(\mathbb{R})$

Let $(P_1, P_2) \longmapsto P := P_1 \boxtimes P_2$ be the group law on $C(\mathbb{R})$, $P_1, P_2, P \in C(\mathbb{R})$. Then this additive law is described by the following picture:



$(P_1 \neq P_2)$ resp.



(as a degenerate configuration of the previous generic case).

Complex locus C($\mathbb{C}$) of C

The complex valued function in the domain of the complex plane $\mathbb{C}$,

$$y \in \mathbb{C} \longrightarrow \sqrt{1-y^2} \in \mathbb{C},$$

is not a single valued function. The solution, proposed by Riemann, is to consider both roots of $\sqrt{1-y^2}$ in the complex plane simultaneously, i.e. to work with so called Riemann surface C($\mathbb{C}$) of (multivalued) analytic function $\sqrt{1-y^2}$. In other words $C(\mathbb{R}) \subset C(\mathbb{C})$, where

$$C(\mathbb{C}) := \{(x,y) \in \mathbb{C}^2 \,|\, x^2+y^2=1\}$$

is usually realized as a Riemann surface with a twofold covering of $\mathbb{C}$

$$\begin{array}{rcl} p: C(\mathbb{C}) & \longrightarrow & \mathbb{C} \\ (x,y) & \longrightarrow & y \end{array} \quad \text{ramified at } y = \pm 1.$$

The function $f(x,y) = x$ is then single valued holomorphic function on $C(\mathbb{C})$. The same conclusion holds for the differential $\omega = \frac{\mathrm{d}x}{y} = -\frac{\mathrm{d}y}{x}$. Summarizing - the Riemann surfaces are natural domains of definition of holomorphic functions that would otherwise be multivalued when considered as functions defined on open subsets of $\mathbb{C}$.

Abel-Jacobi map

In the case of a complex rational curve, $C(\mathbb{C})$, the substitute for $\int_{C(\mathbb{R})} \omega$, $\omega = \frac{\mathrm{d}x}{y} = -\frac{\mathrm{d}y}{x}$, is the Lebesgue integral

$$\int_O^P \omega = \int_O^P \frac{\mathrm{d}y}{x}$$

over piece-wise C^∞-differentiable path $p : \langle 0,1\rangle \to |OP|_t$, $P = (x_P, y_P) \in C(\mathbb{C})$, $O = (x_O, y_O) \in C(\mathbb{C})$. Because $\mathrm{d}\omega = \overline{\partial}\omega = O$ for holomorphic differentials on Riemann surfaces, the Stokes theorem gives

$$\int_{\partial A} \omega = \int_A \mathrm{d}\omega = 0$$

for any C^∞-differentiable 2-chain A (and its C^∞-differentiable 1-boundary ∂A). This implies that the integral $\int_c \omega$ along any C^∞-differentiable 1-cycle c depends only on the homology class of c in the homology group, $[c] \in H_1(C(\mathbb{C}), \mathbb{Z})$. Note that the 1-cycle $c = p * (-p')$ comes from two piecewise C^∞-differentiable maps $\left\{ \begin{array}{l} p : \langle 0,1\rangle \to |OP|_t \\ p' : \langle 0,1\rangle \to |OP|_t \end{array} \right\}$ and their composition $c = p*(-p')$ in the first homotopy group $\pi_1(C(\mathbb{C}))$ of $C(\mathbb{C})$.
In our case

$$H_1(C(\mathbb{C}), \mathbb{Z}) = \mathbb{Z}[\gamma], \;\; \gamma := C(\mathbb{R}) \text{ (with positive orientation)},$$

which means

$$[p * (-p')] = n[\gamma], \;\; n \in \mathbb{Z},$$

and so

$$\int_p \omega - \int_{p'} \omega = n \int_\gamma \omega = 2\pi n \in 2\pi\mathbb{Z}$$

is an integral multiple of the period of ω along γ

$$\int_\gamma \omega = 2 \int_{-1}^{1} \frac{\mathrm{d}t}{\sqrt{1-t^2}} = 2\pi.$$

The result is that the integral is defined modulo the group of periods

$$\left\{ \int_c \omega \mid [c] \in H_1(C(\mathbb{C}), \mathbb{Z}) \right\} \equiv 2\pi\mathbb{Z}$$

and gives the **Abel-Jacobi map**

$$\begin{array}{ccc} C(\mathbb{C}) & \longrightarrow & \mathbb{C}/2\pi\mathbb{Z} \\ P & \longrightarrow & \displaystyle\int_O^P \omega \pmod{2\pi\mathbb{Z}} \end{array}$$

as a complex variant of the real case of the function arcsin.

3.2.2 Arithmetic

Definition 2. *$r \in \mathbb{Q}^+$ is the congruent number* $\Leftrightarrow \exists$ $\underset{x}{\overset{z}{\triangle}}\,y$ $\quad \begin{array}{l} x, y, z \in \mathbb{Q} \\ P(\triangle) = r \end{array}$.

It is clear that $\forall r \in \mathbb{Q}\ \exists s \in \mathbb{Q} : s^2 r$ is a square free integer, i.e. $s^2 r \in (\mathbb{Z}/\mathbb{Z}^2)^+$:

$$\left\{ \begin{array}{c} x \\ y \\ z \end{array} \right\} \overset{s}{\longrightarrow} \left\{ \begin{array}{c} sx \\ sy \\ sz \end{array} \right\}$$ has area $s^2 r \Rightarrow$ assume $r \in \mathbb{Z}^+/(\mathbb{Z})^2$ $(r = n,$ $n \in \mathbb{Z}$ square free)

Example 2.

$$\left. \begin{array}{l} x = 1\frac{3}{2} \\ y = 6\frac{2}{3} \\ z = 6\frac{5}{6} \end{array} \right\} \longleftrightarrow n = 5 \textit{ (}n = 5 \textit{ is the smallest congruent number)}$$

Suppose the situation $x, y, z \in \mathbb{Q}$, $n \in \mathbb{N}$: $\underset{x}{\overset{z}{\triangle}}\,y$ *i.e.* $\begin{array}{l} x^2 + y^2 = z^2, \\ xy = 2n. \end{array}$

We can assume $x < y < z$ ($z \ldots$ the hypotenuse, $x, y \ldots$ the legs, $x \neq y$ because $2x^2 = z^2$, $x = \frac{\sqrt{2}}{2} z$ and so it cannot happen $x \in \mathbb{Q} \wedge z \in \mathbb{Q}$).

Theorem 2. *Let $n \in \mathbb{Z}^+/(\mathbb{Z})^2$. Let $X, Y, Z, x \in \mathbb{Q}^+$, $X < Y < Z$. Then there is a bijection*

$$\left\{ \underset{X}{\overset{Z}{\triangle}}\,Y, \quad P(\triangle) = n \right\} \overset{1:1}{\longleftrightarrow} \left\{ x \in \mathbb{Q}^+ : x, x+n, x-n \in \mathbb{Q}^2 \right\}$$

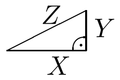
$$X, Y, Z \quad \longrightarrow \quad x = \left(\frac{Z}{2}\right)^2$$

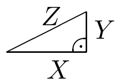
$$\left.\begin{array}{l} X = \sqrt{x+n} - \sqrt{x-n} \\ Y = \sqrt{x+n} + \sqrt{x-n} \\ Z = 2\sqrt{x} \end{array}\right\} \quad \longleftarrow \quad x$$

Proof: If $\left.\begin{array}{c} X^2+Y^2=Z^2 \\ XY=2n \end{array}\right\} \Rightarrow \left.\begin{array}{c} (X \pm Y)^2 = Z^2 \pm 4n \\ \left(\frac{X \pm Y}{2}\right)^2 = \left(\frac{Z}{2}\right)^2 \pm n \end{array}\right\} \Rightarrow x = \left(\frac{Z}{2}\right)^2$ has desired property, because $x \pm n$ are squares of $\left(\frac{X \pm Y}{2}\right)$. The converse and uniqueness is clear. ■

Another characterization:

$\left(\frac{X \pm Y}{2}\right)^2 = \left(\frac{Z}{2}\right)^2 \pm n$, so after multiplication " $+$ " with " $-$ " $\left(\frac{X^2-Y^2}{4}\right)^2 = \left(\frac{Z}{2}\right)^4 - n^2$ and the equation $u^4 - n^2 = v^2$ has rational solution $(u,v) : u = \frac{Z}{2}$, $v = \frac{X^2-Y^2}{4}$. Let us multiply by u^2 : $u^6 - n^2u^2 = u^2v^2 = (uv)^2$ and set $\left.\begin{array}{l} x = u^2 = \left(\frac{Z}{2}\right)^2 \\ y = uv = \frac{(X^2-Y^2)Z}{8} \end{array}\right\} \Rightarrow y^2 = x^3 - n^2x$ is a cubic curve with rational solution $(x,y) \in \mathbb{Q} \times \mathbb{Q}$. Hence we have proved:

Theorem 3.
If $\exists$  *with* $P(\triangle) = n \Rightarrow \exists (x,y) \in \mathbb{Q} \times \mathbb{Q} :\ y^2 = x^3 - n^2x$ (the notation $C : y^2 = x^3 - n^2x$)

Remark 2. *The inverse implication "$\Leftarrow$" is not true. However a given point* $P \equiv (x,y) \in \mathbb{Q} \times \mathbb{Q} : y^2 = x^3 - n^2x$ *yields*  $P(\triangle) = n$ *if* $\exists\, P' \in C(\mathbb{Q})$:

$P' \boxtimes P' = P$ *for* $\boxtimes$ *being the group law on this elliptic curve.*

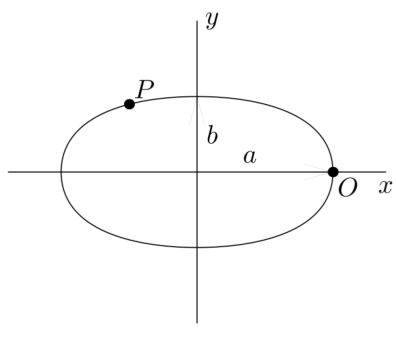
3.2.3 Function theory (elliptic integrals)

Definition 3. *An* **elliptic** *integral is an expression of the form*

$$I = \int R(x, \sqrt{f(x)})\mathrm{d}x,$$

where $R(x,y)$ *is a rational function of* x, y *and* $f(x) \in \mathbb{C}[x]$ *is a square free polynomial of degree* $n = 3, 4$.

Remark 3. *If degree of* f *is* $n = 1, 2$*, then the integral* I *is an elementary function. For example, for* $f(x) = 1 - x^2$ *leads the substitution* $x = \frac{t^2-1}{t^2+1}$ *to an integral of a rational function of* t.



Arclength of an ellipse

An ellipse

$$\left(\frac{x}{a}\right)^2+\left(\frac{y}{b}\right)^2=1 \quad (a\geq b>0)$$

can be parametrized by $x=a\cos\varphi,\ y=b\sin\varphi$ ($\varphi\in\langle 0,2\pi)$). Its arclength $s=s(x_0,y_0)$ ($P\equiv(x_0,y_0)$, $O=(a,0)$) satisfies (in the space of symmetric quadratic differentials)

$$(ds)^2=(dx)^2+(dy)^2=(a^2\sin^2\varphi+b^2\cos^2\varphi)(\mathrm{d}\varphi)^2=a^2(1-k^2\cos^2\varphi)(\mathrm{d}\varphi)^2,$$

where $k^2=1-\frac{b^2}{a^2}>0$. The normalization of the long axis of the ellipse to $a=1$ yields $b=\sqrt{1-k^2}$ and so

$$\mathrm{d}x=-\sin\varphi\mathrm{d}\varphi,\ (\mathrm{d}x)^2=(1-x^2)(\mathrm{d}\varphi)^2,\ (ds)^2=\frac{1-k^2x^2}{1-x^2}(dx)^2,$$

hence

$$s=\int\sqrt{\frac{1-k^2x^2}{1-x^2}}\,\mathrm{d}x=\int\frac{1-k^2x^2}{\sqrt{(1-k^2x^2)(1-x^2)}}\,\mathrm{d}x.$$

Chapter 4

Differentials

Beside the traditional rôle in the calculus on algebraic curves, differentials will allow us to determine when an algebraic map between algebraic curves is separable.

Definition 4. *Let C be a curve. The space of (meromorphic) differential forms on C, Ω_C, is the $\overline{K}(C)$—vector space generated by symbols of the form dx for $x \in \overline{K}(C)$, subject to the normal relation:*

$$\begin{aligned} &1/\ d(x+y) = dx + dy && \forall x, y \in \overline{K}(C), \\ &2/\ d(xy) = xdy + ydx && \forall x, y \in \overline{K}(C), \\ &3/\ da = 0 && \forall a \in \overline{K}, \end{aligned} \tag{4.1}$$

This definition is equivalent to the adelic one, although we shall not prove it. Let C_1/K and C_2/K be algebraic curves and $\varphi : C_1 \to C_2$ a non-constant rational map defined over K. Then composition with φ induces an injection of function fields (fixing K),

$$\begin{aligned} \varphi^* : K(C_2) &\longrightarrow K(C_1), \\ f &\longmapsto \varphi^* f := f \circ \varphi. \end{aligned} \tag{4.2}$$

For a non-constant map φ, $K(C_1)$ is a finite extension of $\varphi^* K(C_2)$, i.e. $[K(C_1) : \varphi^* K(C_2)] < \infty$.

Definition 5. *Let $\varphi : C_1 \to C_2$ be a map of curves defined over K. If φ is constant, we define the degree of φ to be 0, otherwise we say that φ is finite, and define its degree by*

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

We say that φ is separable (inseparable, purely inseparable) if the extension $K(C_1)/\varphi^* K(C_2)$ has he corresponding property, and we denote corresponding degrees (separable, inseparable) by $deg_s\, \varphi$, $deg_i\, \varphi, \ldots$

For a non-constant map of curves C_1, C_2, $\varphi : C_1 \to C_2$, the map φ^* induces a map on differentials

$$\begin{aligned} \varphi^* : \Omega_{C_2} &\longrightarrow \Omega_{C_1} \\ \sum_i f_i \mathrm{d}\, x_i &\longrightarrow \varphi^*\Big(\sum_i f_i \mathrm{d}\, x_i\Big) := \sum_i (\varphi^* f_i)\, \mathrm{d}\, (\varphi^* x_i)\,. \end{aligned} \tag{4.3}$$

This map provides a useful criterion for determining when φ is separable.

Theorem 4. *Let C/K be a curve. Then*

1/ Ω_C is a $1-$dimensional $\overline{K}(C)$-vector space;

2/ Let $x \in \overline{K}(C)$. Then dx is a $\overline{K}(C)$ basis for Ω_C if and only if $\overline{K}(C)/\overline{K}(x)$ is a finite separable extension;

3/ Let $\varphi : C_1 \to C_2$ be a non-constant map of curves. Then φ is separable if and only if the map $\varphi^* : \Omega_{C_2} \to \Omega_{C_1}$ is injective (equivalently, non-zero).

For the sake of reader's convenience we recall the basics of morphisms between projective varieties.

Definition 6. *Let $\mathbb{V}_1, \mathbb{V}_2 \subset \mathbb{P}^n$ be projective varieties. A rational map from $\mathbb{V}_1$ to $\mathbb{V}_2$ is a map*

$$\begin{aligned} \varphi : \mathbb{V}_1 &\longrightarrow \mathbb{V}_2 \\ \varphi &\equiv [f_0, \dots, f_n], \end{aligned} \tag{4.4}$$

where $f_0, \dots, f_n \in \overline{K}\,(\mathbb{V}_1)$ are rational functions with property that $\forall P \in \mathbb{V}_1$ at which $f_0, \dots, f_n$ are regular,

$$\varphi(P) = [f_0(P), \dots, f_n(P)] \in \mathbb{V}_2.$$

If $\mathbb{V}_1/K, \mathbb{V}_2/K$, then $\mathrm{Gal}\left(\overline{K}/K\right)$ acts on φ by

$$\varphi^g(P) := [f_0^g(P), \dots, f_n^g(P)]\,,\; g \in \mathrm{Gal}\left(\overline{K}/K\right).$$

Notice that

$$(\varphi(P))^g = \varphi^g\left(P^g\right),\; P \in \mathbb{V}_1,\; g \in \mathrm{Gal}\left(\overline{K}/K\right).$$

A rational map $\varphi : \mathbb{V}_1 \to \mathbb{V}_2$ is not necessarily a function on all of $\mathbb{V}_1$. However, it is sometimes possible to evaluate $\varphi(P)$ at points $P \in \mathbb{V}_1$ where some f_i is not regular by replacing

$$f_i \longrightarrow g f_i \quad \forall i = 0, \dots, n\,,\; g \in \overline{K}\,(\mathbb{V}_1)\,.$$

Definition 7. *A rational map*

$$\begin{aligned} \varphi : \mathbb{V}_1 &\longrightarrow \mathbb{V}_2 \\ \varphi &\equiv [f_0, \dots, f_n],\; f_i \in \overline{K}\,(\mathbb{V}_1)\; (\forall i)\,. \end{aligned} \tag{4.5}$$

is regular at $P \in \mathbb{V}_1$ if there is $g \in \overline{K}\,(\mathbb{V}_1)$ such that

1/ $g_i f_i$ *is regular at* $P\, \forall i = 0, \ldots, n,$ *and*

2/ $\exists i \in \{0, \ldots, n\} : (gf_i)\,(P) \neq 0.$

If g *exists, we set*

$$\varphi(P) = [(gf_0)(P), \ldots, (gf_n)(P)]\,.$$

A rational map, regular at every point of $\mathbb{V}_1$*, is called a morphism.*

Proposition 1. *Let* $P \in C$*,* $t \in \overline{K}(C)$ *be a uniformizing variable (parameter) at* P*.*

1/ For every $\omega \in \Omega_C$ *there exists a unique* $g \in \overline{K}(C)$*, depending on* ω, t *such that*

$$\omega = g\, d\, t.$$

2/ Let $f \in \overline{K}(C)$ *be regular at* P*. Then* $\frac{d\,f}{d\,t}$ *is also regular at* P*. (take* $\omega = d\,f$*, then* $\frac{d\,f}{d\,t}$ *is an element of* $\overline{K}(C)$*).*

3/ The quantity

$$ord_P\left(\frac{\omega}{d\,t}\right)$$

depends only on ω *and* P*, independent of the choice of uniformizer* t*. We call this value the order of* ω *at* P*, and denote it by* $ord_P\,(\omega)$*.*

4/ Let $char\,(K) = p,\ x, f \in \overline{K}(C)$ *with* $x(P) = 0$*. Then*

$$\begin{aligned} ord_P\,(f\,d\,x) &= ord_P\,(f) + ord_P\,(x) - 1 && \text{if } p = 0 \text{ or } p \nmid ord_P\,(x)\,, \\ ord_P\,(f\,d\,x) &\geq ord_P\,(f) + ord_P\,(x) && \text{if } p > 0 \text{ and } p \mid ord_P\,(x)\,. \end{aligned} \tag{4.6}$$

5/ For all but finitely many $P \in C$*,*

$$ord_P\,(\omega) = 0.$$

Proof:

We shall prove only 3/,4/, because the other items require some further prerequisities.

3/ Let t' be another uniformizer at P. Then from 2/ $\frac{\mathrm{d}\,t}{\mathrm{d}\,t'}$, $\frac{\mathrm{d}\,t'}{\mathrm{d}\,t}$ are both regular at P, so $\mathrm{ord_P}\left(\frac{\mathrm{d}\,t'}{\mathrm{d}\,t}\right) = 0$. Since

$$\omega = g\mathrm{d}\,t' = g\left(\frac{\mathrm{d}\,t'}{\mathrm{d}\,t}\right)\mathrm{d}\,t,$$

the result follows.

4/ Write $x = ut^n$ with $n = \mathrm{ord_P}\,(x) \geq 0\,(\Leftarrow x(P) = 0)$. Then

$$\mathrm{d}\,x = \left[nut^{n-1} + \left(\frac{\mathrm{d}\,u}{\mathrm{d}\,t}\right)t^n\right]\mathrm{d}\,t.$$

It follows from 2/ that $\frac{\mathrm{d}\,u}{\mathrm{d}\,t}$ is regular at P, so provided $n \neq 0$, the first term dominates (i.e. $nut^{n-1} + \left(\frac{\mathrm{d}\,u}{\mathrm{d}\,t}\right)t^n = nut^{n-1}\left(1 + \frac{1}{nu}\frac{\mathrm{d}\,u}{\mathrm{d}\,t}t\right)$ for $P-$unit $\left(1 + \frac{1}{nu}\frac{\mathrm{d}\,u}{\mathrm{d}\,t}t\right)$) and we obtain

$$\mathrm{ord_P}\,(f\mathrm{d}\,x) = \mathrm{ord_P}\left(fnut^{n-1}\mathrm{d}\,t\right) = \mathrm{ord_P}\,(f) + n - 1.$$

Finally, if $p > 0$ and $p \mid n$, then the first term vanishes and we get

$$\mathrm{ord_P}\,(f\mathrm{d}\,x) = \mathrm{ord_P}\left(f\frac{\mathrm{d}\,u}{\mathrm{d}\,t}t^n\mathrm{d}\,t\right) \geq \mathrm{ord_P}\,(f) + n.$$

Note that $\mathrm{ord_P}\left(\frac{\mathrm{d}\,u}{\mathrm{d}\,t}\right) \geq 0$ for a unit $u \in \mathcal{O}_P\backslash P \equiv \mathcal{O}_P^*$ $(u = \alpha + \beta t + \gamma t^2 + \ldots)$ for $\alpha \neq 0 \Rightarrow \frac{\mathrm{d}\,u}{\mathrm{d}\,t} = \beta + 2\gamma t + \ldots$ for $\beta, \gamma \in K$.

■

Definition 8. *Let $\omega \in \Omega_C$. The divisor associated to ω is*

$$\mathrm{div}\,(\omega) = \sum_{P \in C} ord_P\,(\omega)\,(P) \in Div\,(C)\,.$$

A differential ω is regular (or holomorphic) if

$$ord_P\,(\omega) \geq 0 \quad \forall P \in C.$$

It is non-vanishing if

$$ord_P\,(\omega) \leq 0 \quad \forall P \in C.$$

The canonical divisor class on C is the image Cl_F of $\mathrm{div}\,(\omega)$ *for any non-zero differential $\omega \in \Omega_C$. It is well-defined, because Ω_C is $1-$dim $F-$module. Any divisor in this divisor class is called canonical divisor.*

Ex. 3. *Let us show that there are no regular(holomorphic) differentials on $\mathbb{P}^1$. First, if t is a coordinate function on $\mathbb{P}^1$, then*

$$\mathrm{div}\,(dt) = -2(\infty), \quad \infty \equiv P_\infty \in \mathbb{P}_F.$$

Note that if t is uniformizing parameter of $\mathcal{O} \in \mathbb{P}_F$, then $\forall \alpha \in K$, $t - \alpha$ is a uniformizing variable at α, i.e.

$$ord_\alpha\,(dt) = ord_\alpha\,(d\,(t-\alpha)) = 0, \quad \forall \alpha \in K.$$

(we used 4/ of proposition 1, $ord_\alpha\,(dt) = ord_P\,(t) - 1 = 0$.)
However, at $P_\infty \in \mathbb{P}_F$, $\frac{1}{t}$ is the uniformizing variable, so

$$\begin{aligned} ord_\infty\,(dt) &= ord_\infty\left(-t^2 d\left(\frac{1}{t}\right)\right) = ord_\infty\left(-\frac{1}{\frac{1}{t^2}}d\left(\frac{1}{t}\right)\right) \\ &= ord_\infty\left(-\frac{1}{\frac{1}{t^2}}\right) + ord_\infty\left(d\left(\frac{1}{t}\right)\right) - 1 = -2 + 1 - 1 = -2, \end{aligned} \tag{4.7}$$

where we used

$$0 = d(1) = d\left(\frac{t}{t}\right) = t\,d\left(\frac{1}{t}\right) + \frac{1}{t}\,dt \implies dt = -t^2 d\left(\frac{1}{t}\right).$$

Thus dt is not regular, i.e. for any $\omega \in \Omega_{\mathbb{P}^1}$

$$\deg \operatorname{div}(\omega) = \deg \operatorname{div}(dt) = -2$$

and ω cannot be regular either.

Ex. 4. *Consider the smooth, elliptic curve $C : y^2 = x^3 + x$. Note that for valuation $P_{(0,0)}$ corresponding to $(0,0) \in C$, we have $x^3 + x = x(1 + x^2)$, i.e. $(1 + x^2)$ is unit in the local ring $\mathcal{O}_{P_{(0,0)}} \setminus P_{(0,0)}$ and the uniformizing variable of $P_{(0,0)}$ can be chosen as y (because $x = y^2$ in $\mathcal{O}_{P_{(0,0)}}$). Then, for example, for $x, y, 2y^2 - x$ we get*

$$\begin{aligned} &ord_{P_{(0,0)}}(y) = 1,\ ord_{P_{(0,0)}}(x) = 2, \\ &ord_{P_{(0,0)}}\left(2y^2 - x\right) = ord_{P_{(0,0)}}\left(2x^3 + x\right) = ord_{P_{(0,0)}}(x) + ord_{P_{(0,0)}}\left(2x^2 + 1\right) = 2 \end{aligned} \tag{4.8}$$

Ex. 5. *Assume $char(K) \neq 2$. Let $e_1, e_2, e_3 \in \overline{K}$ be distinct, and consider $C : y^2 = (x - e_1)(x - e_2)(x - e_3)$. C is smooth and it has a single point at infinity, which we will denote P_∞. For $i = 1, 2, 3$, let $P_i \equiv (e_i, 0) \in C$. Then it follows from the previous example*

$$\operatorname{div}(x - e_i) = 2(P_i) - 2(P_\infty)$$

and

$$\operatorname{div}(y) = (P_1) + (P_2) + (P_3) - 3(P_\infty).$$

Concerning differential of $x \in \overline{K}(C)$ we get

$$\operatorname{div}(dx) = (P_1) + (P_2) + (P_3) - 3(P_\infty),$$

because $ord_{e_i}(dx) = ord_{e_i}(d(x - e_i)) = ord_{e_i}(x - e_i) - 1 = 2 - 1 = 1$, and $P_\infty = P_{z=0}$ corresponds to $(zy^2 = x^3 + \alpha x^2 z + \beta x z^2 + \delta z^3)\ x^3 = 0$, i.e.

$$\begin{aligned} ord_{P_\infty}(dx) &= ord_{P_\infty}\left(-\frac{1}{\frac{1}{x^2}} d\left(\frac{1}{x}\right)\right) = ord_{P_\infty}\left(x^2\right) + ord_{P_\infty}\left(\frac{1}{x}\right) - 1 \\ &= -2 \cdot 2 + 2 - 1 = -3 \end{aligned} \tag{4.9}$$

(note that $ord_{P_0}(x) = 2 \Rightarrow ord_{P_\infty}(x) = -2$). This result nicely fits with the fact that $deg(dx) = 0$ for elliptic function field. We thus see that

$$\operatorname{div}\left(\frac{dx}{y}\right) = \operatorname{div}(dx) - \operatorname{div}(y) = 0,$$

hence $\frac{dx}{y}$ is both regular and non-vanishing differential.

Ex. 6. *Assume char*$(K) \neq 2$*, and let* $\mathbb{V} : x^2 + y^2 = z^2 \subseteq \mathbb{P}^2$*. Consider the rational map*

$$\begin{aligned} \varphi &: \mathbb{V} \longrightarrow \mathbb{P}^1, \\ \varphi &\equiv [x+z, y]. \end{aligned} \tag{4.10}$$

φ *is clearly regular except possibly* $[1, 0, -1]$ *(where* $x + z = 0 = y$*). But using*

$$(x+z)(x-z) = -y^2 \, mod \, I_{\mathbb{V}},$$

we get

$$\varphi = [x+z, y] = [x^2 - y^2, y(x-z)] = [-y^2, y(x-z)] = [-y, x-z].$$

Thus

$$\varphi([1, 0, -1]) = [0, 2] = [0, 1]$$

and so φ *is a morphism. One can check that the map*

$$\begin{aligned} \psi &: \mathbb{P}^1 \longrightarrow \mathbb{V} \\ \psi &\equiv [s^2 - t^2, 2st, s^2 + t^2] \end{aligned} \tag{4.11}$$

is a morphism and $\psi \circ \varphi = \varphi \circ \psi = \mathbb{I}$*.*

Chapter 5

The Frobenious map

Assume char $(K) = p > 0$, and let $q = p^r$. For any polynomial $f \in K[x_0, \ldots, x_n]$, let $f^{(q)} \in K[x]$ be defined by

$$\begin{aligned} f &\longmapsto f^{(q)}, \\ \sum_{i_0,\ldots i_n} a_i x_0^{i_0} \ldots x_n^{i_n} &\longmapsto \sum_{i_0,\ldots i_n} a_i^q x_0^{i_0} \ldots x_n^{i_n}. \end{aligned} \tag{5.1}$$

Then for a curve C/K, defined by $I(C) \subseteq K[x_0, \ldots, x_n]$, we define a new curve $C^{(q)}/K$ as $I(C^{(q)}) \equiv \{$ ideal generated by $f^{(q)} \mid f \in I(C)\}$. There is a natural map φ called $q-$th power Frobenious morphism, given by

$$\begin{aligned} \varphi : C &\longrightarrow C^{(q)}, \\ [x_0, \ldots, x_n] &\longrightarrow [x_0^q, \ldots, x_n^q]. \end{aligned} \tag{5.2}$$

Note that for every $P = [x_0, \ldots, x_n] \in C$, $\varphi(P)$ is zero for each generator $f^{(q)}$ of $I(C^{(q)})$:

$$f^{(q)}(\varphi(P)) = f^{(q)}(x_0^q, \ldots, x_n^q) \overset{\mathrm{char}(K)=p}{=} (f(x_0, \ldots, x_n))^q \overset{f(P)=0}{=} 0.$$

Ex. 7. *Let C be the curve in $\mathbb{P}^2$ given by (single) equation*

$$C: \; ax_0^3 + bx_1^3 + cx_2^3 = 0, \quad a, b, c \in K,$$

then

$$C^{(q)}: \; a^q x_0^3 + b^q x_1^3 + c^q x_2^3 = 0.$$

We shall describe basic properties of Frobenious maps.

Theorem 5. *Let K be a perfect field, char $(K) = p > 0$, $q = p^r$, C/K a curve, $\varphi : C \to C^{(q)}$ be a $q-$th power Frobenious morphism. Then*

1/ $\varphi^*(K(C^{(q)}) = K(C)^{(q)}$, $K(C)^{(q)} = \{f^q \mid f \in K(C)\}$.

2/ φ *is purely inseparable.*

3/ $deg(\varphi) = q$.

Proof (sketch)**:**

1/ Using the description of $K(C)$ as consisting of elements of the form $\frac{f}{g}$ of homogeneous polynomials, $\deg(f) = \deg(g)$, we get elements of $\varphi^*\left(K\left(C^{(q)}\right)\right)$:

$$\varphi^*\left(\frac{f}{g}\right) = \frac{f\left(x_0^q, \ldots, x_n^q\right)}{g\left(x_0^q, \ldots, x_n^q\right)}.$$

similarly, $K(C)^q$ is the subfield given by quotients $\frac{f(x_0,\ldots,x_n)^q}{g(x_0,\ldots,x_n)^q}$. Since K is perfect, $\forall a \in K\ \exists b \in K:\ a = b^q$, so

$$\Big(K[x_0, \ldots, x_n]\Big)^q = K[x_0^q, \ldots, x_n^q],$$

and the two subfields $\varphi^*\left(K\left(C^{(q)}\right)\right)$, $K(C)^{(q)}$ of $K(C)$ are isomorphic.

2/ This follows from 1/.

3/ It is based on the properties of representation $\deg\varphi = [K(C)^{(q)}(t) : K(C)^{(q)}]$, where $K(C) = K(C)^{(q)}(t)$ and $t \in K(C)$ is a unimorfizer at some smooth $P \in C$. Note that $[K(C) : K(t)]$ is separable extension.

■

Corollary 1. *Every map* $\tilde{\varphi}: C_1 \to C_2$ *of smooth algebraic curves over a field* K*,* $char(K) = p > 0$*, factors as*

$$\tilde{\varphi} = \lambda\varphi:\ C_1 \xrightarrow{\varphi} C_1^{(q)} \xrightarrow{\lambda} C_2,$$

where $deg(\tilde{\varphi}) = q$*,* φ *is the* $q-th$ *power Frobenious map (i.e. it is purely inseparable) and* λ *is separable.*

Proof:

Let S be the separable closure of $\tilde{\varphi}^*K(C_2)$ in $K(C_1)$. Then $K(C_1)/S$ is purely inseparable of degree q, so $K(C_1)^{(q)} \subset S$. It follow from previous theorem 5, 1/,3/,

$$K(C_1)^{(q)} = \varphi^*\left(K\left(C_1^{(q)}\right)\right), \left[K(C_1) : \varphi^*\left(K\left(C_1^{(q)}\right)\right)\right] = q.$$

Hence by comparing degrees, $S = \varphi^*\left(K\left(C_1^{(q)}\right)\right)$. We have the tower of field extensions:

$$K(C_1) \supseteq \varphi^*\left(K\left(C_1^{(q)}\right)\right) \supseteq \tilde{\varphi}^*(K(C_2)).$$

It follows from the following result:

Let $i : K(C_2) \rightarrow K(C_1)$ be an injection of functions fields (fixing K). Then there exists a unique non-constant map $\tilde{\varphi} : C_1 \rightarrow C_2$ defined over K such that $\tilde{\varphi}^* = i$, that the extension **??** corresponds to maps

$$\begin{tikzcd} C_1 \arrow[r, "\varphi"] \arrow[rr, bend right, "\tilde{\varphi}"'] & C_1^{(q)} \arrow[r, "\lambda"] & C_2. \end{tikzcd} \tag{5.3}$$

■

Chapter 6

Normal Forms and its Invariants

Recall that we have proved that on elliptic curve E/K there exist function $x, y \in K(E)$ such that the map

$$\begin{aligned} &\varphi : E \longrightarrow \mathbb{P}^2 \\ &\varphi \equiv [x, y, 1],\ \varphi(0) = [0, 1, 0]\,. \end{aligned} \tag{6.1}$$

gives isomorphism of E/K onto the curve given by Weierstrass equations

$$E/K:\ y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6, \quad a_1, \ldots, a_6 \in K\,. \tag{6.2}$$

Theorem 6. *Any two Weierstrass equations for E/K are related by a linear change of variables of the form*

$$\begin{aligned} x &= u^2x' + r\,, \\ y &= u^3y' + su^2x' + t, \quad u, r, s, t \in K, u \neq 0\,. \end{aligned} \tag{6.3}$$

Proof: Let $\{x, y\}, \{x', y'\}$ be two sets of Weierstrass coordinate functions on E/K. Then $x, x' \in \mathcal{L}\big(2(O)\big)\backslash\mathcal{L}\big((O)\big)$, $y, y' \in \mathcal{L}\big(3(O)\big)\backslash\mathcal{L}\big(2(O)\big)$, where $O \in E/K$. Hence $\{1, x\}, \{1, x'\}$ are both bases for $\mathcal{L}\big(2(O)\big)$, and similarly $\{1, x, y\}$ resp. $\{1, x', y'\}$ are both bases for $\mathcal{L}\big(3(O)\big)$. It follows that there are $u_1, u_2, r, s_3, t \in K$, $u_1u_2 \neq 0$ such that

$$\begin{aligned} x &= u_1x' + r\,, \\ y &= u_2y' + s_2x' + t\,. \end{aligned} \tag{6.4}$$

But $(x, y), (x', y')$ both satisfy Weierstrass equation in which the coefficients of y^2 and x^3 are 1, i.e. $u_1^3 = u_2^2$. Letting $u = \frac{u_2}{u_1}$, $s = \frac{s_2}{u^2}$ puts the change of variable formula in the desired form. ■

It it straightforward to verify, for

$$\begin{aligned} y^2 + a_1xy + a_3x \;&=\; x^3 + a_2x^2 + a_4x + a_6\,, \\ y'^2 + a'_1x'y' + a'_3y' \;&=\; x'^3 + a'_2x'^2 + a'_4x' + a'_6\,, \end{aligned} \tag{6.5}$$

the transformation rules (Eq. (6.3))

$$\begin{aligned} ua'_1 \;&=\; a_1 + 2s\,, \\ u^2a'_2 \;&=\; a_2 - sa_1 + 3r - s^2\,, \\ u^3a'_3 \;&=\; a_3 + ra_1 + 2t\,, \\ u^4a'_4 \;&=\; a_4 - sa_3 + 2ra_2 - (t+rs)a_1 + 3r^2 - 2st\,, \\ u^6a'_6 \;&=\; a_6 + ra_4 + r^2a_2 + r^3 - ta_3 - rta_1 - t^2\,. \end{aligned} \tag{6.6}$$

Associated to the coefficient $a_1, \ldots, a_6 \in K$ in the Weierstrass cubic for (6.2) there are

$$\begin{aligned} b_2 \;&=\; a_1^2 + 4a_2\,, \\ b_4 \;&=\; a_1a_3 + 2a_4\,, \\ b_6 \;&=\; a_3^2 + 4a_6\,, \\ b_8 \;&=\; a_1^2a_6 - a_1a_3a_4 + 4a_2a_6 + a_2a_3^2 - a_4^2\,. \end{aligned} \tag{6.7}$$

These quantities are related by $4b_8 = b_2b_6 - b_4^2$. We introduce the discriminant by

$$\Delta = -b_2^2b_8 - 8b_4^3 - 27b_6^2 + 9b_2b_4b_6\,. \tag{6.8}$$

Under an admissible change of variable (6.4), we get

$$\begin{aligned} u^2b'_2 \;&=\; b_2 + 12r\,, \\ u^4b'_4 \;&=\; b_4 + rb_2 + 6r^2\,, \\ u^6b'_6 \;&=\; b_6 + 2rb_4 + r^2b_2 + 4r^3\,, \\ u^8b'_8 \;&=\; b_8 + 3rb_6 + 3r^2b_4 + 3r_4\,, \\ u^{12}\Delta' \;&=\; \Delta\,. \end{aligned} \tag{6.9}$$

The last variables are

$$\begin{aligned} c_4 \;&=\; b_2^2 - 24b_4\,, \\ c_6 \;&=\; -b_2^3 + 36b_2b_4 - 216b_6\,, \\ j \;&=\; \frac{c_4^3}{\Delta} \quad (\text{for } \Delta \text{ invertible})\,, \end{aligned} \tag{6.10}$$

with relation:

$$12^3\Delta = c_4^3 - c_6^2 \Longrightarrow j = 12^3\frac{c_4^3}{c_4^3 - c_6^2}\,. \tag{6.11}$$

and the transformation rule

$$\begin{aligned} u^4c'_4 \;&=\; c_4\,, \\ u^6c'_6 \;&=\; c_6\,, \\ j' \;&=\; j\,. \end{aligned} \tag{6.12}$$

If two elliptic curves E/K, E'/K are isomorphic, then $j(E') = j(E)$. We take up the question of when the Weierstrass normal form defines a nonsingular curve. Let $P = (x_0, y_0)$ be a point satisfying a Weierstrass equation

$$f(x,y) = y^2 + a_1xy + a_3y - x^3 - a_2x^2 - a_4x - a_6 = 0\,. \tag{6.13}$$

By definition, $P(x_0, y_0)$ is a singular (non-smooth) point on the curve $f(x,y) = 0$ iff $\frac{\partial f}{\partial x}(P) = \frac{\partial f}{\partial y}(P) = 0$. The Taylor expansion of f at P has the form

$$f(x,y) - f(x_0,y_0) = [(y-y_0)-\alpha(x-x_0)][(y-y_0)-\beta(x-x_0)] - (x-x_0)^3 \tag{6.14}$$

for some $\alpha, \beta \in \bar{K}$.

Definition 9. *The singular point P is a <u>node</u> (Figure 1) if $\alpha \neq \beta$. In this case, the lines*

$$\begin{aligned} L_1:\ y - y_0 &= \alpha(x - x_0)\,, \\ L_2:\ y - y_0 &= \beta(x - x_0) \end{aligned} \tag{6.15}$$

are tangent lines at P.

The singular point P is a <u>cusp</u> (Figure 2) if $\alpha = \beta$, in which case the tangent line at P is given by

$$L : y - y_0 = \alpha(x - x_0)\,. \tag{6.16}$$

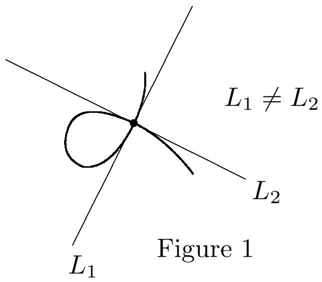


Figure 1

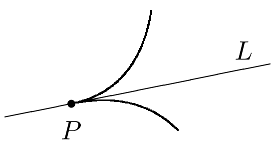


Figure 2

If $char(K) \neq 2, 3$, the substitutions

$$\begin{aligned} y' &= y + \frac{(a_1x + a_3)}{2}, \quad x' = x \quad (char\ k \neq 2)\,, \\ y'' &= y', \quad x'' = x'\frac{b_2}{12} \qquad\qquad (char\ k \neq 2,3)\,, \end{aligned} \tag{6.17}$$

give the following normal form of Weierstrass equation:

$$(y'')^2 = (x'')^3 - \frac{c_4}{48}x'' - \frac{c_6}{864}\,. \tag{6.18}$$

The reader can quickly verify the following ($char(K) \neq 2, 3$):

Proposition 2. *The elliptic curve given by Weierstrass equation can be classified in the following way*

(1) It is non–singular iff $\Delta \neq 0$.

(2) It has a node iff $\Delta = 0 \ \wedge \ c_4 \neq 0$.

(3) It has a cusp iff $\Delta = c_4 = 0$.

Consider a polynomial $f(x) = x^3 + px + q$. The discriminant $D(f)$ is by definition, the resultant $R(f, f')$, where $f'(x) = 3x^2 + p$. We compute

$$D(f) = \begin{vmatrix} q & p & 0 & 1 & 0 \\ 0 & q & p & 0 & 1 \\ p & 0 & 3 & 0 & 0 \\ 0 & p & 0 & 3 & 0 \\ 0 & 0 & p & 0 & 3 \end{vmatrix} = 27q^2 + 4p^3 \,. \tag{6.19}$$

Remark 4. *For*

$$\begin{array}{rcl} f(x) & = & a_0 + a_1 x + \cdots + a_m x^m, \\ g(x) & = & b_0 + b_1 x + \cdots + b_n x^n, \end{array} \qquad f, g \in R[x] \tag{6.20}$$

the resultant $R(f, g) \in R$ *is defined as the determinant of the following* $(n + m) \times (n + m)$ *matrix over* R*:*

$$D(f) = \left.\begin{vmatrix} a_0 & a_1 & \ldots & \ldots & \ldots & a_m & 0 & \ldots & \ldots & 0 \\ 0 & a_0 & \ldots & \ldots & \ldots & a_{m-1} & a_m & 0 & \ldots & 0 \\ \vdots & \vdots & \ldots & \ldots & \ldots & \vdots & \ldots & \ldots & \ldots & \vdots \\ 0 & 0 & \ldots & \ldots & a_0 & a_1 & \ldots & \ldots & \ldots & a_m \\ b_0 & b_1 & \ldots & b_{n-1} & b_n & 0 & \ldots & \ldots & \ldots & 0 \\ 0 & b_0 & \ldots & \ldots & b_{n-1} & b_n & \ldots & \ldots & \ldots & 0 \\ \vdots & \ldots & \ldots & \ldots & \vdots & \ldots & \ldots & \ldots & \ldots & \vdots \\ 0 & 0 & \ldots & b_0 & b_1 & \ldots & \ldots & \ldots & \ldots & b_n \end{vmatrix} \begin{array}{l} \left.\vphantom{\begin{matrix} a \\ a \\ \vdots \\ a \end{matrix}}\right\} n \\ \left.\vphantom{\begin{matrix} a \\ a \\ \vdots \\ a \end{matrix}}\right\} m \end{array}\right. \tag{6.21}$$

The polynomial $f(x) = x^3 + px + q$ has repeated root in some extension of K iff $D(f) = 0$. An explicit computation reveals that for

$$y^2 = (x - e_1)(x - e_2)(x - e_3), \quad e_1, e_2, e_3 \in \bar{K} \tag{6.22}$$

we get

$$\Delta = 16(e_1 - e_2)^2 (e_1 - e_3)^2 (e_2 - e_3)^2. \tag{6.23}$$

For the elliptic curve in normal form (6.18) we get

$$-2^4 D(f) = \frac{c_4^3 - c_6^2}{12^3} = \Delta \tag{6.24}$$

Using the Proposition 2, we have the following result.

Proposition 3. *Let char*$(K) \neq 2, 3$. *The cubic curve* $y^2 = x^3 - \frac{c_4}{48}x - \frac{c_6}{864}$ *represents a normal form of non–singular elliptic curve iff* $\Delta \neq 0$.

Theorem 7. *Let char* $(K) \neq 2, 3$.

(1) Two elliptic curves are isomorphic over $\bar{K}$ *iff they have the same* j*–invariant.*

(2) Let $j_0 \in \bar{K}$. *Then there exists an elliptic curve (defined over* $K(j_0)$*) with* j*–invariant equal to* j_0.

Proof:

(1) The implication "⇒" has been already shown. The other direction "⇐" can be proved as follows. Let E/k, E'/k be elliptic curves with the same j–invariant:

$$\begin{aligned} E : y^2 &= x^3 + Ax + B\,, \\ E' : (y')^2 &= (x')^3 + A'x' + B'\,, \end{aligned} \tag{6.25}$$

with

$$j(E) = 12^3 \frac{4A^3}{4A^3 + 27B^2} = 12^3 \frac{4A'^3}{4A'^3 + 27B'^2} = j(E')\,. \tag{6.26}$$

This yields

$$A^3 B'^2 = A'^3 B^2\,. \tag{6.27}$$

We look for an isomorphic of the form $(x, y) = (u^2 x', u^3 y')$ and consider there cases:

(A) $A = 0$ ($\Rightarrow j = 0$). Then $B \neq 0$ (since $\Delta \neq 0$), so $A' = 0$ and we obtain an isomorphism with $u = (B/B')^{1/6}$.

(B) $B = 0$ ($\Rightarrow j = 1728$). Then $A \neq 0$ (since $\Delta \neq 0$), so $B' = 0$ and we obtain an isomorphism with $u = (A/A')^{1/4}$.

(C) $AB \neq 0$ ($j \neq 0, 1728$). Then $A'B' \neq 0$, since if one of them would be zero then they both are, contradicting $\Delta' \neq 0$. Hence $u = (A/A')^{1/4} = (B/B')^{1/6}$ gives the desired isomorphism.

(2) Assume that $j_0 \neq 0$, 1728, and look at the curve

$$E : y^2 + xy = x^3 - \frac{36}{j_0 - 1728}x - \frac{1}{j_0 - 1728}\,. \tag{6.28}$$

One computes

$$\Delta = \frac{j_0^2}{(j_0 - 1728)^3}, \quad j = j_0\,. \tag{6.29}$$

Thus E gives desired elliptic curves (in any characteristic) provided $j_0 \neq 0,\, 1728$. To complete the list, here are the two curves

$$\begin{aligned} E\,:\,y^2+y=x^3, &\quad \Delta=-27, \quad j=0\,;\\ E\,:\,y^2=x^3+x, &\quad \Delta=-64, \quad j=1728\,. \end{aligned} \tag{6.30}$$

■

Definition 10. *A Weierstrass equation is in normal Legendre form iff it can be written as* $y^2 = x(x-1)(x-\lambda),\ \lambda \in K$.

Proposition 4. *Assume* $char(K) \neq 2$.

(1) Every elliptic curve E/K *is isomorphic (over* $\bar{K}$*) to an elliptic curve in Legendre form*

$$E_\lambda : y^2 = x(x-1)(x-\lambda), \quad \lambda \in \bar{K},\ \lambda \neq 0,\, 1\,. \tag{6.31}$$

(2) The j*–invariant of* E_λ *is*

$$j(E_\lambda) = 2^8 \frac{(\lambda^2-\lambda+1)^3}{\lambda^2(\lambda-1)^2}\,. \tag{6.32}$$

(3) The map

$$\begin{aligned} j : \bar{K}\backslash\{0,1\} &\longrightarrow \bar{K}\\ \lambda &\longmapsto j(E_\lambda) \end{aligned} \tag{6.33}$$

is surjective and $6:1$ *except above* $j=0$ *resp.* $j=1728$*, where it is* $2:1$ *resp.* $3:1$.

Proof:

(1) Since $char(K) \neq 2$, we know that E has a Weierstrass equation of the form

$$(y')^2 = (x')^3 + \frac{b_2}{4}(x')^2 + \frac{b_4}{2}x' + \frac{b_6}{4}\,, \tag{6.34}$$

as follows from the substitution $x' = x,\ y' = y + \frac{(a_1x+a_3)}{2}$ into normal form $y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$. This implies

$$(y')^2 = (x'-e_1)(x'-e_2)(x'-e_3), \quad e_1, e_2, e_3 \in \bar{K}\,. \tag{6.35}$$

Since $\Delta \neq 0,\ e_1 \neq e_2 \neq e_3$. The substitution

$$x' = (e_2-e_1)x'' + e_1,\ y' = (e_2-e_1)^{3/2}y'' \tag{6.36}$$

given an equation in Legendre form

$$(y'')^2 = x''(x''-1)(x''-\lambda), \quad \lambda = \frac{e_3-e_1}{e_2-e_1} \in \bar{K},\ \lambda \neq 0,\ 1\,. \tag{6.37}$$

(2) Direct calculation.

(3) Either use (2), or the following line of reasoning. The j–invariant classifies an elliptic curve up to isomorphism (⇈???). Thus suppose $j(E_{\lambda_1}) = j(E_{\lambda_2})$, then $E_{\lambda_1} \simeq E_{\lambda_2}$ and $x = u^2x' + r,\ y = u^3y'$ gives

$$\begin{aligned} u^6x'(x'-1)(x'-\mu) &= (y')^2u^6 = y^2 = x(x-1)(x-\lambda) \\ &= u^6(x' + \frac{r}{u^2})(x' + \frac{r-1}{u^6})(x' + \frac{r-\lambda}{u^2})\,. \end{aligned} \tag{6.38}$$

There are six ways of assigning the linear terms to one another:

$$\mu \in \left\{\lambda,\ \frac{1}{\lambda},\ 1-\lambda,\ \frac{1}{1-\lambda},\ \frac{\lambda}{\lambda-1},\ \frac{\lambda-1}{\lambda}\right\}\,. \tag{6.39}$$

For example, comparison

$$\begin{aligned} (x-1) &\longleftrightarrow (x + \frac{r}{u^2})\,, \\ x &\longleftrightarrow (x + \frac{r-1}{u^2})\,, \\ (x-\mu) &\longleftrightarrow (x + \frac{r-\lambda}{u^2}) \end{aligned} \tag{6.40}$$

leads to $r = -u^2,\ r = 1 \Rightarrow \mu = 1 - \mu$.

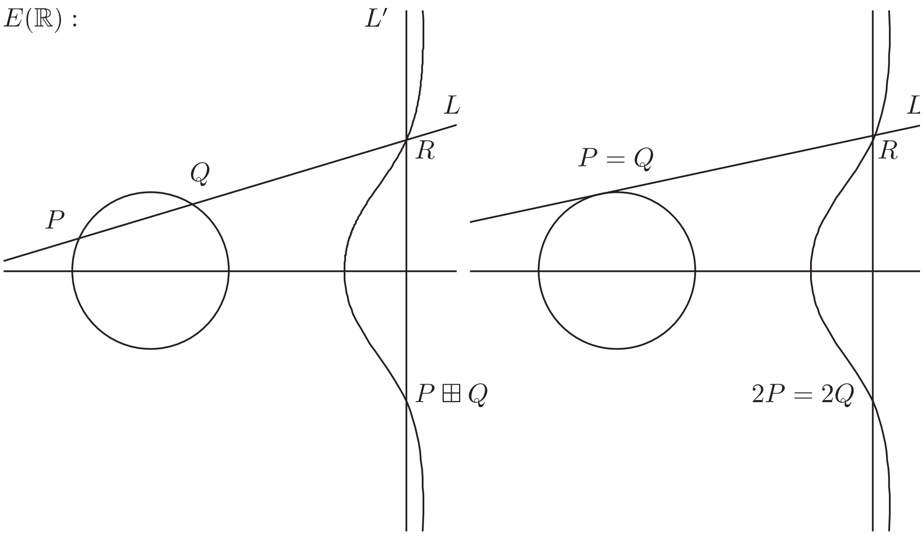
Hence $\lambda \mapsto j(E_\lambda)$ is exactly $6 : 1$ unless two or more of these values coincide. This only occurs for $\lambda = -1,\, 2,\, 1/2$ and $\lambda^2 - \lambda + 1 = 0$, for which $\#\mu_{\lambda=-1} = \#\mu_{\lambda=1/2} = \#\mu_{\lambda=2} = 3,\ \#\mu_{\lambda^2-\lambda+1=0} = 2$, and these values correspond to $j = 1728$ and $j = 0$. ■

Chapter 7

Geometry of the group law on elliptic curves

Remember that $E \subset \mathbb{P}^2$, an elliptic curve given by Weierstrass equation, consists of the points $P = (x, y)$ solving the equation, together with the point $O = P_\infty = [0, 1, 0]$. Let $L \subset \mathbb{P}^2$ be a line. Since $\deg(E) = 3$, $L \cap E$ contains three points (counted with multiplicity) as a special case of Bezout's theorem.

Definition 11. *Let $P, Q \in E$, $L \subset \mathbb{P}^2$ a line connecting P, Q (tangent line to E if $P = Q$), and R the third point of intersection of L with E. Let L' be the line connecting R and O. Then $P \boxplus Q$ is the point such that $L' \cap E = \{R, O, P \boxplus Q\}$.*



Lemma 4. *The composition law definition 11 has the following properties:*

1/ *If a line L intersects E at the (not necessarily distinct) points P, Q, R, then $(P \boxplus Q) \boxplus R = O$.*

2/ $P \boxplus O = P \quad \forall P \in E$.

3/ $P \boxplus Q = Q \boxplus P \quad \forall P, Q \in E$.

4/ *Let $P \in E$. There is a point of E, denoted $-P$, so that $P \boxplus -P = O$.*

5/ *Let $P, Q, R \in E$. Then $(P \boxplus Q) \boxplus R = P \boxplus (Q \boxplus R)$. In other words, the composition law in definition 11 makes $(E, \boxplus, O)$ an abelian group.*

6/ *Suppose $E = E/K$. Then $E(K) = \{(x, y) \in K^2 \mid E(x, y) = 0\} \cup \{0\}$ is a subgroup of E.*

Proof:

1/ Obvious from definition 11 (note that the tangent line to E at O intersects E with multiplicity 3 at O).

2/ Taking $Q = O$ in definition 11, the lines L, L' coincides. We have $L \cap E = \{P, O, R\}$, $L' \cap E = \{R, O, P \boxplus O\}$, and so $P \boxplus O = P$.

3/ Obvious since the construction in definition 11 is symmetric in P, Q.

4/ Let the line through P, O also intersects E in R. Then we get from 1/,2/, $O = (P \boxplus O) \boxplus R = P \boxplus R$. We define $-P := R$.

5/ Using the formulas for the group law, we can explicitly verify the associativity of the group law. The second possibility is to use the results of **??**.

6/ If P, Q have coordinates in K, then the line $L = \overline{PQ}$ has the coefficients in K, and if E is defined over K, then the third point of intersection has the coordinates also in K.

■

<u>**Notation**</u>. *For $m \in \mathbb{Z}$, $P \in E$, we let*

$$\begin{aligned} [m]P &= P \boxplus P \boxplus \ldots \boxplus P \, (m - \textit{terms}), m > 0 \\ [0]P &= 0, [m]P = [-m](-P), m < 0 \, (P \boxplus (-P) = 0). \end{aligned} \tag{7.1}$$

We shall derive explicit formulas for the group operation E/K:

$$E/K : \; E(x, y) = y^2 + a_1 xy + a_3 y - x^3 - a_2 x^2 - a_4 x - a_6 = 0,$$

and let $P_0 = (x_0, y_0) \in E$. To calculate $(-P_0) \in E/K$, we take the line L through P_0, O and find it the third intersection point with E/K. The line is given by $L : x - x_0 = 0$. Substitution into E/K, we see that E/K has roots y_0, y_0', where $-P = (x_0, y_0')$. Writing

$$E(x_0, y) = c(y - y_0)(y - y_0')$$

and comparison the coefficient of y^2 gives $c = 1$, and comparison of the coefficients of y gives

$$y_0' = -y_0 - a_1x_0 - a_3 \Longrightarrow -P_0 = (x_0, -y_0 - a_1x_0 - a_3).$$

Next we derive a formula for the group law. Let $P_1 = (x_1, y_1), P_2 = (x_2, y_2)$ be points of E/K. If $x_1 = x_2, y_1 + y_2 + a_1x_2 + a_3 = 0$, then from the above formula $P_1 \boxplus P_2 = O$.
The line L through P_1 and P_2 (tangent line to E if $P_1 = P_2$) has an equation $L : y = \lambda x + v$. Substituting into the equation for E, we see that $E(x, \lambda x + v)$ has roots x_1, x_2, x_3, where $P_3 = (x_3, y_3)$ is the third point of intersection, $P_3 \in L \cap E$. From lemma 4, $P_1 \boxplus P_2 \boxplus P_3 = O$, while

$$E(x, \lambda x + v) = c'(x - x_1)(x - x_2)(x - x_3)$$

and equating the coefficients of x^3, x^2 yields

$$c' = -1, x_1 + x_2 + x_3 = \lambda^2 + a_1\lambda - a_2.$$

This gives the formula for x_3 and substituting back into L gives $y_3 = \lambda x_3 + v$. Finally, to find $P_1 \boxplus P_2 = -P_3$, we apply **??**. We summarize this development in the following.

Theorem 8 (Group law algorithm). *Let E/K be an elliptic curve given by a Weierstrass equation*

$$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6,\ a_i \in K \text{ for } i = 1, \ldots, 6.$$

1/ Let $P_0 \equiv (x_0, y_0) \in E$. Then

$$-P_0 = (x_0, -y_0 - a_1x_0 - a_3).$$

Now let

$$P_1 \boxplus P_2 = P_3, \quad P_i = (x_i, y_i) \in E.$$

2/ If $x_1 = x_2$, $y_1 + y_2 + a_1x_2 + a_3 = 0$, then $P_1 \boxplus P_2 = O$.
Otherwise, let

$$\begin{aligned} \lambda &= \frac{y_2 - y_1}{x_2 - x_1}, \quad v = \frac{y_1x_2 - y_2x_1}{x_2 - x_1} \text{ if } x_1 \neq x_2, \\ \lambda &= \frac{3x_1^2 + 2a_2x_1 + a_4 - a_1y_1}{2y_1 + a_1x_1 + a_3}, \ v = \frac{-x_1^3 + a_4x_1 + 2a_6 - a_3y_1}{2y_1 + a_1x_1 + a_3} \text{ if } x_1 = x_2. \end{aligned} \tag{7.2}$$

Then $y = \lambda x + v$ is the line $\overline{P_1P_2}$, or the tangent to E if $P_1 = P_2$.

3/ $P_3 = P_1 \boxplus P_2$ *is given by*

$$\begin{aligned} x_3 &= \lambda^2 + a_1\lambda - a_2 - x_1 - x_2, \\ y_3 &= -(\lambda + a_1)x_3 - v - a_3. \end{aligned} \tag{7.3}$$

4/ As a special case of 3/, where for $P_1 \neq \pm P_2$,

$$x(P_1 \boxplus P_2) = \left(\frac{y_2 - y_1}{x_2 - x_1}\right)^2 + a_1\left(\frac{y_2 - y_1}{x_2 - x_1}\right) - a_2 - x_1 - x_2,$$

and for $P = (x, y) \in E$,

$$x([2]P) = x(P \boxplus P) = \frac{x^4 - b_4x^2 - 2b_6x - b_8}{4x^3 + b_2x^2 + 2b_4x + b_6},$$

where b_2, b_4, b_6, b_8 *are the polynomials in the* a_i*'s given in* **??**.

The final achievement of this section is the comparison between geometric group law and the group law coming from the transport of canonical group structure from C_F^0.

Theorem 9. *If* E *is given by Weierstrass equation, then the geometric group law given by definition 11 and the group law induced from* C_F^0 *are the same (coincide).*

Proof:

Let $f(X, Y, Z) = \alpha X + \beta Y + \gamma Z = 0$ be a line L in $\mathbb{P}^2 = [X, Y, Z]$, going through P and Q, $P, Q \in E$ and let R be the third point of intersection of $L \cap E$. Let $f'(X, Y, Z) = \alpha' X + \beta' Y + \gamma' Z = 0$ be the line L' going through R, O. Let us consider two functions on E:

$$\frac{f}{Z} : \mathbb{P}^2/K \to K,\ \frac{f'}{Z} : \mathbb{P}^2/K \to K \Longrightarrow \left.\frac{f}{Z}\right|_E : E/K \to K,\ \left.\frac{f'}{Z}\right|_E : E/K \to K.$$

It follows from $\deg\operatorname{div}\left(\left.\frac{f}{Z}\right|_E\right) = \deg\operatorname{div}\left(\left.\frac{f'}{Z}\right|_E\right) = 0$ that

$$\begin{aligned} \operatorname{div}\left(\left.\frac{f}{Z}\right|_E\right) &= (P) + (Q) + (R) - 3(O), \\ \operatorname{div}\left(\left.\frac{f'}{Z}\right|_E\right) &= (R) + (P \boxplus Q) - 2(O). \end{aligned} \tag{7.4}$$

The multiplicity if the divisor (O) can be directly checked from the fact that the line $Z = 0$ intersects E at O with multiplicity 3. Hence

$$(P \boxplus Q) - (P) - (Q) + (O) = \operatorname{div}\left(\left.\frac{f'}{f}\right|_E\right) = 0.$$

This means that due to $i : E \to C_F^0$, $P \to [(P) - (0)]$, definition 11 is equivalent to $i\{P \boxplus Q\} = i\{P\} + i\{Q\}$, which is the definition of the group law via lemma 3.

■

Chapter 8

Isogenies

Let $(E_1, 0),\ (E_2, 0)$ be elliptic curves with a distinguished point (denoted by the same letter 0 for both E_1, E_2).

Definition 12. *Let $(E_1, 0),\ (E_2, 0)$ be elliptic curves. An isogeny between E_1, E_2 is a morphism $\varphi : E_1 \to E_2$ satisfying $\varphi(0) = 0$. If there is an isogeny $\varphi : E_1 \to E_2,\ \varphi(E_1) \neq \{0\}$, we say that E_1, E_2 are isogenous.*

Note that because $\varphi(E_1) \neq \{0\}$, the map φ is surjective. Thus except for the trivial isogeny defined by $[0](P) = 0\ \forall P \in E_1$, every non–trivial isogeny is a finite map of curves. Hence we obtain usual injection of function fields

$$\varphi^* :\ \bar{K}(E_2) \longrightarrow \bar{K}(E_1)\,. \tag{8.1}$$

All properties of φ, i.e. $deg(\varphi)$, its separability and/or inseparability, are determined by the finite extension $\bar{K}(E_1)/\varphi^*\bar{K}(E_2)$. By convention, we set $deg[0] = 0$.

The maps between elliptic curves form an abelian group – if we define

$$Hom(E_1, E_2) := \{\text{isogenies } \varphi :\ E_1 \longrightarrow E_2\}\,, \tag{8.2}$$

then $Hom(E_1, E_2)$ is a group under the addition law

$$(\varphi_1 + \varphi_2)\,(P) = \varphi_1(P) \boxplus \varphi_2(P), \quad \varphi_1, \varphi_2 \in Hom(E_1, E_2)\,. \tag{8.3}$$

If $E_1 = E_2$, then $End(E_1) = Hom(E_1, E_1)$ form a ring with addition as above and multiplicative structure given by composition of isogenies:

$$(\varphi_1 \circ \varphi_2)\,(P) = \varphi_1\left(\varphi_2(P)\right)\,. \tag{8.4}$$

The distributive properties will be proved later. $End(E)$ is called the endomorphism ring of E, and the subset of invertible elements of $End(E)$ forms a subgroup $Aut(E)$ of $End(E)$ called automorphism group of E. If E_1/K, $E_2/K,\ E/K$, then all objects $Hom_K(E_1, E_2),\ End_K(E),\ Aut_K(E)$ are defined over K.

Ex. 8. *For each $m \in \mathbb{Z}$, define the isogeny "multiplication by m" as*

$$\begin{array}{lll} m > 0 : & [m] : & E \longrightarrow E\,, \\ & & P \longmapsto \underbrace{P \boxplus \ldots \boxplus P}_{m}\,. \\ m < 0 : & & P \longmapsto [m](P) = [-m](-P)\,, \\ m = 0 & & P \longmapsto 0\,. \end{array} \tag{8.5}$$

It follows from the formulae for the group law that this map is an isogeny, and it is defined over K.

Proposition 5. *(1) Let E/K be an elliptic curve and let $m \in \mathbb{Z}$, $m \neq 0$. Then the "multiplication by m" map $[m] : E \to E$ is non–constant.*

(2) Let E_1, E_2 be elliptic curves. Then the group of isogenies $Hom(E_1, E_2)$ is a torsion free $\mathbb{Z}$–module.

(3) Let E be an elliptic curve. Then $End(E)$ is not necessarily commutative ring of characteristic 0 with no zero divisors.

Proof:

(1) We first show $[2] \neq [0]$. From the duplication formula Eq(⇈???), if a point $P = (x, y) \in E$ has order 2, $[2](P) = 0$, then it must satisfy

$$4x^3 + b_2x^2 + 2b_4x + b_6 = 0\,. \tag{8.6}$$

If $char(K) \neq 2$, this shows that there are only finitely many such points. If $char(K) = 2$, the only way to have $[2] = [0]$ is for this polynomial to be identically 0, which means $b_2 = b_6 = 0$, and so $\Delta = -8b_4^3 = 0 \; mod \; 2$. Hence in all cases $[2] \neq [0]$. It follows from $[mn] = [m] \circ [n]$ that we are reduced to the case of odd m. Assume $char(K) \neq 2$. Then $4x^3 + b_2x^2 + 2b_4x + b_6 \nmid x^4 - b_4x^2 - 2b_6x - b_8$. I.e. if it does, then $\Delta = 0$. Hence we can find an $x_0 \in \bar{K}$ so that the former polynomial, $4x^3 - b_4x^2 - 2b_6x - b_8$ vanishes to a higher order at $x = x_0$ than the polynomial $x^4 - b_4x^2 - 2b_6x - b_8$. Choosing $y_0 \in \bar{K}$ so that $P_0 = (x_0, y_0) \in E$, the formula Eq(↑???) implies $[2]P_0 = 0$. In other words, we have shown that E has a non–trivial point of order 2. But then for m odd, $[m]P_0 = P_0 \neq 0$, so $[m] \neq [0]$. If $char(K) = 2$, we can construct a point of order 3 and the same line.

(2) This follows from (1). Suppose $\varphi \in Hom(E_1, E_2)$ and $m \in \mathbb{Z}$ satisfying $[m] \circ \varphi = [0]$. Taking degrees of maps, $deg([m])deg(\varphi) = deg[0] = 0$, so either $m = 0$, or (1) implies that $deg[m] \geq 1$, hence $\varphi = [0]$.

(3) It follows from (2) that $char(End(E)) = 0$. Moreover, if $\varphi_1, \varphi_2 \in End(E)$ satisfy $\varphi_1 \circ \varphi_2 = [0]$, then

$$(deg\ \varphi_1)\,(deg\ \varphi_2) = deg\,(\varphi_1 \circ \varphi_2) = 0\,. \tag{8.7}$$

It follows that either $\varphi_1 = [0]$ $\varphi_2 = [0]$ and therefore $End(E)$ is an integral domain. ■

Definition 13. *Let E/K be an elliptic curve, $m \in \mathbb{Z}$, $m \neq 0$. The m–torsion subgroup of E, denoted $E[m]$, is the set of points of order m in E,*

$$E[m] := \{P \in E \,|\, [m]P = 0\} . \tag{8.8}$$

The torsion subgroup of E, denoted E_{tors}, is the set of points of finite order, $E_{tors} = \bigcup_{m=1}^{\infty} E[m]$. Note that $E_{tors}(K)$ defines the set of torsion points defined over K.

Later on we shall prove that $deg[m] = m^2$, from which the structure of $E[m]$ can be deduced. For $char(K) = 0$, the map $[\ ] : \mathbb{Z} \to End(E)$ is usually onto, i.e. $End(E) \simeq \mathbb{Z}$. If $End(E)$ is strictly larger then $\mathbb{Z}$, we say that E has complex multiplication. If K is a finite field, then $End(E)$ is always larger than $\mathbb{Z}$.

Ex. 9. *Assume $char(K) \neq 2$, $E/K : y^2 = x^3 - x$. Then, in addition to $\mathbb{Z}$, $End(E)$ contains an element $[i] : (x, y) \to (-x, iy)$ (here $i \in \bar{K}$ is a primitive fourth root of unity). Note $[i]$ is defined over K iff $i \in K$. Hence even if E is defined over K, $End_K(E)$ may be strictly smaller then $End(E)$. Because $[i] \circ [i] = [-1]$, we have a ring homomorphism*

$$\begin{aligned} \mathbb{Z}[i] &\longrightarrow End(E) , \\ m + ni &\longmapsto [m] + [n] \circ [i] . \end{aligned} \tag{8.9}$$

Ex. 10. *Suppose $char(K) = p > 0$, and let $q = p^r$. Recall the Frobenious morphism*

$$\begin{aligned} Fr :\ E &\longrightarrow E^{(q)}, , \\ (x, y) &\longmapsto (x^q, y^q) . \end{aligned} \tag{8.10}$$

Using the fact that q–th power map is an isomorphism, one sees

$$\Delta(E^{(q)}) = \Delta(E)^{(q)}, \quad j(E^{(q)}) = j(E)^{(q)} . \tag{8.11}$$

Theorem 10. *Every isogeny is a group homomorphism, i.e. for an isogeny $\varphi : E_1 \to E_2$ holds*

$$\varphi\left(P \boxplus_{E_1} Q\right) = \varphi(P) \boxplus_{E_2} \varphi(Q) \quad \forall P, Q \in E_1 . \tag{8.12}$$

Proof: If $\varphi(P) = 0$ for all $P \in E_1$, we are done. Otherwise, φ is a finite map, so it induces a homomorphism

$$\varphi_* :\ Cl^0(E_1) \longrightarrow Cl^0(E_2) \tag{8.13}$$

defined by

$$\varphi_*\left(\left[\sum_i n_i(P_i)\right]\right) = \left[\sum_i n_i\left(\varphi(P_i)\right)\right] . \tag{8.14}$$

It follows from the group isomorphisms $E_i \xrightarrow{\sim} Cl^0(E_i),\ i = 1, 2$ and the property $\varphi(0) = 0$ that the diagram

$$\begin{array}{ccc} E_1 & \xrightarrow{\sim} & Cl^0(E_1) \\ \downarrow \varphi & & \downarrow \varphi_* \\ E_2 & \xrightarrow{\sim} & Cl^0(E_2) \end{array} \tag{8.15}$$

is commutative. Because the map φ_* is a homomorphism φ is also a homomorphism. ■

Corollary 2. *Let $\varphi : E_1 \to E_2$ be a nonzero isogeny. Then $Ker(\varphi) = \varphi^{-1}(0)$ is a finite subgroup of E_1.*

8.1 The invariant differential

Recall that the differential $\omega = \frac{dx}{2y+a_1+a_3} \in \Omega(E)$ on an elliptic curve E/K has neither zeros nor poles. We now justify its name invariant differential. For $Q \in E$, we define a translation map by Q:

$$\begin{aligned} T_Q :\ E &\longrightarrow E \\ P &\longmapsto P \boxplus Q\,. \end{aligned} \tag{8.16}$$

Lemma 5. *Let T_Q be as above. Then*

$$T_Q^* \omega = \omega \quad \forall Q \in E\,. \tag{8.17}$$

Proof: There is, of course, brutal force proof based on addition formulas for $x(P \boxplus Q),\ y(P \boxplus Q)$ in terms of $x(P),\ y(P),\ x(Q),\ y(Q)$ and direct comparison yields

$$\frac{dx(P \boxplus Q)}{2y(P \boxplus Q) + a_1 x(P \boxplus Q) + a_3} = \frac{dx(P)}{2y(P) + a_1 x(P) + a_3} \quad \forall Q \in E\,. \tag{8.18}$$

More illuminating proof goes as follows. Since $\Omega(E)$ is a 1–dimensional $\bar{K}(E)$–module, there is a function $f_Q \in \bar{K}(E)$ such that

$$T_Q^* \omega = f_Q \omega \quad (T_Q^* \text{ is an isomorphism} \Longrightarrow f_Q \neq 0)\,. \tag{8.19}$$

By definition

$$div(f_Q) = div(T_Q^* \omega) - div(\omega) = T_Q^* div(\omega) - div(\omega) = 0 \tag{8.20}$$

since $div(\omega) = 0$ (see Eq(⇈???)), hence $f_Q \in \bar{K}^*$. Recall that for $\varphi :\ C_1 \to C_2$ a nonconstant map of (smooth) curves, the ramification index of φ at $P \in C_1$, denoted by $e_\varphi(P)$ is given by

$$e_\varphi(P) = ord_P \left(\varphi^* t_{\varphi(P)}\right)\,, \tag{8.21}$$

where $t_{\varphi(P)} \in \bar{K}(C_2)$ ($\varphi^* t_{\varphi(P)} \in \bar{K}(C_1)$) is uniformizer at $\varphi(P)$. Note that $e_\varphi(P) \geq 1$. The map φ is unramified at P if $e_\varphi(P) = 1$. It is easy to prove that

$$\sum_{P \in \varphi^{-1}(Q)} e_\varphi(P) = deg\ \varphi, \quad \forall Q \in C_2\,. \tag{8.22}$$

We define the map φ^* on the divisor groups as

$$\begin{aligned} \varphi^* :\ Div(C_2) &\longrightarrow Div(C_1)\,, \\ (Q) &\longmapsto \sum_{P \in \varphi^{-1}(Q)} e_\varphi(P)(P)\,. \end{aligned} \tag{8.23}$$

This map fulfills

$$\varphi^*(div\ f) = div(\varphi^* f), \quad \forall f \in \bar{K}(C_2)\,. \tag{8.24}$$

In particular, $T_Q^* div(\omega) = div(T_Q^* \omega)$.

Consider the map

$$\begin{aligned} g :\ E/K &\longrightarrow \mathbb{P}^1 \\ Q &\longmapsto [f_Q, 1]\ . \end{aligned} \tag{8.25}$$

Because f_Q is a rational function of $x(Q), y(Q)$ g is a rational map which is not surjective (i.e. the image Im(g) does not contain the points $[0,1]$ and $[1,0]$). Then Eq(⇈???) implies that g is constant,

$$f_Q = f_0 = 1 \quad \forall Q \in E\,. \tag{8.26}$$

This concludes the proof. ■

Theorem 11. *Let E, E' be two elliptic curves, let ω be an invariant differential on E, $\varphi_1, \varphi_2 : E' \to E$ two isogenies. Then*

$$(\varphi_1 + \varphi_2)^* \omega = \varphi_1^* \omega + \varphi_2^* \omega\,. \tag{8.27}$$

Note that the "+" on the LHS is the addive structure on $Hom(E', E)$, while the "+" on the RHS is the additive structure on $\Omega(E')$.

Proof: If $\varphi_1 = [0]$ or $\varphi_2 = [0]$, the result is trivial. If $\varphi_1 + \varphi_2 = [0]$, then using the fact that

$$\varphi_2^* = (-\varphi_1)^* = \varphi_1^* \circ [-1]^*\,, \tag{8.28}$$

it is sufficient to check

$$[-1]^* \omega = -\omega\,. \tag{8.29}$$

Since

$$[-1](x, y) = (x, -y - a_1 x - a_3)\,, \tag{8.30}$$

we obtain

$$[-1]^*\left(\frac{dx}{2y+a_1x+a_3}\right) = \frac{dx}{2(-y-a_1x-a_3)+a_1x+a_3}$$
$$= -\frac{dx}{2y+a_1x+a_3}\,. \tag{8.31}$$

The proof of the general case will be omitted – it just relies on realization of E in $\mathbb{P}^2\times\mathbb{P}^2$ via

$$\begin{aligned} i_1:\ E &\hookrightarrow E\times E\hookrightarrow \mathbb{P}^2\times\mathbb{P}^2\,,\\ x &\mapsto (x,0)\,,\\ i_2:\ E &\hookrightarrow E\times E\hookrightarrow \mathbb{P}^2\times\mathbb{P}^2\,,\\ x &\mapsto (0,x)\,. \end{aligned} \tag{8.32}$$

■

Corollary 3. *Let $\omega\in\Omega(E)$ be an invariant differential on an elliptic curve E. Let $m\in\mathbb{Z}$. Then*

$$[m]^*\omega = m\omega\,. \tag{8.33}$$

Proof: The assertion is true for $m=0$ (by definition) and $m=1$ (this is also clear, because $[1]=\mathrm{Id}$). From the previous Th(↑) we conclude, for $\varphi_1=[m],\ \varphi_2=[1]$:

$$[m+1]^*\omega = [m]^*\omega+\omega\,, \tag{8.34}$$

and the result follows by induction. ■

Corollary 4. *Let $\omega\in\Omega(E)$ be an invariant on an differential elliptic curve, and let $m\in\mathbb{Z},\ m\neq 0$. Assume either that $char(K)=0$ or that $gcd(m, char(K))=1$. Then the map $[m]:E\to E$ is a finite, separable endomorphism.*

Proof: Let ω be an invariant differential on E. The from Cor(↑???),

$$[m]^*\omega = m\omega\neq 0\,, \tag{8.35}$$

so $[m]\neq[0]$ and the map $[m]^*$ is surjective. The condition in Th(↑↑???) implies that $[m]$ is separable. ■

Corollary 5. *Let $char(K)=p>0$ ($K=\mathbb{F}_q,\ q=p^r$ for some r), E/K an elliptic curve, $\varphi:E\to E$ be the q–th power Frobenius endomorphism (see Chapter 5), and let $m,n\in\mathbb{Z}$. Then the map*

$$[m]+[n]\varphi:\ E\to E \tag{8.36}$$

is separable iff $p\nmid m$. In particular, the map $1-\varphi$ is separable.

Proof: Let ω be an invariant differential on E. From Th(⇈???) a map $\tilde{\varphi} : E \to E$ is inseparable iff $\tilde{\varphi}\omega = 0$. Using theorem 11 and corollary 3, we conclude for $\tilde{\varphi} = m + n\varphi$,

$$(m + n\varphi)^* \, \omega = m\omega + n\varphi^*\omega \,. \tag{8.37}$$

But $\varphi^*\omega = 0$ because φ is inseparable – or directly, because $\varphi^*(dx) = d\,(\varphi(x)) = d(x^q) = qx^{q-1}dx = 0$ for $char(K) = p$. We have

$$(m + n\varphi)^* \, \omega = m\omega \,, \tag{8.38}$$

and so $(m + n\varphi)^* \, \omega = 0$ iff $p|m$, which is the desired result. ■

8.2 The dual isogeny

Let $\varphi : E_1 \to E_2$ be a non–constant isogeny, inducing a map (see proof of lemma 5)

$$\varphi^* : \; Cl^0(E_2) \longrightarrow Cl^0(E_1) \,. \tag{8.39}$$

On the other hand, we have a group isomorphisms

$$\begin{aligned} i_j : \; E_j &\xrightarrow{\sim} Cl^0(E_j), \quad j = 1, 2 \,, \\ P &\longmapsto [(P) - (O)] \,. \end{aligned} \tag{8.40}$$

Hence we obtain a homomorphism going in the opposite direction (to Eq(↑???)):

$$i_1^{-1} \circ \varphi^* \circ i_2 : \; E_2 \xrightarrow{\sim} Cl^0(E_2) \xrightarrow{\varphi^*} Cl^0(E_1) \xrightarrow{\sim} E_1 \,. \tag{8.41}$$

It is by no means clear that the homomorphism $i_1^{-1} \circ \varphi^* \circ i_2$ is an isogeny, i.e. given by a rational map. The process of finding a point P, such that $\varphi(P) = Q$ for a given $Q \in E_2$, will involve the quest for roots of various polynomial equations.

Theorem 12. *Let $\varphi : E_1 \to E_2$ be an isogeny (non–constant) of degree m.*

(1) There exists a unique isogeny $\hat{\varphi} : E_2 \to E_1$ satisfying $\hat{\varphi} \circ \varphi = [m]$.

(2) $\hat{\varphi}$ is a group homomorphism given by

$$\begin{aligned} E_2 &\longrightarrow Div^0(E_2) \xrightarrow{\varphi^*} Div^0(E_1) \xrightarrow{\sum} E_1 \,, \\ P &\longmapsto (P) - (0) \quad \sum_P n_P(P) \longmapsto \sum [n_p] P \,. \end{aligned} \tag{8.42}$$

Proof:
Uniqueness. Suppose $\hat{\varphi}, \hat{\varphi}'$ are two such isogenies. Then

$$(\hat{\varphi} - \hat{\varphi}') \circ \varphi = [m] - [m] = [0] \,. \tag{8.43}$$

Since φ is non–constant map (i.e. surjective), it follows from Th(↑???) that $\hat{\varphi} - \hat{\varphi}'$ must be constant, i.e. $\hat{\varphi} = \hat{\varphi}'$.

Composition. Suppose $\psi : E_2 \to E_3$ is a non–constant isogeny, $deg\psi = n$, and let us suppose that $\hat{\varphi}, \hat{\psi}$ exist. Then

$$\left(\hat{\varphi} \circ \hat{\psi}\right) \circ (\psi \circ \varphi) = \hat{\varphi} \circ [n] \circ \varphi = \hat{\varphi} \circ \varphi \circ [n] = [nm]\,, \tag{8.44}$$

where the last but one equality follows from the property of φ of being goup homomorphism. Then $\widehat{\psi \circ \varphi} = \hat{\varphi} \circ \hat{\psi}$.

To prove the existence, it is necessary to distinguish the cases of separable and nonseparable isogenies. Both cases are threated, for example, in [5]. ■

Definition 14. *Let $\varphi : E_1 \to E_2$ be an isogeny. The dual isogeny to φ is the isogeny $\hat{\varphi} : E_2 \to E_1$ given in theorem 12. If $\varphi = [0]$, we set $\hat{\varphi} = [0]$.*

Theorem 13. *Let $\varphi : E_1 \to E_2$ be an isogeny.*

(1) Let $deg\,\varphi = m$. Then

$$\begin{aligned} \hat{\varphi} \circ \varphi &= [m] \;\; on\ E_1\,, \\ \varphi \circ \hat{\varphi} &= [m] \;\; on\ E_2\,. \end{aligned} \tag{8.45}$$

(2) Let $\tilde{\varphi} : E_2 \to E_3$ be another isogeny. Then

$$\widehat{\tilde{\varphi} \circ \varphi} = \hat{\varphi} \circ \hat{\tilde{\varphi}} : \; E_3 \longrightarrow E_1\,. \tag{8.46}$$

(3) Let $\psi : E_1 \to E_2$ be another isogeny. Then

$$\widehat{\varphi + \psi} = \hat{\varphi} + \hat{\psi}\,. \tag{8.47}$$

(4) For all $m \in \mathbb{Z}$,

$$\widehat{[m]} = [m], \quad deg\,[m] = m^2\,. \tag{8.48}$$

(5) $deg\,\hat{\varphi} = deg\,\varphi$.

(6) $\hat{\hat{\varphi}} = \varphi$.

Proof: If φ is constant, then the entire theorem is trivial (similarly for (2), (3) if $\tilde{\varphi}$ or ψ is constant). We stall assume from now on that all isogenies are non–constant.

(1) The first statement is the defining property of $\hat{\varphi}$. For the second, we have

$$(\varphi \circ \hat{\varphi}) \circ \varphi = \varphi \circ (\hat{\varphi} \circ \varphi) = \varphi \circ [m] = [m] \circ \varphi\,, \tag{8.49}$$

where the last equality comes from the homomorphism property of φ. Since φ is non–constant, $\varphi \circ \hat{\varphi} = [m]$.

(2) Let $deg\,\tilde{\varphi} = n$. Then we have

$$\left(\hat{\varphi} \circ \hat{\tilde{\varphi}}\right) \circ (\tilde{\varphi} \circ \varphi) = \hat{\varphi} \circ [n] \circ \varphi = [n] \circ \hat{\varphi} \circ \varphi = [n] \circ [m] = [nm]\,. \quad (8.50)$$

Hence from the uniqueness statement in Th(↑???),

$$\hat{\varphi} \circ \hat{\tilde{\varphi}} = \widehat{\tilde{\varphi} \circ \varphi}\,. \quad (8.51)$$

(3) We shall not proved it. For the proof, see for example [5].

(4) This is true, by definition, for $m = 0$, and it is trivial statement for $m = 1$. It follows form (3) for $\varphi = [m],\ \psi = [1]$ that

$$\widehat{[m+1]} = \widehat{[m]} + \widehat{[1]} = \widehat{[m]} + [1]\,, \quad (8.52)$$

and the result follows for all m by ascending and descending induction. Let $deg\,[m] = d$ and let us study he multiplication by d map. Then

$$[d] = \widehat{[m]} \circ [m] = [m] \circ [m] = [m^2]\,. \quad (8.53)$$

Since the endomorphism ring of an elliptic curve is a torsion–free $\mathbb{Z}$–module (see Th(↑???)), it follows $d = m^2$.

(5) Let $deg\,(\varphi) = m$. Then using (1), (4),

$$m^2 = deg\,[m] = deg\,(\varphi \circ \hat{\varphi}) = (deg\,\varphi)\,(deg\,\hat{\varphi}) = m\ deg\,\hat{\varphi}\,, \quad (8.54)$$

i.e. $deg\,\hat{\varphi} = m$.

(6) Let $deg\,(\varphi) = m$. Then using (1), (2), (4),

$$\hat{\varphi} \circ \varphi = [m] = \widehat{[m]} = \widehat{\hat{\varphi} \circ \varphi} = \hat{\varphi} \circ \hat{\hat{\varphi}}\,, \quad (8.55)$$

$\varphi = \hat{\hat{\varphi}}$ because $\hat{\varphi}$ is a non–constant isogeny. ■.

Definition 15. *Let A be an abelian group. A function*

$$d:\ A \longrightarrow \mathbb{R} \quad (8.56)$$

is a quadratic form provided

(1) $d(\alpha) = d(-\alpha) \quad \forall \alpha \in A$.

(2) The map

$$\begin{aligned} A \times A &\longrightarrow \mathbb{R} \\ (\alpha, \beta) &\longmapsto d(\alpha+\beta) - d(\alpha) - d(\beta) \end{aligned} \quad (8.57)$$

is bilinear.

A quadratic form d is positive definite if

(3) $d(\alpha) \geq 0 \quad \forall \alpha \in A$, *and*

(4) *if* $d(\alpha) = 0 \Rightarrow \alpha = 0$.

Corollary 6. *Let E_1, E_2 be elliptic curves. The degree map*

$$deg: \; Hom(E_1, E_2) \longrightarrow \mathbb{Z} \tag{8.58}$$

is a positive definite quadratic form.

Proof:

(1) For $\varphi \in Hom(E_1, E_2)$, $-\varphi \in Hom(E_1, E_2)$ corresponds to $[-1] \circ \varphi$ and so $deg([-1] \circ \varphi) = deg\,[-1]\; deg\,\varphi = deg\,\varphi$.

(3), (4) are clear.

(2) Let $\varphi, \psi \in Hom(E_1, E_2)$. We would like to prove that

$$\varphi, \psi \longmapsto \langle \varphi, \psi \rangle = deg(\varphi + \psi) - deg\,\varphi - deg\,\psi \tag{8.59}$$

is a bilinear form. Using the injection $[\;] : \mathbb{Z} \to End(E_1)$, we have

$$\begin{aligned} [\langle \varphi, \psi \rangle] &= [deg(\varphi + \psi)] - [deg\,\varphi] - [deg\,\psi] \\ &= \widehat{(\varphi + \psi)} \circ (\varphi + \psi) - \hat{\varphi} \circ \varphi - \hat{\psi} \circ \psi \\ &= \hat{\varphi} \circ \psi + \hat{\psi} \circ \varphi, \end{aligned} \tag{8.60}$$

where we used Th(↑??), (3) in the last equality. Using once again Th(↑??), (3), we get

$$\begin{aligned} [\langle \varphi_1 + \varphi_2, \psi \rangle] &= \widehat{\varphi_1 + \varphi_2} \circ \psi + \hat{\psi} \circ (\varphi_1 + \varphi_2) \\ &= (\hat{\varphi}_1 + \hat{\varphi}_2) \circ \psi + \hat{\psi} \circ (\varphi_1 + \varphi_2) \\ &= \Big(\hat{\varphi}_1 \circ \psi + \hat{\psi} \circ \varphi_1 \Big) + \Big(\hat{\varphi}_2 \circ \psi + \hat{\psi} \circ \varphi_2 \Big) \\ &= [\langle \varphi_1, \psi \rangle] + [\langle \varphi_2, \psi \rangle]\;, \end{aligned} \tag{8.61}$$

and similarly for the linearity in the second component. This completes the proof. ■

Corollary 7. *Let E be an elliptic curve and $m \in \mathbb{Z}$, $m \neq 0$.*

(1) If $char(K) = 0$ or if $gcd\,(m, char(K)) = 1$, then

$$E[m] \simeq (\mathbb{Z}/m\mathbb{Z}) \times (\mathbb{Z}/m\mathbb{Z})\;. \tag{8.62}$$

(2) If $char(K) = p > 0$, then

$$\begin{array}{lll} either & E[p^e] \simeq \{0\} & \forall e \in \mathbb{N}_+\,, \\ or & E[p^e] \simeq \mathbb{Z}/p^e\mathbb{Z} & \forall e \in \mathbb{N}_+\,. \end{array} \tag{8.63}$$

8.3 The Tate module

Let E/K be an elliptic curve and $m \geq 2$ integer. If $char(K) = p > 0$, then let m be such that $gcd(char(K), m) = 1$. Because $E[m] \simeq (\mathbb{Z}/m\mathbb{Z}) \times (\mathbb{Z}/m\mathbb{Z})$. Let $g \in Gal(\bar{K}/K)$. Then there is a (continuous) representation of $Gal(\bar{K}/K)$ on $E[m]$, given by

$$\begin{aligned} Gal(\bar{K}/K) &\longrightarrow Aut\,(E[m]) \simeq Aut\,(\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}) \\ g &\longmapsto (P \longrightarrow P^g)\,, \quad GL\,(2, \mathbb{Z}/m\mathbb{Z})\,. \end{aligned} \tag{8.64}$$

since if $[m]P = 0$, then $[m]\,(P^g) = ([m]P)^q = 0^g = 0$ (note that 0 is defined over K, i.e. $0^g = 0\ \forall g \in Gal\left(\bar{K}/K\right)$). Here $P \in E/K$ is defined over finite field extension $\tilde{K}$ of K, $\left[\tilde{K} : K\right] < \infty$, and $P \to P^g$ is the action of $g \in Gal\left(\tilde{K}/K\right) = Aut_K\left(\tilde{K}\right)$.

It is more suitable to work with invertible linear maps with the coefficients in the ring of characteristic zero instead of finite characteristic.

Definition 16. *Let E/K be an elliptic curve, $l \in \mathbb{Z}$ a prime. The l–adic Tate module of E is the group*

$$T_l(E) = \lim_{\leftarrow n} E[l^n]\,, \tag{8.65}$$

the inverse limit of the ordered system of abelian groups $\{E[l^n]\}_n$ w.r. to the natural maps

$$E\left[l^{n+1}\right] \xrightarrow{[l]} E\left[l^n\right]\,. \tag{8.66}$$

Since each $E[l^n]$ is a $\mathbb{Z}/l^n\mathbb{Z}$–module, we see that the Tate module has a natural structure as a $\mathbb{Z}e$–module. The multiplication -by- l maps are surjective and so the inverse limit topology on $T_l(E)$ is equivalent to the l–adic topology coming from a $\mathbb{Z}e$–module structure. These is a natural inclusion $\mathbb{Z}e \subset \mathbb{Q}e$ in the quotient field of $\mathbb{Z}e$, and

$$char(Qe) = 0\,. \tag{8.67}$$

As a $\mathbb{Z}e$–module, the Tate module has the following structure:

- $T_l(E) \simeq \mathbb{Z}e \times \mathbb{Z}e, \quad l \neq char(K)$,
- $T_p(E) \simeq \{0\}$ or $\mathbb{Z}_p, \quad p = char(K) > 0$.

As we have shown, the action of $Gal(\bar{K}/K)$ on each $E[l^n]$ commutes with the multiplication -by- l maps used to form $\lim_{\leftarrow n} E[l^n]$, so $Gal(\bar{K}/K)$ acts also on $T_l(E)$. Because the action is continuous on each $E[l^n]$, the resulting action on $T_l(E)$ is also continuous.

Definition 17. *The l–adic representation ρ_l of $Gal(\bar{K}/K)$ on E is the map*

$$\rho:\ Gal(\bar{K}/K) \longrightarrow Aunt(T_l(E)) \simeq GL(2, \mathbb{Z}e) \subset GL(2, \mathbb{Q}e) \tag{8.68}$$

after choice of a $\mathbb{Z}e$–basis of $T_l(E)$.

The following Theorem characterizes the image $\rho_l(Gal(\bar{K}/K))$ in $Aut(T_l(E))$ for number field K.

Theorem 14. *(Serse). Let K be a number field and E/K an elliptic curve without complex multiplication.*

(1) $\rho_l(Gal(\bar{K}/K))$ is of finite index in $Aut(T_l(E))$, $\forall l$.

(2) $\rho_l(Gal(\bar{K}/K)) = Aut(T_l(E))$ for all but finitely many primes l.

8.4 The Weil Pairing

Let E/K be an elliptic curve. Let us fix an integer $m \geq 2$, relative prime to the characteristic $char(K) = p > 0$. Recall that $\sum_i n_i(P_i)$ is the divisor of an (elliptic) function, i.e. an element of $\bar{K}(E)$, iff $\sum_i n_i = 0$ and $\sum_i [n_i]P_i = O$. Let $T \in E[m]$. Then there is a function $f \in \bar{K}(E)$ such that

$$div(f) = m(T) - m(O)\,. \tag{8.69}$$

Letting $T' \in E$ with $[m]T' = T$, there is a function $g \in \bar{K}(E)$ satisfying

$$div(g) = [m]^*(T) - [m]^*(O) = \sum_{R \in E[m]} \left((T' \boxplus R) - (R)\right)\,, \tag{8.70}$$

where the equality $\sum_{R \in E[m]} T' \boxplus R \boxplus -R = 0$ follows from two facts:

(1) $\#E[m] = m^2$ (Eq(↑???)),

(2) $[m^2]T' = [m] \circ [m]T' = [m]T = 0$.

It is easy to quickly verify that functions $f \circ [m]$ and g^m have the same divisors, i.e. perhaps after the multiplication by an element of $\bar{K}^*$, we may assume that $f \circ [m] = g^m$.

Now suppose that $S \in E[m]$ is another m–torsion point (it could be $T = S$). Then for any point $X \in E$,

$$\begin{aligned}(g\,(X \boxplus S))^m &= f\,([m]\,(X \boxplus S)) \\ &= f\,([m]X \boxplus [m]S) = f\,([m]X) = (g(X))^m\,.\end{aligned} \tag{8.71}$$

Hence we can define a pairing

$$\begin{aligned} e_m:\ E[m] \times E[m] &\longrightarrow \mu_m\,, \\ (S,T) &\longmapsto \frac{g(X \boxplus S)}{g(X)}\,, \end{aligned} \tag{8.72}$$

where $X \in E$ is a point such that $g(X \boxplus S)$, $g(X)$ are both defined and non–zero, and $\mu_m = \left\{e^{\frac{2\pi i}{m}j} \,|\, j = 0, \ldots, m-1\right\}$ is the set of m–th roots of unity. Although g is only defined up to multiplication by an element of $\bar{K}^*$, $e_m(S,T)$ is independent of this choice. This pairing is called the Weil e_m–pairing.

Theorem 15. *The Weil e_m–pairing has the following properties:*

(1) *Bilinear:*

$$\begin{aligned} e_m(S_1 \boxplus S_2, T) &= e_m(S_1, T)\, e_m(S_2, T) \\ e_m(S, T_1 \boxplus T_2) &= e_m(S, T_1)\, e_m(S, T_2)\ \forall S, S_1, S_2, T, T_1, T_2 \in E\,. \end{aligned} \tag{8.73}$$

(2) *Alternating:*

$$e_m(T, T) = 1, \quad e_m(S, T) = e_m(T, S)^{-1}\,. \tag{8.74}$$

(3) *Non–degenerate: If $e_m(S, T) = 1\ \forall S \in E[m]$, then $T = 0$.*

(4) *Galois invariant: For all $g \in Gal(\bar{K}/K)$,*

$$e_m(S, T)^g = e_m(S^g, T^g)\,. \tag{8.75}$$

(5) *Compatibility with "multiplication -by- m'" isogenies:*

$$e_{mm'}(S, T) = e_m\left([m']S, T\right)\,. \tag{8.76}$$

Proof:

(1) The proof of the linearity in the first argument is easy:

$$\begin{aligned} e_m(S_1 \boxplus S_2, T) &= \frac{g\left(X \boxplus S_1 \boxplus S_2\right)}{g\left(X \boxplus S_1\right)} \frac{g\left(X \boxplus S_1\right)}{g\left(X\right)} \\ &= e_m\left(S_2, T\right)\, e_m\left(S_1, T\right)\,, \end{aligned} \tag{8.77}$$

because in $e_m\left(S_2, T\right) = \frac{g(Y \boxplus S_2)}{g(Y)}$, we may choose any value for Y, such as $Y = X + S_1$. For the second, let $f_1, f_2, f_3,\ g_1, g_2, g_3$ be functions as above for $T_1, T_2,\ T_3 = T_1 \boxplus T_2$. Choose $h \in \bar{K}(E)$ with divisor

$$div(h) = (T_1 \boxplus T_2) - (T_1) - (T_2) + (0)\,. \tag{8.78}$$

Then $div\left(\frac{f_3}{f_1 f_2}\right) = m\, div(h)$, so $f_3 = c f_1 f_2 h^m$ for some $c \in \bar{K}^*$. Compose with the multiplication -by- $[m]$ map, use $f_i \circ [m] = g_i^m$, we arrive at

$$\begin{aligned} g_3^m = f_3 \circ [m] &= c f_1 f_2 h^m \circ [m] = c\left(f_1 \circ [m]\right)\left(f_2 \circ [m]\right)\left(h^m \circ [m]\right) \\ &= c g_1^m g_2^m\left(h^m \circ [m]\right)\,. \end{aligned} \tag{8.79}$$

Taking the m–th roots of unity, we find

$$g_3 = c' g_1 g_2\left(h \circ [m]\right), \quad c' \in \bar{K}^*\,. \tag{8.80}$$

Finally,

$$\begin{aligned} e_m\left(S, T_1 \boxplus T_2\right) = \frac{g_3\left(X \boxplus S\right)}{g_3(X)} &= \frac{g_1\left(X \boxplus S\right)\ g_2\left(X \boxplus S\right)\ h\left([m]X + [m]S\right)}{g_1(X)\, g_2(X)\, h\left([m]X\right)} \\ &= e_m\left(S, T_1\right)\ e_m\left(S, T_2\right)\,. \end{aligned} \tag{8.81}$$

(2) It follows from (1),

$$e_m\,(S+T,S+T) = e_m(S,S)\,e_m(S,T)\,e_m(T,S)\,e_m(T,T)\,, \qquad (8.82)$$

so it is sufficient to prove that $e_m(T,T) = 1$ for all $T \in E[m]$. For any $P \in E$, recall that $T_P : E \to E$ denotes the translation by -P- map. Then

$$div\left(\prod_{i=0}^{m-1} f \circ T_{[i]T}\right) = m\sum_{i=0}^{m-1}([1-i]T) \boxminus ([-i]T) = 0\,, \qquad (8.83)$$

hence $\prod_{i=0}^{m-1} f \circ T_{[i]T}$ is constant function. If we choose some $T' \in E,\ [m]T' = T$, then $\prod_{i=0}^{m-1} g \circ T_{[i]T'}$ is also constant (because its m–th power is the former product of $f's$). Evaluating the product of $g's$ at X, $X+T'$ yields

$$\prod_{i=0}^{m-1} g\,(X \boxplus [i]T') = \prod_{i=0}^{m-1} g\,(X \boxplus [i+1]T')\ , \qquad (8.84)$$

i.e.

$$g(x) = g\,(X \boxplus [m]T') = g\,(X \boxplus T)\ . \qquad (8.85)$$

This gives immediately the required result,

$$e_m(T,T) = \frac{g\,(X \boxplus T)}{g\,(X)} = 1\,. \qquad (8.86)$$

(3) We shall use the following fact, which we did not prove if $g\,(X \boxplus S) = g\,(X)$ for all $S \in E[m]$, then $\exists h \in \bar{K}(E) : g = h \circ [m]$. Let $e_m(S,T) = 1$ for all $S \in E[m]$, so $g\,(X \boxplus S) = g\,(X)$ for all $S \in E[m]$. But then

$$(h \circ [m])^m = g^m = f \circ [m]\,, \qquad (8.87)$$

so $f = h^m$. Hence

$$m\,div(h) = div(f) = m(T) - m(0)\,, \qquad (8.88)$$

so

$$div(h) = (T) - (0)\,. \qquad (8.89)$$

Because h is an elliptic function, $T = 0$ and the form is non–degenerate.

(4) Let $g \in Gal\left(\bar{K}/K\right)$. If f, g are the functions for T as above, then f^g, g^g are corresponding functions for T^σ. Then

$$e_m\,(S^g, T^g) = \frac{g^g\,(X^g \boxplus S^g)}{g^g\,(X^g)} = \left(\frac{g\,(X \boxplus S)}{g\,(X)}\right)^g = e_m\,(S,T)^g \qquad (8.90)$$

(5) We have

$$div\left(f^{m'}\right) = mm'(T) - nm'(0) \tag{8.91}$$

and

$$(g \circ [m'])^{mm'} = (f \circ [mm'])^{m'} \ . \tag{8.92}$$

Then from the definition of $e_{mm'}, e_m$,

$$\begin{aligned} e_{mm'}(S,T) = \frac{(g \circ [m'])\,(X \boxplus S)}{(g \circ [m'])\,(X)} &= \frac{g\,(Y \boxplus [m']S)}{g\,(Y)} \\ &= e_m\,([m']S, T) \ . \end{aligned} \tag{8.93}$$

■

An easy consequence of this Theorem is the surjectivity of Weil pairing.

Corollary 8. *There exist points $S, T \in E[m]$ such that $e_m(S,T)$ is a primitive m–th root of unity.*

If $\varphi : E_1 \to E_2$ is an isogeny and $\hat{\varphi} : E_2 \to E_1$ its dual isogeny. Then it is easy to prove that $\varphi, \hat{\varphi}$ are dual operators w.r. to the Weil pairing.

Proposition 6. *Let $S \in E_1[m]$, $T \in E_2[m]$, $\varphi : E_1 \to E_2$ an isogeny, $\hat{\varphi} : E_2 \to E_1$ its dual isogeny. Then*

$$e_m\,(S, \hat{\varphi}(T)) = e_m\,(\varphi(S), T) \ . \tag{8.94}$$

Let l be a prime number, $g \subset d\,(l, char(K)) = 1$. We would like to fit together the pairings

$$l_{e^n} : \ E[e^n] \times E[e^n] \longrightarrow \mu_{e^n} \ , \quad n = 1, 2 \ldots \tag{8.95}$$

to give an l–adic pairing on the Tate module:

$$l : \ T_l(E) \times T_l(E) \longrightarrow T_l(\mu) \,. \tag{8.96}$$

The inverse limits for $T_l(e), T_l(\mu)$ are formed using the maps

$$e[l^{n+1}] \xrightarrow{[l]} E[l^n], \quad \mu_{l^n+1} \xrightarrow{l} \mu_{l^n} \ . \tag{8.97}$$

Thus to show that the e^{l^n}–pairings are compatible with taking the inverse limit, we must show that for any $S, T \in E[l^n + 1]$,

$$e_{e^{n+1}}(S,T)^l = e_{e^n}\,([l]S, [l]T) \ . \tag{8.98}$$

By linearity Th(↑???),

$$e_{e^{l+1}}(S,T)^l = e_{e^n+1}(S, [l]T) \,. \tag{8.99}$$

By compatibility Th(↑???), (5)$(m = l^n, \ m' = l)$,

$$e_{l^{n+1}}(S,T)^l = e_{l^{n+1}}(S, [l]T) = e_{l^n}([l]S, [l]T) \,, \tag{8.100}$$

which proves the following proposition.

Proposition 7. *There exists a bilinear, alternating, non–degenerate, Galois–invariant pairing*

$$e : \ T_l(E) \times T_l(E) \longrightarrow T_l(\mu) \,. \tag{8.101}$$

8.5 The endomorphism ring and the automorphism group of elliptic curves

Let E/K be an elliptic curve. We derived the following properties of the ring of endomorphisms of elliptic curve:

- $End(E/K)$ is a characteristic 0 integral domain of rank at most 4 over $\mathbb{Z}$.
- $End(E)$ possesses an anti involution $\hat{\ }: End(E) \to End(E)$.
- For $\varphi \in End(E)$, we have $\varphi\hat{\varphi} \in \mathbb{Z},\ \varphi\hat{\varphi} \geq 0$ and $\varphi\hat{\varphi} = 0 \Leftrightarrow \varphi = 0$.

It is possible to classify the rings with these properties.

Definition 18. *Let $A/\mathbb{Q}$ be a finitely generated $\mathbb{Q}$–algebra (not necessarily commutative). An order R_A of A is a subring of A, finitely generated over $\mathbb{Z}$ and fulfilling $R_A \otimes \mathbb{Q} \xrightarrow{\sim} A$.*

Ex. 11. *Let K be a quadratic imaginary field and $\mathcal{O}_K$ its ring of integers. Then $\forall f \in \mathbb{Z},\ f > 0$, the ring $\mathbb{Z} + f\mathcal{O}$ is an order of K (and each order can be constructed in this way).*

Definition 19. *A quaternion algebra $A/\mathbb{Q}$ is as a $\mathbb{Q}$–vector space*

$$A/\mathbb{Q} = \mathbb{Q} + \mathbb{Q}\alpha + \mathbb{Q}\beta + \mathbb{Q}\alpha\beta \tag{8.102}$$

with the multiplication rules

$$\alpha^2, \beta^2 \in \mathbb{Q}, \quad \alpha^2 < 0,\ \beta^2 < 0,\ \alpha\beta = -\beta\alpha. \tag{8.103}$$

These algebras are more properly called definite quaternion algebras over $\mathbb{Q}$.

The main result, which we shall not prove, is:

Theorem 16. *Let R be a ring fulfilling*

- *$char(R) = 0$, R has no zero divisors,*
- *There is an anti–involution $\alpha \to \hat{\alpha}$, i.e. $\widehat{\alpha + \beta} = \hat{\alpha} + \hat{\beta},\ \widehat{\alpha\beta} = \hat{\beta}\hat{\alpha},\ \hat{\hat{\alpha}} = \alpha,\ \alpha = \hat{\alpha}$ for $\alpha \in \mathbb{Z}$,*
- *for $\alpha \in R,\ \alpha\hat{\alpha} \in \mathbb{Z}_+,\ \alpha\hat{\alpha} = 0 \Leftrightarrow \alpha = 0$.*

Then R is one of the following rings:

(1) $R \xrightarrow{\sim} \mathbb{Z}$,

(2) R is an order in a quadratic imaginary extension of $\mathbb{Q}$.

(3) R is an order in a quaternion algebra over $\mathbb{Q}$

Proof: See [5], Th. 9.3., p.100. ■

Note that the isomorphism classes of quaternion algebras are classified by $Br(\mathbb{Q}) \xrightarrow{\sim} H^2\left(Gal\left(\bar{\mathbb{Q}}/\mathbb{Q}\right), \bar{\mathbb{Q}}^*\right)$, $Br\left(\mathbb{Q}_p\right) \xrightarrow{\sim} H^2\left(Gal\left(\bar{\mathbb{Q}}_p/\mathbb{Q}_p\right), \bar{\mathbb{Q}}_p^*\right)$. The computation of the group of automorphisms of an elliptic curve is much simper then the determination of its ring of endomorphisms.

Theorem 17. *Let E/K be an elliptic curve. Then its automorphism group $Aut(E)$ is a finite group of order dividing 24. More precisely, we have the following set of possibilities:*

- $\#Aut(E) = 2$ *iff* $j(E) \neq 0,\ 1728$*;*
- $\#Aut(E) = 4$ *iff* $j(E) = 1728 \wedge char(K) \neq 2,\ 3$*;*
- $\#Aut(E) = 6$ *iff* $j(E) = 0 \wedge char(K) \neq 2,\ 3$*;*
- $\#Aut(E) = 12$ *iff* $j(E) = 0 = 1728 \wedge char(K) = 3$*;*
- $\#Aut(E) = 24$ *iff* $j(E) = 0 = 1728 \wedge char(K) = 2$.

Proof: Let us restrict to the case $char(K) \neq 2,\ 3$. The normal form of E/K is

$$E: \ y^2 = x^3 + Ax + B, \quad A, B \in K\,. \tag{8.104}$$

Every automorphism is of the form (see Eq(⇈???))

$$\begin{aligned} x' &\longmapsto x = u^2 x'\,, \\ y' &\longmapsto y = u^3 y'\,, \quad u \in \bar{K}^*\,. \end{aligned} \tag{8.105}$$

This implies that

$$\begin{aligned} A' &\longmapsto A = u^{-4} A'\,, \\ B' &\longmapsto B = u^{-6} B'\,, \end{aligned} \tag{8.106}$$

and because Eq(↑???) gives the automorphism,

$$u^{-4} A = A, \quad u^{-6} B = B\,. \tag{8.107}$$

Hence if $AB \neq 0$ (i.e. $j(E) \neq 0,\ 1728$), the only possibilities are $u = \pm 1$. $(g \subset d(4,6) = 2)$. If $B = 0$ ($j(E) = 1728$) or $A = 0$ ($j(E) = 0$), then u satisfies respectively $u^4 = 1$ or $u^6 = 1$, so $Aut(E)$ will be cyclic group of order 4 or 6. ■

Chapter 9

Jacobi q-parametrisation, q-expansion of Eisenstein series

For a lattice $L, L = \mathbb{Z}_{w_1} \oplus \mathbb{Z}_{w_1}$ with $\tau = \frac{w_1}{w_2}$ for $Im(\tau) > 0$, we have $L = w_2 L_\tau$ where $L_\tau = \mathbb{Z}\tau + \mathbb{Z}$. Now multiplication by ω_2 carries $\mathbb{C}/L$ with $\mathbb{C}/L_\tau$ isomorphically and substitution $f \to f\omega_2 \quad (f(z) \to f(\omega_2 z)\, \forall z \in \mathbb{C})$ carries the field of elliptic functions for L isomorphically into the field of elliptic functions for L_τ.

A function $f, f : \mathbb{C}/L \to \mathbb{C}$, on the focus $\mathbb{C}/L$ is equivalent to a function $g : \mathbb{C} \to \mathbb{C}$ which is L-periodic, i.e. $g(z + w) = g(z)\, \forall \omega \in L$. For a projection $p : \mathbb{C} \to \mathbb{C}/L$, we have $g = fp$.

Definition 20. *Two lattices $L, L' \subseteq \mathbb{C}$ are equivalent provided there exists $\lambda \in \mathbb{C}^*$ with $\lambda L = L'$, i.e. L, L' are homothetic. Multiplication by $\lambda \in \mathbb{C}^*$, $\lambda : \mathbb{C} \to \mathbb{C}, z \to \lambda z$ induces an isomorphism $T = \mathbb{C}/L \to \mathbb{C}/L' = T'$, also denoted by λ, defined by the commutative diagram*

$$\begin{array}{ccc} \mathbb{C} & \xrightarrow{\lambda} & \mathbb{C} \\ \Big\downarrow p & & \Big\downarrow p' \\ T = \mathbb{C}/L & \xrightarrow{\lambda} & \mathbb{C}/L' = T' \end{array}$$

Remark 5. *Any $\lambda \in \mathbb{C}$ satisfying $\lambda L \subset L'$ induces a homomorphism, also denoted $\lambda : T = \mathbb{C}/L \to T' = \mathbb{C}/L'$ as in the previous definition, either*

$$\mathbb{C}/L \to \mathbb{C}/\lambda L \to \mathbb{C}/L'$$

$\lambda = 0 \in \mathbb{C}$ or $\lambda \in \mathbb{C}^* : T \to T'$ is surjective with kernel isomorphic to $L'/_{\lambda L} \simeq \lambda^{-1} L'/_L$. Such a nonzero morphism is called an isogeny.

Under the analytic map

$$\begin{array}{ccc} z & \xrightarrow{\exp} & exp(2\pi i z) = w \\ \cap & & \cap \\ \mathbb{C} & \longrightarrow & \mathbb{C}^* \end{array}$$

, $Ker(exp) \simeq \mathbb{Z}$. The lattice $L = \mathbb{Z}\tau + \mathbb{Z} \subset \mathbb{C}$ is mapped to $q^{\mathbb{Z}} \subset \mathbb{C}^*$, the infinite cyclic set group p of $\mathbb{C}^*$ generated by $q = exp(2\pi i\tau)$, $|q| < 1$ (for $Im(\tau) > 0$). In other words, we have analytic isomorphism

$$E_\tau = \mathbb{C}/L\tau \longrightarrow \mathbb{C}^*/q^{\mathbb{Z}}.$$

Let us start with the well known formula from complex analysis:

$$\sum_{n\in\mathbb{Z}} \frac{1}{(\xi+n)^2} = \frac{\pi^2}{\sin^2 \pi\xi}$$

For $T = e^{2\pi i\xi}$ this becomes

$$\begin{aligned} \sum_{n\in\mathbb{Z}} \frac{1}{(\xi+n)^2} &= (2\pi i)^2 \frac{1}{(e^{i\pi\xi} - e^{-i\pi\xi})} = (2\pi i)^2 \frac{e^{2\pi i\xi}}{(1-e^{2\pi i\xi})^2} = \\ &= (2\pi i)^2 \frac{T}{(1-T)^2} = (2\pi i)^2 \sum_{n\geq 1} nT^n. \end{aligned} \tag{9.1}$$

The chain rule implies $\frac{\mathrm{d}}{\mathrm{d}\,\xi} = (2\pi i)T\frac{\mathrm{d}}{\mathrm{d}\,T}$, $\left(\frac{\mathrm{d}}{\mathrm{d}\,\xi}\right)^{\otimes k-2} = (2\pi i)^{k-2}\left(T\frac{\mathrm{d}}{\mathrm{d}\,T}\right)^{\otimes k}$ and

$$(k-1)!\,(-1)^k \sum_{n\in\mathbb{Z}} \frac{1}{(\xi+n)^k} = (2\pi i)^k \sum_{n\geq 1} n^{k-1}T^n = (2\pi i)^k\, g_k(T)\,,\ k \geq 2.$$

Note that

$$\begin{aligned} g_{k+1}(T) &= \left(T\frac{\mathrm{d}}{\mathrm{d}\,T}\right) g_k(T)\,, \\ g_k\left(\frac{1}{T}\right) &= (-1)^k\, g_k(T). \end{aligned} \tag{9.2}$$

The first property is trivial, the second follows from the first using

$$\frac{\mathrm{d}}{\mathrm{d}\,T} = T\frac{\mathrm{d}}{\mathrm{d}\left(\frac{1}{T}\right)}\frac{\mathrm{d}\left(\frac{1}{T}\right)}{\mathrm{d}\,T} = -\frac{1}{T}\frac{\mathrm{d}}{\mathrm{d}\left(\frac{1}{T}\right)} \Longrightarrow \left(T\frac{\mathrm{d}}{\mathrm{d}\left(\frac{1}{T}\right)}\right)^k = (-1)^k\left(\frac{1}{T}\frac{\mathrm{d}}{\mathrm{d}\left(\frac{1}{T}\right)}\right)^k$$

Two important special cases are

$$g_2(T) = \frac{T}{(1-T)^2}, \quad g_3(T) = T\frac{1+T}{(1-T)^3}.$$

The following modular functions, called Eisenstein series, arose for example as the coefficients of Weierstrass γ-function ($\wedge = \mathbb{Z} \oplus \tau\mathbb{Z}$):

$$G_{2k}(\tau) = \sum_{(m,n)\neq(0,0)} \frac{1}{(m\tau+n)^{2k}} = 2\sum_{n\geq 1}\frac{1}{n^{2k}} + 2\sum_{m\geq 1}\sum_{n\in\mathbb{Z}}\frac{1}{(m\tau+n)^{2k}}$$

which for $q = e^{2\pi i\tau}$ becomes

$$2\zeta(2k) + 2\frac{(2\pi i)^{2k}}{(2k-1)!}\sum_{m,n\geq 1} n^{2k-1}q^{mn},$$

where $\zeta(s) = \sum_{n\geq 1} n^{-s}$ is the Riemann zeta function. For $\tau_s(n) = \sum_{d|m} d^s$ this formula takes the form of so called q-expansion of the Eisenstein series,

$$\begin{aligned} G_{2k}(\tau) &= 2\zeta(2k) + 2\frac{(2\pi i)^{2k}}{(2k-1)!}\sum_{n\geq 1}\tau_{2k-1}(n)q^n \\ &= 2\zeta(2k) + 2\frac{(2\pi i)^{2k}}{(2k-1)!}\sum_{n\geq 1}\frac{n^{2k-1}q^n}{1-q^n}. \end{aligned} \tag{9.3}$$

Note that the numbers $n \to \tau_s(n)$ are the basic functions in the arithmetic of integers. Also

$$G_{2k}(\tau) \xrightarrow{Im(\tau)\to\infty} 2\zeta(2k).$$

There is suitable normalization: $G_{2k}(\tau) = 2\zeta(2k)E_{2k}(\tau)$, where

$$\begin{aligned} G_4(\tau) &= \frac{(2\pi i)^4}{720}\left(1 + 240\sum_{n\geq 1}\tau_3(n)q^n\right) = \frac{(2\pi i)^4}{720}E_4(\tau), \\ G_6(\tau) &= -\frac{(2\pi i)^6\cdot 2}{2^6 945}\left(1 - 504\sum_{n\geq 1}\tau_5(n)q^n\right) = -\frac{(2\pi i)^6\cdot 2}{2^6\cdot 3^3\cdot 5\cdot 7}E_4(\tau), \end{aligned} \tag{9.4}$$

hence

$$\begin{aligned} g_2(\tau) &= 60\,G_4(\tau) = \frac{(2\pi i)^4}{12}E_4(\tau), \\ g_3(\tau) &= 140\,G_6(\tau) = -\frac{(2\pi i)^6}{2^3 3^3}E_6(\tau). \end{aligned} \tag{9.5}$$

It is also easy to verify (HW)

$$\begin{aligned} \gamma(z,\tau) &= (2\pi i)^2\left(\sum_m \frac{wq^m}{(1-wq^m)^2} + \frac{1}{12} - \sum_{m\neq 0}\frac{q^m}{(1-q^m)^2}\right), \\ \gamma'(z,\tau) &= (2\pi i)^3\left(\sum_m \frac{wq^m(1+wq^m)}{(1-wq^m)^3}\right), \end{aligned} \tag{9.6}$$

which yields

Theorem 18. *The Weierstrass equation divided by $4(2\pi i)^6$ in terms of the variables $w = e^{2\pi iz}$ and $q = e^{2\pi i\tau}$ is*

$$E_q:\ y^2 = x^3 - e_2(q)x - e_3(q),$$

where

$$
\begin{aligned}
x = x(w,q) &= \sum_m \frac{wq^m}{(1-wq^m)} + \frac{1}{12} - 2\sum_{m\geq 1}\frac{q^m}{(1-q^m)^2},\\
y = y(w,q) &= \frac{1}{2}\sum_m \frac{wq^m(1+wq^m)}{(1-wq^m)^3},\\
e_2 = e_2(q) &= \frac{1}{48}E_4(\tau) = \frac{1}{48}\Big(1+240\sum_{n\geq 1}\tau_3(n)q^n\Big),\\
e_3 = e_3(q) &= -\frac{2}{12^3}E_6(\tau) = -\frac{2}{12^3}\Big(1-504\sum_{n\geq 1}\tau_5(n)q^n\Big). \qquad (9.7)
\end{aligned}
$$

Chapter 10

Definition of supersingular elliptical curves

Definition 21. *An elliptic curve E defined by a cubic equation $f(z,x,y)$ over a field K, $char(K) = p$, is supersingular provided the coefficient of $(zxy)^{p-1}$ in $f(z,x,y)^{p-1}$ is zero.*

Ex. 12. *For $p = 2$ the cannonical equation of elliptic curve E amounts*

$$E_0 : zy^2 + z^2y + axyz = x^3.$$

Since $p - 1 = 1$, E_a is supersingular iff $a = 0$, i.e.

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

The number $\#\left\{(x,y) \in \mathbb{F}_2^2 : y^2 + y = x^3\right\}$ is clearly 3.

Ex. 13. *For $p = 3$ the cannonical equation of elliptic curve E amounts*

$$E_{a,b,c} : x^3 + azx^2 + bz^2x + cz^3 - zy^2 = 0.$$

Since $p-1 = 2$, $E_{a,b,c}$ is supersingular iff $a = 0$ (because the coefficient of $(zxy)^2$ is equal to $-2a = a \bmod 3$). Hence the cannonical equation of supersingular elliptic curve E is

$$y^2 = x^3 + bx + c.$$

The linear transformation $x \to \alpha x + \beta$, $x^3 \to \alpha^3x^3 + \beta^3$ and suitable choice of α, β leads to the only one supersingular elliptic curve for $p = 3$:

$$y^2 = x^3 - x.$$

Obviously $\#\left\{(x,y) \in \mathbb{F}_3^2 : y^2 = x^3 - x\right\}$ is 4.

Lemma 6. *The coefficient of x^k in $(x-1)^k(x-\lambda)^k$ is*

$$(-1)^k \sum_{j=0}^{k} \binom{k}{j}^2 \lambda^j.$$

Proof:

Expand both

$$\begin{aligned} (x-1)^k &= \sum_a \binom{k}{a} (-1)^{k-a} x^a, \\ (x-\lambda)^k &= \sum_b \binom{k}{b} \lambda^{k-b} x^b. \end{aligned} \tag{10.1}$$

Hence the product is given by

$$(x-1)^k(x-\lambda)^k = \sum_i \sum_{a+b=i} \lambda^{k-b} \binom{k}{a} \binom{k}{b} (-1)^{2k-i} x^i.$$

Hence the coefficient of x^k is

$$(-1)^k \sum_{j=0}^{k} \binom{k}{j}^2 \lambda^j.$$

■

Lemma 7. *In characteristic $p > 2$ the curve in Legendre form $E_\lambda : y^2 = x(x-1)(x-\lambda)$ is supersingular iff λ is a root of the Hasse invariant*

$$H_p(\lambda) = (-1)^m \sum_{i=0}^{m} \binom{m}{i}^2 \lambda^i, \text{ where } m = \frac{p-1}{2}.$$

Proof:

Let us compute first the coefficient of $(xyz)^{p-1}$ in f^{p-1}, where

$$f(x,y,z) = zy^2 - x(x-z)(z-\lambda z).$$

In $f(x,y,z)^{p-1}$ the term $(xyz)^{p-1}$ will appear in the middle of binomical expansion, i.e. the term $\binom{p-1}{m} (zy^2)^m \left(x(x-z)(x-\lambda z)\right)^m$. Observe that $\binom{p-1}{m} = (-1)^m \bmod p$:

$$\begin{aligned} \binom{p-1}{\frac{p-1}{2}} = (-1)^{\frac{p-1}{2}} \bmod p \Leftrightarrow \underbrace{(p-1)\ldots\left(\frac{p+3}{2}\right)\left(\frac{p+1}{2}\right)}_{m} = \\ = (-1)^{\frac{p-1}{2}} \left(\frac{p-1}{2}\right)\left(\frac{p-3}{2}\right)\ldots 1 \bmod p \Leftrightarrow \end{aligned} \tag{10.2}$$

$$\Leftrightarrow \quad \left(-\tfrac{p-1}{2}\right)\left(-\tfrac{p-3}{2}\right)\dots(-1) \bmod p \quad \Leftrightarrow \quad \left(p-\tfrac{p-1}{2}\right)\left(p-\tfrac{p-3}{2}\right)\dots(p-1) \bmod p$$

$$\| \qquad\qquad\qquad\qquad \|$$

$$(p-1)\dots\left(\tfrac{p+3}{2}\right)\left(\tfrac{p+1}{2}\right) \bmod p \qquad\qquad (p-1)\dots\left(\tfrac{p+3}{2}\right)\left(\tfrac{p+1}{2}\right) \bmod p$$

Since $2m = p-1$, the coefficient of $(xyz)^{p-1}$ is just the coefficient of $(xz)^m$ in$((x-z)(x-\lambda z))^m$ up to factor $(-1)^m$. By the previous lemma **??**, this is $H_p(\lambda)$. ■

The expansion $G_p(\lambda) := (-1)^m H_p(\lambda) = \sum_{i=0}^m \left(\begin{array}{c} m \\ i \end{array}\right)^2 \lambda^i$ is called Denning polynomial. There are many equivalent criterions for a curve to be supersingular. One of them is the following:

Proposition 8. *An elliptic curve E is supersingular iff the invariant differential ω is exact.*

Proof:

For $p = 2$ we have $\omega = \mathrm{d}\,x/(ax+1)$ for $E_a : y^2 + y + axy = x^3$. Then ω is exact iff $a = 0$, i.e. E_a is supersingular. For $p > 2$ we have $\omega = \mathrm{d}\,x/2y$, and we put E in to the form $y^2 = x(x-1)(x-\lambda)$. Then ω is exact iff $y^{p-1}\,\mathrm{d}\,x/y^p$ is exact (note that $\mathrm{d}\,x/y = y^{p-1}/y^p\ \mathrm{d}\,x$) or $y^{p-1}\,\mathrm{d}\,x$ is exact (note $\mathrm{d}(f/g) = (\mathrm{d}\,f(g) - f\,\mathrm{d}\,g)/g^2 = \mathrm{d}\,f/g$, i.e. in *char* $= p$, $f = 0$, $g = y^p$, then $\mathrm{d}\,g = 0$). For $m = (p-1)/2$, we have

$$y^{p-1}\,\mathrm{d}\,x = [x(x-1)(x-\lambda)]^m\,\mathrm{d}\,x.$$

This form is exact iff the coefficient of x^{p-1} in $[x(x-1)(x-\lambda)]^m$ is zero (note that there is no other power of x divisible by p then just x^p). However this is just the coefficient of x^m in $[x(x-1)(x-\lambda)]^m$ is zero. By the lemma **??**, this coefficient is $G_p(\lambda)$. Now the proposition follows from lemma **??**. ■

Chapter 11

Hypergeometric functions, elliptic integrals and periods associated with elliptic curves

11.1 Hypergeometric functions and differential equations

Definition 22. *Let* $\mathrm{Re}\,(s) > 0$*. Then the gamma function* $\Gamma(s)$ *is defined by integral*

$$\Gamma(s) = \int_0^\infty x^s e^{-x} \frac{\mathrm{d}\,x}{x} \quad (x^{s-1} \in L^1 \langle 0, \varepsilon \rangle \ \textit{for} \ \mathrm{Re}\,(s) > 0!)$$

$\Gamma(s)$, defined for $\mathrm{Re}\,(s) > 0$, can be analytically continued to $\mathbb{C}$ as a meromorphic function with poles in $(-\mathbb{N})$ by

$$\Gamma(s) := \frac{\Gamma(s+n)}{s(s+1)\ldots(s+n-1)} \text{ for } \mathrm{Re}\,(s) > -n$$

By change of variables $x \rightarrow t = \sqrt{x}$, $\mathrm{d}\,x = 2t\,\mathrm{d}\,t$, $\mathrm{d}\,x/x = 2\,\mathrm{d}\,t/t$, the integral formula for gamma function becomes

$$\Gamma(s) = 2\int_0^\infty t^{2s} e^{-t^2} \frac{\mathrm{d}\,t}{t}.$$

Lemma 8. *For* $a, b \in \mathbb{N}_+$*, we have*

$$2\int_0^{\frac{\pi}{2}} \cos^{2a-1}\theta \sin^{2b-1}\theta\,\mathrm{d}\,\theta = \frac{\Gamma(a)\Gamma(b)}{\Gamma(a+b)}.$$

Proof:

$$\Gamma(a)\Gamma(b) = 4\int_0^\infty \int_0^\infty \xi^{2a-1}\eta^{2b-1}\exp\left(-\eta^2-\xi^2\right)\mathrm{d}\,\xi\,\mathrm{d}\,\eta = \\ = 2\int_0^\infty r^{2a+2b}e^{-r^2}\frac{\mathrm{d}\,r}{r}2\int_0^{\frac{\pi}{2}}\cos^{2a-1}\theta\sin^{2b-1}\theta\,\mathrm{d}\,\theta. \tag{11.1}$$

■

For example, $a = b = 1/2$ gives $2\int_0^{\frac{\pi}{2}}\mathrm{d}\,\theta = \Gamma(1/2)\Gamma(1/2)/\Gamma(1) = \Gamma(1/2)^2$, hence $\Gamma(1/2) = \sqrt{\pi}$. The gamma function allows to analytically continue not only factorial, but also binomial formulas

$$\begin{pmatrix} s \\ n \end{pmatrix} := \frac{s(s-1)\dots(s-n+1)}{n!},$$

$$(1+x)^s := \sum_{n\geq 0}\begin{pmatrix} s \\ n \end{pmatrix} x^n \text{ for } |x|<1,\ \mathrm{Re}\,(s)>0, \tag{11.2}$$

Proposition 9. *The relation*

$$2\int_0^{\frac{\pi}{2}}\sin^{2m}\theta\,\mathrm{d}\,\theta = \pi\,(-1)^m\begin{pmatrix} -1/2 \\ m \end{pmatrix}$$

holds for any $m \in \mathbb{N}$.

Proof:

$$2\int_0^{\frac{\pi}{2}}\sin^{2m}\theta\,\mathrm{d}\,\theta = \frac{\Gamma(\frac{1}{2})\Gamma(m+\frac{1}{2})}{\Gamma(m+1)} = \frac{\Gamma(\frac{1}{2})(m-\frac{1}{2})(m-\frac{3}{2})\dots\frac{1}{2}\Gamma(\frac{1}{2})}{m(m-1)\dots 2\cdot 1} \\ = \pi\,(-1)^m\begin{pmatrix} -\frac{1}{2} \\ m \end{pmatrix}. \tag{11.3}$$

■

We use the following notation:

$$(a)_n \begin{cases} (a)_0 = 1 \\ (a)_n = a(a+1)\dots(a+n-1) = (a+n-1)(a)_{n-1}. \end{cases}$$

Definition 23. *The hypergeometric series for $a, b \in \mathbb{C}$, $c \in \mathbb{C}\backslash\mathbb{N}$ is given by*

$$F(a,b,c,z) = \sum_{n\geq 0}\frac{(a)_n(b)_n}{(c)_n n!}z^n.$$

An easy application of the ratio test shows that $F(a,b,c,z)$ is absolutely convergent for $|z| < 1$ and uniformly convergent for $|z| \leq r \leq 1$, and, hence, it represents an analytic function on the unit disc called hypergeometric function.

11.2 Properties of hypergeometric functions:

$$\left.\begin{array}{lrcl} 1) & F(a,b,c,z) & = & F(b,a,c,z), \\ 2) & F(a,b,b,z) & = & (1-z)^{-q}, \\ 3) & F(a,a,1,z) & = & \sum\limits_{n\geq 0} \begin{pmatrix} -a \\ n \end{pmatrix}^2 z^n. \end{array}\right\} \quad \text{use} \quad \begin{array}{rcl} (1)_n & = & n! \\ \frac{(a)_n}{n!} & = & (-1)^n \begin{pmatrix} -a \\ n \end{pmatrix} \end{array}$$

In particular, $F\left(\frac{1}{2},\frac{1}{2},1,z\right) = \sum_{n\geq 0} \begin{pmatrix} -\frac{1}{2} \\ n \end{pmatrix}^2 z^n$.

The hypergeometric function F satisfies the following differential equation called hypergeometric differential equation:

$$z(1-z)\frac{\mathrm{d}^2}{\mathrm{d}\,z^2}F + \Big[c-(a+b+1)z\Big]\frac{\mathrm{d}}{\mathrm{d}\,z}F - abF = 0.$$

In the case $F\left(1/2,1/2,1,z\right)$, we have

$$z(1-z)\frac{\mathrm{d}^2}{\mathrm{d}\,z^2}F + (1-2z)\frac{\mathrm{d}}{\mathrm{d}\,z}F - \frac{1}{4}F = 0.$$

Theorem 19. *For a complex number λ, $|\lambda|<1$, holds*

$$2\int_0^{\frac{\pi}{2}} \left(1-\lambda\sin^2\theta\right)^{-\frac{1}{2}}\mathrm{d}\,\theta = \pi F\left(\frac{1}{2},\frac{1}{2},1,\lambda\right).$$

Proof:

Binomial formulas imply

$$\left(1-\lambda\sin^2\theta\right)^{-\frac{1}{2}} = \sum_{n\geq 0} \begin{pmatrix} -\frac{1}{2} \\ n \end{pmatrix} (-\lambda)^n \sin^{2n}\theta.$$

Uniform convergence on compact subsets of $|\lambda|<1$ implies

$$2\int_0^{\frac{\pi}{2}} \left(1-\lambda\sin^2\theta\right)^{-\frac{1}{2}}\mathrm{d}\,\theta = \sum_{n\geq 0} \begin{pmatrix} -\frac{1}{2} \\ n \end{pmatrix} (-\lambda)^n \int_0^{\frac{\pi}{2}} \sin^{2n}\theta\,\mathrm{d}\,\theta,$$

and so

$$\begin{aligned} 2\int_0^{\frac{\pi}{2}} \left(1-\lambda\sin^2\theta\right)^{-\frac{1}{2}}\mathrm{d}\,\theta &= \sum_{n\geq 0} \begin{pmatrix} -\frac{1}{2} \\ n \end{pmatrix} (-1)^n\lambda^n \left(\pi\,(-1)^n \begin{pmatrix} -\frac{1}{2} \\ n \end{pmatrix}\right) \\ &= \pi\sum_{n\geq 0} \begin{pmatrix} -\frac{1}{2} \\ n \end{pmatrix}^2 \lambda^n = \pi F\left(\frac{1}{2},\frac{1}{2},1,\lambda\right). \end{aligned} \tag{11.4}$$

■

<u>HW</u>. *Show that, for $|z|<1$:*

1/ $zF(1,1,2,-z) = \log(1+z)$,

2/ $\frac{\mathrm{d}}{\mathrm{d}\,z}F(a,b,c,z) = \frac{ab}{c}F(a+1,b+1,c+1,z)$.

11.3 Periods associated with elliptic curves-elliptic integrals

Let $\mathrm{E}/\mathbb{C}$ be a complex elliptic curve, $\mathrm{E}/\mathbb{C}: \ y^2 = f(x), \deg f = 3$. We wish to determine a complex forms $\mathbb{C}/L$ with $L = \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2$ such that $(\gamma, \gamma') : \mathbb{C}/L \to \mathrm{E}(\mathbb{C})$ is an analytic isomorphism. The goal is to determine ω_1, ω_2 in terms of $\mathrm{E}/\mathbb{C}(\mathbb{C})$ using the fact that ω_1, ω_2 are examples of period integrals

$$\omega_1 = \int_{\mathrm{C}_1} \omega \quad \omega_2 = \int_{\mathrm{C}_2} \omega, \quad \omega = \frac{\mathrm{d}\,x}{f'(x)} = \frac{\mathrm{d}\,x}{2y} \left((\gamma, \gamma')^* \frac{\mathrm{d}\,x}{f'(x)} = \mathrm{d}\,z \right).$$

where $\mathrm{C}_1, \mathrm{C}_2$ are suitably chosen curves in $\mathrm{E}/\mathbb{C}(\mathbb{C})$, for example $\{\mathrm{C}_1, \mathrm{C}_2\} = \mathrm{E}(\mathbb{R})$ if E is defined over $\mathbb{R}$.
In general, the suitably chosen closed paths on $\mathrm{E}(\mathbb{C})$ are determined by projection $(\gamma, \gamma') \xrightarrow{\pi} \gamma$ inducing $2:1$ ramified map between Riemann surface of $\mathrm{E}/\mathbb{C}$ and the Riemann sphere. The choice of ramification points corresponding to half-periods $0, \frac{\omega_1}{2}, \frac{\omega_2}{2}, \frac{\omega_1+\omega_2}{2}$ leads to the the following explicit description:
We can normalize the roots of f in such a way that $\gamma\left(\frac{\omega_1}{2}\right) \to 0$, $\gamma\left(\frac{\omega_2}{2}\right) \to 1$, $\gamma\left(\frac{\omega_1+\omega_2}{2}\right) \to \lambda$ for the elliptic curve in Legendre form $E_\lambda : \ y^2 = x(x-1)(x-\lambda)$ for $\lambda \in \mathbb{C} \setminus \{0, 1\}$. It follows from the invariance of j-function, $j : \mathbb{C} \to \mathbb{C}$, that $j(\lambda) = j(1-\lambda) = j(1/\lambda) = j(1/(1-\lambda)) = j((\lambda-1)/\lambda) = j(\lambda/(\lambda-1))$. Let us choose $\lambda \in \mathbb{C} \setminus \{0, 1\}$ such that $|\lambda| < 1$, $|\lambda - 1| < 1$, and calculate $\omega_1(\lambda)$, $\omega_2(\lambda)$ for λ in this open set:

$$\begin{aligned} \omega_1(\lambda) &= \int_{\mathrm{C}_1} \omega = \int_{\mathrm{C}_1{}'} \frac{\mathrm{d}\,x}{2\sqrt{x(x-1)(x-\lambda)}}, \\ \omega_2(\lambda) &= \int_{\mathrm{C}_2} \omega = \int_{\mathrm{C}_2{}'} \frac{\mathrm{d}\,x}{2\sqrt{x(x-1)(x-\lambda)}}. \end{aligned} \tag{11.5}$$

In the limit when $\omega \to 0$ and C_1, C_2 are sides of the fundamental parallelogram, the contours $\mathrm{C}_1{}'$, $\mathrm{C}_2{}'$ $\big(\mathrm{C}_i{}' = \gamma(\mathrm{C}_i),\ i = 1, 2\big)$ give rise to the computable integral expression for periods:

$$\begin{aligned} \omega_1(\lambda) &= \int_{-\infty}^{0} \frac{\mathrm{d}\,x}{\sqrt{x(x-1)(x-\lambda)}}, \\ \omega_2(\lambda) &= \int_{1}^{\infty} \frac{\mathrm{d}\,x}{\sqrt{x(x-1)(x-\lambda)}}. \end{aligned} \tag{11.6}$$

Theorem 20. *For a complex number λ, $|\lambda| < 1$, $|\lambda - 1| < 1$, the periods have the following form in terms of the hypergeometric function*

$$\begin{aligned} \omega_1(\lambda) &= i\pi F\left(\frac{1}{2}, \frac{1}{2}, 1, 1-\lambda\right), \\ \omega_2(\lambda) &= \pi F\left(\frac{1}{2}, \frac{1}{2}, 1, \lambda\right). \end{aligned} \tag{11.7}$$

For the lattice $\mathrm{L}_\lambda = \mathbb{Z}\omega_1(\lambda) + \mathbb{Z}\omega_2(\lambda)$ *the complex tori* $\mathbb{C}/\lambda L$ *and* $\mathrm{E}_\lambda(\mathbb{C})$ *are isomorphic by a map valued in affine combination of the Weierstrass* γ*-function and its derivative.*

Proof:

The periods can be computed by suitable change of variables. As for $\omega_2(\lambda)$, we change the variable $t \to x = 1/t$, $t = s^2$, $s = \sin\theta$:

$$\begin{aligned}\omega_2(\lambda) &= \int_1^\infty \frac{\mathrm{d}\,x}{\sqrt{x(x-1)(x-\lambda)}} = \int_1^0 \frac{-\frac{\mathrm{d}\,t}{t^2}}{\sqrt{\frac{1}{t}\left(\frac{1}{t}-1\right)\left(\frac{1}{t}-\lambda\right)}} = \int_0^1 \frac{\mathrm{d}\,t}{\sqrt{t(1-t)(1-\lambda t)}} \\ &= 2\int_0^1 \frac{\mathrm{d}\,s}{\sqrt{(1-s^2)(1-\lambda s^2)}} = \int_0^{\frac{\pi}{2}} \frac{\mathrm{d}\,\theta}{\sqrt{1-\lambda\sin^2\theta}} = \pi F\left(\frac{1}{2},\frac{1}{2},1,\lambda\right),\end{aligned} \tag{11.8}$$

The change of variables for $\omega_1(\lambda)$, $x \to y = -x+1\,(x = 1-y)$:

$$\begin{aligned}\omega_1(\lambda) &= \int_{-\infty}^0 \frac{\mathrm{d}\,x}{\sqrt{x(x-1)(x-\lambda)}} = \int_1^\infty \frac{\mathrm{d}\,y}{\sqrt{-(y-1)(-y)(y-(1-\lambda))}} \\ &= i\int_1^\infty \frac{\mathrm{d}\,y}{\sqrt{y(y-1)(y-(1-\lambda))}} = i\pi F\left(\frac{1}{2},\frac{1}{2},1,\lambda\right).\end{aligned} \tag{11.9}$$

The rest is clear. ■

We have shown the correspondence

$$\begin{aligned}\mathbb{C}/L &\xrightarrow{(\gamma,\gamma')} \mathrm{E}/\mathbb{C}(\mathbb{C}), \\ \mathrm{E}/\mathbb{C}(\mathbb{C}) &\xrightarrow{F\left(\frac{1}{2},\frac{1}{2},1,\lambda\right)} \mathbb{C}/L.\end{aligned}$$

Ex. 14. *Let us explicitly calculate the periods for* $\lambda = 1/2, -1, -2$. *Since for* $\lambda = 1/2, 1-\lambda = 1/2$, *we have* $\omega_1(1/2) = i\omega_2(1/2)$ *and the lattice is of the form* $\mathbb{Z}[i]\Omega = (\mathbb{Z}_i + \mathbb{Z})\Omega$. *To determine* Ω *for one of these curves (all isomorphic over* $\mathbb{C}$*), we calculate*

$$\begin{aligned}\omega_2(-1) = \Omega &= \int_0^1 \frac{\mathrm{d}\,t}{\sqrt{t(1-t^2)}} = \int_0^{\frac{\pi}{2}} \frac{\mathrm{d}\,\theta}{\sqrt{\sin\theta}} = \int_0^{\frac{\pi}{2}} \sin^{2\frac{1}{4}-1}\theta\cos^{2\frac{1}{2}-1}\theta\,\mathrm{d}\,\theta \\ &= \frac{\Gamma\left(\frac{1}{4}\right)\Gamma\left(\frac{1}{2}\right)}{\Gamma\left(\frac{3}{4}\right)}.\end{aligned} \tag{11.10}$$

Corollary 9. *The period lattice for the elliptic curve given by* $y^2 = x^3 - x$ *is* $\mathbb{Z}[i] : \Omega$, *where*

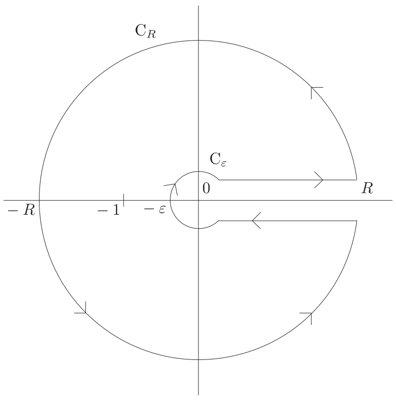
$$\Omega = \sqrt{\pi}\frac{\Gamma\left(\frac{1}{4}\right)}{\Gamma\left(\frac{3}{4}\right)}.$$

Ex. 15.

$$\Gamma(s)\Gamma(1-s) = \pi/\sin(\pi s) \quad \forall s \in \mathbb{C},\ 0 < \mathrm{Re}\,(s) < 1.$$

Proof:

$$\begin{aligned}
\Gamma(s)\Gamma(1-s) &= \int_0^\infty x^{s-1}e^{-x}\,\mathrm{d}\,x \int_0^\infty y^{-s}e^{-y}\,\mathrm{d}\,y = \begin{pmatrix} x & \longrightarrow & x^2=\tilde{x} \\ y & \longrightarrow & y^2=\tilde{y} \end{pmatrix} \\
&= \int_0^\infty 2\tilde{x}^{2s-1}e^{-\tilde{x}^2}\,\mathrm{d}\,\tilde{x} \int_0^\infty 2\tilde{y}^{-2s+1}e^{-\tilde{y}^2}\,\mathrm{d}\,\tilde{y} = \begin{pmatrix} (\tilde{x},\tilde{y}) & \longrightarrow & (r,\theta) \\ r^2 = x^2+y^2 & & \end{pmatrix} \\
&= \int_0^\infty \int_0^{\frac{\pi}{2}} 4e^{-r^2}(\cos\theta)^{2s-1}(\sin\theta)^{1-2s}\,r\,\mathrm{d}\,r\,\mathrm{d}\,\theta \\
&= 2\int_0^{\frac{\pi}{2}} (\tan\theta)^{1-2s}\,\mathrm{d}\,\theta \\
&= \int_0^\infty u^{-s}\frac{\mathrm{d}\,u}{1+u} \qquad \left(u=\tan^2\theta,\ \theta=\arctan\sqrt{u},\ \mathrm{d}\,\theta = \frac{1}{2}\frac{1}{1+u}\,\mathrm{d}\,u\right)
\end{aligned} \tag{11.11}$$



$$\begin{aligned}
\int_{C_R} \frac{u^{-s}}{1+u}\,\mathrm{d}\,u &\le c\frac{2\pi R}{R^{1+\mathrm{Re}((s))}} \xrightarrow{R\to\infty} 0, \\
\int_{C_\varepsilon} \frac{u^{-s}}{1+u}\,\mathrm{d}\,u &\le c'\frac{2\pi\varepsilon}{\varepsilon^s} = c' 2\pi\varepsilon^{1-\mathrm{Re}((s))} \xrightarrow{\varepsilon\to 0} 0.
\end{aligned} \tag{11.12}$$

the only pole is at $u=-1$:

$$\operatorname*{Res}_{\substack{u=-1\\ =e^{\pi i}}} \frac{u^{-s}}{1+u} = e^{-\pi i s}$$

$$\underbrace{\left(1-e^{-\pi i s}\right)\Gamma(s)\Gamma(1-s)}_{\int_{\leftrightarrows}} = 2\pi i \operatorname*{Res}_{u=-1}\left(\frac{u^{-s}}{1+u}\right) = 2\pi i e^{-\pi i s}$$

$$\Downarrow$$

$$\Gamma(s)\Gamma(1-s) = \frac{\pi}{\sin(\pi s)}. \tag{11.13}$$

■

Chapter 12

Gauss, Jacobi sums and their relation to ζ-functions

Let us return to affine part of elliptic curve $E_n/K : y^2 = x^3 - n^2x$, $n \neq \Box$, $n \in \mathbb{Z}_+$, where $\mathrm{char}\,(K) \nmid 2n$ and $K = \mathbb{F}_q$, $q = p^r$. The task is to determine the number of $\mathbb{F}_q$-points on E_n in terms of Jacobi sums.
We first transform the equation of E_n to a "diagonal form". We say that a hypersurface $f(x_1, \ldots, x_m) = 0$ in $\mathbb{A}^m/K$ is "diagonal" if each monomial in f involves at most one of the variables, and each variable occurs in at most one monomial. It turns out that diagonal hypersurfaces lend themselves to easy computation of the N_r (the number of $(x, y) \in \mathbb{F}_{p^r}$ solving E_n).
We first show a relation between points on $E_n : y^2 = x^3 - n^2x$ and points on the curve $E'_n : u^2 = v^4 + 4n^2$. As usual, suppose $p \nmid 2n$. Let $(u, v) \in E'_n$. Then the point $(x, y) := \big(\frac{1}{2}(u + v^2), \frac{1}{2}v(u + v^2)\big)$ is a point on E_n. Conversely, if (x, y) is on E_n and its x-coordinate is non-zero, then we check that the point $(u, v) := \big(2x - y^2/x^2, y/x\big)$ is on E'_n. Moreover, these two maps are inverse each other. We have bijection between points on E'_n and points on $E_n \setminus \{(0, 0)\}$ – if N' is the number of $\mathbb{F}_q$ solutions (u, v) to $u^2 = v^4 + 4n^2$, then $N_1 = \#E_n(\mathbb{F}_q) = N' + 2$. We are going to compute N' for diagonal curve $u^2 = v^4 + 4n^2$.
A multiplicative character on $\mathbb{F}_p$ is a map $\chi : \mathbb{F}_p^* \to \mathbb{C}^*$, fulfilling

$$\chi(a, b) = \chi(a)\chi(b) \quad \forall\, a, b \in \mathbb{F}_p^*. \tag{12.1}$$

An example is the Legendre (Jacobi) symbol $(\frac{-}{p}) : a \longrightarrow (\frac{a}{p})$. A second example is the trivial multiplicative character $\epsilon : a \to 1\,\forall a \in \mathbb{F}_p^*$. We extend any character by

$$\begin{aligned} &\chi(0) = 0, \quad \chi \neq \epsilon, \\ &\chi(0) = 1, \quad \chi = \epsilon. \end{aligned} \tag{12.2}$$

Lemma 9. *Let χ be a multiplicative character on $\mathbb{F}_p^*$. Then*

1/ $\chi(1) = 1$,

2/ $\chi(a)$ *is a root of unity of order* $p-1$,

3/ $\chi(a^{-1}) = \chi(a)^{-1} = \overline{\chi(a)}$.

Proof:

Trivial. ∎

Lemma 10. *Let* χ *be a multiplicative character. If* $\chi \neq \epsilon$*, then* $\sum_{a \in \mathbb{F}_p} \chi(a) = 0$*. If* $\chi = \epsilon$*, then* $\sum_{a \in \mathbb{F}_p} \chi(a) = p$*.*

Proof:

The assertion for $\chi = \epsilon$ is trivial, so let $\chi \neq \epsilon$. Then there is an element $a \in \mathbb{F}_p^* : \chi(a) \neq 1$. Let $T := \sum_b \chi(b)$, then

$$\chi(a)T = \sum_b \chi(a)\chi(b) = \sum_b \chi(ab) = T, \tag{12.3}$$

where we used the bijectivity of the map

$$\begin{aligned} \mathbb{F}_p^* &\longrightarrow \mathbb{F}_p^* \\ \forall a \in \mathbb{F}_p^* : b &\overset{a}{\longmapsto} ab. \end{aligned}$$

Because $\chi(a) \neq 1$, $\chi(a)T = T$ implies $T = 0$. ∎

Lemma 11. *The set of characters form a group:*

1/ If χ, λ *are two characters* $\chi\lambda : a \mapsto \chi(a)\lambda(a)\, \forall a \in \mathbb{F}_p^*$ *is a character.*

2/ If χ *is a character, then* χ^{-1} *is also a character:* $a \to \chi^{-1}(a) \equiv \chi(a)^{-1}$.

This group is cyclic of order $p-1$*. If* $a \in \mathbb{F}_p^*$ *and* $a \neq 1$*, then there is a character* $\chi : \chi(a) \neq 1$.

Proof:

1/ and 2/ are trivial. Let $g \in \mathbb{F}_p$ be a generator of the cyclic group $\mathbb{F}_p^*$. Then $\forall a \in \mathbb{F}_p^*$, $\exists l \in \mathbb{N} : a = g^l$. If $a = g^l$ and χ is character, $\chi(a) = \chi(g)^l$, in other words, χ is determined by its value on g. Because $\chi(g)$ is $(p-1)$-th root of unity and there are $(p-1)$ of them, the group of characters has order less or equal to $p-1$. Let us define a function $\lambda : \mathbb{F}_p^* \to \mathbb{C}^*$ by $\lambda(g^k) = \exp(2\pi i k/(p-1))$, $k \in \mathbb{N}$. Obviously, λ is character. We assert that $p-1$ is the least number $n \in \mathbb{N}$ satisfying $\lambda^n = \epsilon$. If $\lambda^n = \epsilon$, then $\lambda^n(g) = \epsilon(g) = 1$, so

$$1 = \lambda^n(g) = \lambda(g)^n = e^{\frac{2\pi i n}{p-1}} \Longrightarrow p-1 \mid n.$$

Clearly,

$$\lambda^{p-1}(a) = \lambda(a)^{p-1} = \lambda(a^{p-1}) = \lambda(1) = 1 \quad \forall a \in \mathbb{F}_p^*,$$

and so $\lambda^{p-1} = \epsilon$. The characters $\{\epsilon, \lambda, \lambda^2, \ldots, \lambda^{p-1}\}$ are pairwise distinct (because the roots of unit are). In the first part we proved that these are no more than $(p-1)$ characters, so there are exactly $(p-1)$ of them with λ a generator of this group.
If $a \in \mathbb{F}_p^*$, $a \neq 1$, then $a = g^l$, $p-1 \nmid l$. We have

$$\lambda(a) = \lambda(g)^l = e^{\frac{2\pi i l}{p-1}} \neq 1,$$

which completes the proof. ■

Lemma 12. *If $a \in \mathbb{F}_p^*$, $a \neq 1$, then $\sum_\chi \chi(a) = 0$ (the sum is over all characters).*

Proof:

Let $S = \sum_\chi \chi(a)$. Because $a \neq 1$ there is by lemma **??** a character λ for which $\lambda(a) \neq 1$. Then

$$\lambda(a)S = \sum_\chi \lambda(a)\chi(a) = \sum_\chi (\lambda\chi)(a) = S,$$

because if χ runs over all characters of $\mathbb{F}_p$, so does $\lambda\chi$. The equality $(\lambda(a)-1)S = 0$ implies $S = 0$. ■

Lemma 13. *If $a \in \mathbb{F}_p^*$, $n|p-1$ and $x^n = a$ is not solvable for some $x \in \mathbb{F}_p^*$, then there is a character χ, such that*

1/ $\chi^n = \epsilon$,

2/ $\chi(a) \neq 1$.

Proof:

Let g, λ be as above, and define $\chi = \lambda^{\frac{p-1}{n}}$. Then

$$\chi(g) = \lambda^{\frac{p-1}{n}}(g) = \lambda(g)^{\frac{p-1}{n}} = e^{\frac{2\pi i}{n}}.$$

Moreover $a = g^l$ for some $l \in \mathbb{N}$, and the non-existence of a solution $x^n = a$ implies $n \nmid l$. We have

$$\begin{aligned} \chi(a) &= \chi(g)^l = e^{\frac{2\pi i l}{n}} \neq 1, \\ \chi^n &= \lambda^{p-1} = \epsilon. \end{aligned} \tag{12.4}$$

■

Let us denote, for $a \in \mathbb{F}_p$, by $N(x^n = a)$ the number of solution of $x^n = a$. If $n \mid p-1$, we get

Lemma 14. *$N(x^n = a) = \sum\limits_{\chi^n=\epsilon} \chi(a)$, where the sum runs over all characters of order n.*

Proof:

There are n characters, whose order divides n. Because the value $\chi(g)$ must be a root of unity, there are at most n such characters. In the previous lemma **??** we have found χ, $\chi(g) = \exp(2\pi i/n)$. This implies that $\{\chi, \chi^2, \ldots, \chi^{n-1}\}$ is the set of n distinct characters.

1/ Let $a = 0$. Then there is only one solution of $x^n = 0$, namely $x = 0$. Moreover, $\sum_{\chi^n=\epsilon} \chi(0) = 1$ because $\epsilon(0) = 1$ and $\chi(0) = 0$ for $\chi \neq \epsilon$.

2/ Let $a \neq 0$ and there is a solution to $x^n = a$, i.e. $\exists b \in \mathbb{F}_p^* : b^n = a$. If $\chi^n = \epsilon$, then

$$\chi(a) = \chi(b^n) = \chi(b)^n = \chi^n(b) = \epsilon(b) = 1,$$

which gives $\sum_{\chi^n=\epsilon} \chi(a) = n$. This agrees with $N(x^n = a)$.

3/ Let $a \neq 0$ and $x^n = a$ doesn't have a solution. We show $\sum_{\chi^n=\epsilon} \chi(a) = 0$. Let us use the solution $T = \sum_{\chi^n=\epsilon} \chi(a)$. The previous lemma **??** shows the existence of a character $\mu : \mu(a) \neq 1, \mu^n = \epsilon$. We get

$$\mu(a)T = \mu(a) \sum_{\chi^n=\epsilon} \chi(a) = \sum_{\chi^n=\epsilon} (\mu\chi)(a) = T \Longrightarrow \Big(\mu(a) - 1\Big)T = 0 \Longrightarrow T = 0.$$

This completes the proof. ∎

Definition 24. *Let χ be a character of $\mathbb{F}_p$, $a \in \mathbb{F}_p$. We define the Gauss sum of $\mathbb{F}_p$, corresponding to χ, by*

$$g_a(\chi) = \sum_t \chi(t) e^{\frac{2\pi i a t}{p}}. \tag{12.5}$$

Lemma 15.

1/ $a \neq 0, \chi \neq \epsilon \Longrightarrow g_a(\chi) = \chi(a^{-1}) g_1(\chi),$

2/ $a \neq 0, \chi = \epsilon \Longrightarrow g_a(\epsilon) = 0,$

3/ $a = 0, \chi \neq \epsilon \Longrightarrow g_0(\chi) = 0,$

4/ $a = 0, \chi = \epsilon \Longrightarrow g_0(\epsilon) = p.$

Proof:

1/ $\chi(a)g_a(\chi) = \chi(a)\sum_t \chi(t)e^{\frac{2\pi iat}{p}} = \sum_t \chi(at)e^{\frac{2\pi iat}{p}} = g_1(t)$.

2/ $a \neq 0 \Longrightarrow g_a(\epsilon) = \sum_t \epsilon(t)e^{\frac{2\pi iat}{p}} = \sum_t e^{\frac{2\pi iat}{p}} = 0$.

3/,4/ $g_0(\chi) = \sum_t \chi(t)e^{\frac{2\pi i0t}{p}} = \sum_t \chi(t) = \begin{cases} p, \ \chi = \epsilon, \\ 0, \ \chi \neq \epsilon. \end{cases}$

■

Lemma 16. *Let $\chi \neq \epsilon$. Then $|g(\chi)| = \sqrt{p}$.*

Proof:

If $a \neq 0$, we have (lemma 15)

$$\overline{g_a(\chi)} = \overline{\chi(a^{-1})}\,\overline{g(\chi)} = \chi(a)\overline{g(\chi)},$$

and so

$$g_a(\chi)\overline{g_a(\chi)} = \chi(a^{-1})\chi(a)g(\chi)\overline{g(\chi)} = |g(\chi)|^2.$$

Then

$$\sum_a g_a(\chi)\overline{g_a(\chi)} = (p-1)|g(\chi)|^2.$$

On the other hand,

$$g_a(\chi)\overline{g_a(\chi)} = \sum_x \sum_y \chi(x)\overline{\chi(y)}e^{\frac{2\pi i(ax-ay)}{p}},$$

So

$$\begin{aligned} \sum_a g_a(\chi)\overline{g_a(\chi)} &= \sum_x \sum_y \chi(x)\overline{\chi(y)}e^{\frac{2\pi ia(x-y)}{p}} = \\ &= \sum_x \sum_y \chi(x)\overline{\chi(y)}p\delta_{x,y} = \sum_x \chi(x)\overline{\chi(x)}p = \\ &= (p-1)p. \end{aligned} \tag{12.6}$$

This gives the result. ■

The relation between $\overline{g(\chi)}$ and $g(\overline{\chi})$ follows from the comparison

$$\overline{g(\chi)} = \sum_t \overline{\chi(t)}e^{-\frac{2\pi it}{p}} = \overline{\chi(-1)}\sum_t \overline{\chi(-t)}e^{-\frac{2\pi it}{p}} = \chi(-1)g(\overline{\chi}),$$

where $\overline{\chi(-1)} = \chi(-1)$ because $\chi(-1) = \pm 1$. This means that the equality $|g(\chi)|^2 = p$ can be written as

$$g(\chi)g(\overline{\chi}) = \chi(-1)p.$$

Now let $N(x^m + y^n = 1)$ be the number of solutions of diagonal equation $x^m + y^n = 1$. We observe that it can be written as

$$N(x^m + y^n = 1) = \sum_{a+b=1} N(x^m = a)N(y^n = b),$$

where the sum is over $(a,b) \in \mathbb{F}_p^2$, $a+b=1$. For example, $N(x^2 = a) = 1 + \left(\frac{a}{p}\right)$ with Legendre symbol $\left(\frac{a}{p}\right) = \begin{cases} 0, a = 0 \\ 1, a = \square \\ -1, a \neq \square \end{cases}$. This is a motivation for

Definition 25. *Let χ, λ be some characters of $\mathbb{F}_p$. Then*

$$J(\chi, \lambda) = \sum_{a+b=1} \chi(a)\lambda(b)$$

is called Jacobi sum.

Lemma 17. *Let $\chi \neq \epsilon, \lambda \neq \epsilon$ be two nontrivial characters. Then*

1/ $J(\epsilon, \epsilon) = p$,

2/ $J(\epsilon, \chi) = 0$,

3/ $J(\chi, \chi^{-1}) = -\chi(-1)$,

4/ if $\chi\lambda \neq \epsilon$, *then* $J(\chi, \lambda) = \frac{g(\chi)g(\lambda)}{g(\chi\lambda)}$,

5/ if $\chi \neq \epsilon, \lambda \neq \epsilon, \chi\lambda \neq \epsilon$, *then* $|J(\chi, \lambda)| = \sqrt{p}$.

Proof:

1/,2/ trivial

3/

$$J(\chi, \chi^{-1}) = \sum_{a+b=1} \chi(a)\chi^{-1}(b) = \sum_{\substack{a+b=1 \\ b\neq 0}} \chi\left(\frac{a}{b}\right) = \sum_{a\neq 1} \chi\left(\frac{a}{1-a}\right).$$

Let $c := \frac{a}{1-a}$. If $c \neq 1$, then $a = \frac{c}{1+c}$. It follows if a runs over $\mathbb{F}_p \setminus \{1\}$ then c runs over the set $\mathbb{F}_p \setminus \{-1\}$. Then

$$J(\chi, \chi^{-1}) = \sum_{c\neq -1} \chi(c) = -\chi(-1).$$

4/

$$\begin{aligned} g(\chi)g(\lambda) &= \left(\sum_x \chi(x)e^{\frac{2\pi i x}{p}}\right)\left(\sum_y \lambda(y)e^{\frac{2\pi i y}{p}}\right) = \\ &= \sum_{x,y} \chi(x)\lambda(y)e^{\frac{2\pi i(x+y)}{p}} = \sum_t \left(\sum_{x+y=t} \chi(x)\lambda(y)\right) e^{\frac{2\pi i t}{p}}. \end{aligned} \tag{12.7}$$

For $t = 0$, we get

$$\sum_{x+y=0} \chi(x)\lambda(y) = \sum_x \chi(x)\lambda(-x) = \lambda(-1)\sum_x (\chi\lambda)(x) = 0$$

provided $(\chi\lambda)$ is non-trivial character.
For $t \neq 0$, let $x = tx', y = ty'$, i.e. $x + y = t \Longrightarrow x' + y' = 1$, and so

$$\sum_{x+y=t} \chi(x)\lambda(y) = \sum_{x'+y'=t} \chi(tx')\lambda(ty') = (\chi\lambda)(t)J(\chi, \lambda).$$

The substitution into **??** leads to

$$g(\chi)g(\lambda) = \sum_t (\chi\lambda)(t)J(\chi, \lambda)e^{\frac{2\pi i t}{p}} = J(\chi, \lambda)\sum_t (\chi\lambda)(t)e^{\frac{2\pi i t}{p}} =$$
$$= J(\chi, \lambda)g(\chi\lambda).$$

5/ We have $|g(\chi)|^2 = p$, $|g(\lambda)|^2 = p$, $|g(\chi\lambda)|^2 = p$. Now 4/ implies the result.

■

Ex. 16. *Let us investigate $N(x^2 + y^2 = 1)$, $N(x^3 + y^3 = 1)$.*

1/

$$N(x^2 + y^2 = 1) = \sum_{a+b=1} N(x^2 = a)N(y^2 = b),$$

where $N(x^2 = a) = 1 + \chi(a)$, where $\chi(a) = \frac{a}{p}$, the Legendre symbol. Then

$$N(x^2 + y^2 = 1) = p + \sum_a \left(\frac{a}{p}\right) + \sum_b \left(\frac{b}{p}\right) + \sum_{a+b=1} \left(\frac{a}{p}\right)\left(\frac{b}{p}\right).$$

*The second and third sum is trivial, lemma **??**, the last is equal to ($\chi : \mathbb{F}_p^* \to \{\pm 1\}$).*

$$\sum_{a+b=1} \left(\frac{a}{p}\right)\left(\frac{b}{p}\right) = \sum_{a+b=1} \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)^{-1} = \sum_{a+b=1} \chi(a)\chi^{-1}(b)$$
$$= J(\chi, \chi^{-1}) = -\chi(-1) \quad (12.8)$$

*by lemma **??**. It is well known that $\chi(-1/p) = (-1)^{\frac{p-1}{2}}$, so finally*

$$N(x^2 + y^2 = 1) = p - 1, \quad p = 1\, mod 4, \quad (12.9)$$
$$N(x^2 + y^2 = 1) = p + 1, \quad p = 3\, mod 4. \quad (12.10)$$

2/ $N(x^3+y^3=1) = \sum_{a+b=1} N(x^3=1)N(y^3=b)$. *Let* χ *be a nontrivial character of order 3, i.e.* $\{\epsilon, \chi, \chi^3\}$ *are all characters of order 3 (so called cubic characters). Then*

$$N(x^3=a) = 1+\chi(a)+\chi^2(a),$$

and so

$$N(x^3+y^3=1) = \sum_{a+b=1}\sum_{i=0}^{2}\chi^i(a)\sum_{j=0}^{2}\chi^j(b) = \sum_{i,j}\left(\sum_{a+b=1}\chi^i(a)\chi^j(b)\right)$$
$$= \sum_{i,j}^{2} J(\chi^i,\chi^j). \tag{12.11}$$

The lemma **??** *then implies*

$$N(x^3+y^3=1) = p-\chi(-1)-\chi^2(-1)+J(\chi,\chi)+J(\chi^2,\chi^2).$$

Because $-1=(-1)^3$, *we get* $\chi(-1)=\chi((-1)^3)=\chi^3(-1)=1$. *Also* $\chi^2=\chi^{-1}=\overline{\chi}$, *which yields*

$$N(x^3+y^3=1) = p-2+2Re\, J(\chi,\chi).$$

Of course, we don't know explicit formula for $J(\chi,\chi)$. *But lemma* **??** *allows to conclude* $\left(|J(\chi,\chi)|=\sqrt{p}\right)$

$$\left|N(x^3+y^3=1)-p+2\right| \le 2\sqrt{p}.$$

In other words, for $p \gg 1$ *there are many solutions in* $\mathbb{F}_p$ *of the equation* $x^3+y^3=1$.

Generally, let us investigate the number of solutions to $x^n+y^n=1$ in $\mathbb{F}_p$. We have

$$N(x^n+y^n=1) = \sum_{a+b=1} N(x^n=a)N(y^n=b).$$

Let χ be a character of order n. Then

$$N(x^n=a) = \sum_{i=0}^{n-1}\chi^i(a).$$

Up to now, we determined Gauss and Jacobi sums over the field $\mathbb{F}_p$. The question is the relation between the corresponding objects for a finite extension of $\mathbb{F}_p$, say $\mathbb{F}_q=\mathbb{F}_{p^n}$.

Definition 26. *The map*

$$\begin{array}{cccc} Tr: & \mathbb{F}_q & \longrightarrow & \mathbb{F}_p, \\ & \cup & & \\ & \alpha & \longrightarrow & \alpha+\alpha^p+\alpha^{p^2}+\ldots+\alpha^{p^{n-1}}. \end{array}$$

Lemma 18. *Let $\alpha, \beta \in \mathbb{F}_q$, $a \in \mathbb{F}_p$. Then*

1/ $Tr(\alpha) \in \mathbb{F}_p$,

2/ $Tr(\alpha+\beta) = Tr(\alpha) + Tr(\beta)$,

3/ $Tr(a\alpha) = a\,Tr(\alpha)$,

3/ Tr is surjective map.

Proof:

1/
$$\left(\alpha + \alpha^p + \ldots + \alpha^{p^n-1}\right)^p = \alpha^p + \alpha^{p^2} + \ldots + \alpha^{p^{n-1}} + \alpha^{p^n}.$$

Because $\alpha^{p^n} = \alpha^q = \alpha$, we have $(\mathrm{Tr}\,(\alpha))^p = \mathrm{Tr}\,(\alpha)$ and 1/ follows.

2/
$$\begin{aligned}\mathrm{Tr}\,(\alpha+\beta) &= (\alpha+\beta) + (\alpha+\beta)^p + \ldots + (\alpha+\beta)^{p^n-1} = \\ &= (\alpha+\beta) + (\alpha^p+\beta^p) + \ldots + (\alpha^{p^n-1} + \beta^{p^n-1}) = \\ &= \left(\alpha + \alpha^p + \ldots + \alpha^{p^n-1}\right) + \left(\beta + \beta^p + \ldots + \beta^{p^n-1}\right) = \\ &= \mathrm{Tr}\,(\alpha) + \mathrm{Tr}\,(\beta)\,. \end{aligned} \tag{12.12}$$

3/
$$\begin{aligned}\mathrm{Tr}\,(a\alpha) &= a\alpha + a^p\alpha^p + \ldots + a^{p^n-1}\alpha^{p^n-1} = \\ &= a\left(\alpha + \alpha^p + \ldots + \alpha^{p^n-1}\right) = \\ &= a\,\mathrm{Tr}\,(\alpha)\,, \end{aligned} \tag{12.13}$$

where we used $a^p = a \quad \forall a \in \mathbb{F}_p$.

4/ The polynomial $x + x^p + \ldots + x^{p^{n-1}}$ has at most p^{n-1} roots in $\mathbb{F}$. Because $\mathbb{F}$ has $p^n\,(> p^{n-1})$ elements, there is an element $\alpha \in \mathbb{F}_p$: $\mathrm{Tr}\,(\alpha) = c \neq 0$. If $b \in \mathbb{F}_p$, it follows from 3/ that

$$\mathrm{Tr}\left(\frac{b}{c}\alpha\right) = \frac{b}{c}\,\mathrm{Tr}\,(\alpha) = b,$$

i.e. Tr is a surjective map.

■

Definition 27. *The map*

$$\begin{aligned} \psi : \mathbb{F}_q &\longrightarrow \mathbb{C}, \\ \alpha \in \mathbb{F}_q &\longrightarrow e^{\frac{2\pi i Tr(a)}{p}} \\ 0 &\longrightarrow 1 \end{aligned} \tag{12.14}$$

is called additive character on $\mathbb{F}_q$.

Now we can define Gauss and Jacobi sums on $\mathbb{F}_q$ in the same way, as for $\mathbb{F}_p$. For example

Definition 28. *Let* χ *be a character on* $\mathbb{F}_q$, *i.e.* $\chi : \mathbb{F}_q \to \mathbb{C}$. *Then*

$$g_\alpha(\chi) := \sum_{t \in \mathbb{F}_q} \chi(t)\psi(\alpha t),\ \alpha \in \mathbb{F}_q^*,$$

is called Gauss sum on $\mathbb{F}_q$, *corresponding to the multiplicative character* χ.

Let us return back to $E_n/\mathbb{F}_q$ and its diagonal form. We arrived at the problem to compute ($q = 1 \bmod 4$)

$$\begin{aligned} N' = &\#\{u \in \mathbb{F}_q \mid u^2 = 4n^2\} + \#\{v \in \mathbb{F}_q \ \mid\ o = v^4 + 4n^2\} + \\ &+ \#\{(u,v) \in \left(\mathbb{F}_q^*\right)^2 \mid u^2 = v^4 + 4n^2\}. \end{aligned} \tag{12.15}$$

Let us denote by χ_i a character of order i. Then it is easy to check

$$N' = q - 1 + \chi_4(-4n^2)\Big(J(\chi_2, \chi_4) + J(\chi_2, \overline{\chi_4})\Big),$$

from which it follows

$$N_1 = \#E_n/\mathbb{F}_q = q + 1 - \alpha - \overline{\alpha}, \quad \alpha = -\chi_2(n)J(\chi_2, \chi_4).$$

Note that α is an algebraic integer in $Q(i)$, since the values of χ_4 in the definition of $J(\chi_2, \chi_4)$ are all $\pm 1, \pm i$.

It is easy to rewrite $\alpha = -\chi_2(n)J(\chi_2, \chi_4)$ to the form

$$\alpha = -\frac{\chi_2(n)g(\chi_2)g(\chi_4)}{g(\overline{\chi_4})}$$

and to check

$$|\alpha|^2 = \alpha\overline{\alpha} = \frac{\chi_2(n)\overline{\chi_2(n)}g(\chi_2)\overline{g(\chi_2)}g(\chi_4)\overline{g(\chi_4)}}{g(\overline{\chi_4})\overline{g(\overline{\chi_4})}} = q.$$

The last relation $|\alpha| = q^{1/2}$ says that the coefficients $L-$polynomial $L(T) = (1 - \alpha T)(1 - \overline{\alpha}T)$ of the zeta function

$$Z(E_n/\mathbb{F}_q, T) = \frac{(1 - \alpha T)(1 - \overline{\alpha}T)}{(1 - T)(1 - pT)}$$

of the elliptic curve $y^3 = x^3 - n^2x$, can be expressed through Gauss and Jacobi sums and multiplicative characters on $\mathbb{F}_q$, i.e. using only tools of harmonic analysis on a finite group!

Chapter 13

Elliptic curves over finite fields

We have discussed many properties of elliptic curves over perfect field in the course on Algebraic geometry in positive characteristic. For a *finite base field* K, $char(K) = p$ ($q = p^n$ for some $n \in \mathbb{Z}$), the results can be proved using more simple methods.

Let E/K be an elliptic curve over K. The aim is to estimate $E(K) := E/K(K)$, i.e. the number $\#E(K)$ of K–rational points on E/K:

$$(x, y) \in K^2 : \; y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 \,. \tag{13.1}$$

A trivial upper bound on $\#E(K)$ is $2q + 1$. In fact, Hasse was able to prove the following conjecture of Artiu:

Theorem 21. *Let E/K be an elliptic curve, $\#K = q = p^n$. Then*

$$|\#E(K) - q - 1| \leq 2\sqrt{q} \,. \tag{13.2}$$

Proof: Let E/K be an elliptic curve written in Weierstrass form, and let

$$\begin{aligned} \varphi : \; E &\longrightarrow E \\ (x, y) &\longrightarrow (x^q, y^q) \end{aligned} \tag{13.3}$$

be the q–th power of arithmetic Frobenious automorphism of $\bar{K}/K$. Since $Gal(\bar{K}/K)$ is, as topological group, generated by $(\varphi : \bar{K} \to \bar{K})$, we have

$$P \in E(\bar{K}) : \; P \in E(K) \Longleftrightarrow \varphi(P) = P \,. \tag{13.4}$$

Thus $E(K) = Ker(1 - \varphi)$, so

$$\#E(K) = \#Ker(1 - \varphi) = deg(1 - \varphi) \,, \tag{13.5}$$

where we used the separability of the map $1-\varphi$ Eq(⇈???). Since the degree map $deg : End(E) \to \mathbb{Z}$ is positive definite quadratic form and $deg(\varphi) = q$, the result follows from Lemma(19) for

$$A = End(E), \quad Q = deg\,. \tag{13.6}$$

■

Lemma 19. *Let A be an abelian group and $Q : A \to \mathbb{Z}$ a positive definitive quadratic form. Then for all $a_1, a_2 \in A$:*

$$|Q(a_1 - a_2) - Q(a_1) - Q(a_2)| \leq 2\sqrt{Q(a_1)Q(a_2)}\,. \tag{13.7}$$

Proof: For $a_1, a_2 \in A$, let us define

$$B(a_1, a_2) = Q(a_1 - a_2) - Q(a_1) - Q(a_2)\,. \tag{13.8}$$

By definition of the quadratic form Q, B is bilinear:

$$B(\lambda a_1, a_2) = \lambda B(a_1, a_2) = B(a_1, \lambda a_2) \quad \forall \lambda \in \mathbb{Z}\,. \tag{13.9}$$

Because Q is positive definitive,

$$0 \leq Q(ma_1 - na_2) = m^2 Q(a_1) + mnB(a_1, a_2) + n^2 Q(a_2) \quad \forall m, n \in \mathbb{Z}\,. \tag{13.10}$$

In particular for $m = -B(a_1, a_2),\ n = 2Q(a_1)$, Eq(13.10) yields

$$\begin{aligned} 0 \ \leq\ & B^2(a_1, a_2)Q(a_1) - 2B(a_1, a_2)Q(a_1)B(a_1, a_2) + 4Q^2(a_1)Q(a_2) \\ =\ & Q(a_1)[-B^2(a_1, a_2) + 4Q(a_1)Q(a_2)]\,. \end{aligned} \tag{13.11}$$

This is desired result for $a_1 \neq 0$. Note that for $a_1 = 0$ the original inequality is trivial. ■

Let $K = \mathbb{F}_q$ with q odd. We use Hasse's Theorem (21) to estimate the value of certain character sums on K. Let

$$f(x) = ax^3 + bx^2 + cx + d \in K[x] \tag{13.12}$$

be a cubic polynomial with distinct roots in $\bar{K}$, and let

$$\chi :\ K^* \longrightarrow \mathbb{Z}_2 \tag{13.13}$$

be the unique non–trivial character of order two, i.e. $\chi(k) = 1$ iff $k = (k')^2$ for some $k' \in K^*$. We extend χ to K by $\chi(0) = 0$. We use χ to count the k–rational points on the elliptic curve

$$E :\ y^2 = f(x)\,. \tag{13.14}$$

Each $x \in K$ will yield 0 resp. 1 resp. 2 point(s) $(x, y) \in E(K)$ if f(x) is non–square resp. zero resp. non zero square in K. Thus (adding the point in infinity)

$$\#E(K) = 1 + \sum_{x \in K} (\chi(f(x)) + 1) = 1 + q + \sum_{x \in K} \chi(f(x))\,. \tag{13.15}$$

Corollary 10. *With notation as above,*

$$\left|\sum_{x\in K} \chi(f(x))\right| \leq 2\sqrt{q}\,. \tag{13.16}$$

The proof follows from Theorem 21. Notice that the sum consists of q terms, each being ± 1. The Corollary 10 says that as x runs through K, the values of cubic polynomial f tend to be equally distributed between squares and non-squares.

13.1 Weil conjectures

Let K be a field with q elements and for each $n \in \mathbb{N}_+$, let K_n be an extension of K of degree n, $dim_K K_n = n$. In other words $\#K_n = q^n$. Let V/K be a projective variety, i.e. V is the set of zeros of finitely many homogeneous polynomials

$$f_1(x_0,\ldots,x_N) = \cdots = f_m(x_0,\ldots,x_N) = 0\,. \tag{13.17}$$

defined over K. Let $V(K_n)$ be the set of points of V with coordinates in K_n. Let us encode the numbers $V(K_n),\ n\in\mathbb{N}$, in suitable generating series.

Definition 29. *The zeta function of V/K is the (formal) power series*

$$Z(V/K,t) := exp\left(\sum_{n=1}^{\infty} (\#V(K_n))\,\frac{t^n}{n}\right)\,. \tag{13.18}$$

Once we know $Z(V/k,t)\in\mathbb{Q}\,[t]$, we recover $\#V(K_n)$ by formula

$$\#V(K_n) = \frac{1}{(n-1)!}\frac{d^n}{dt^n}\log Z(V/K,t)\Big|_{t=0}\,. \tag{13.19}$$

Ex. 17. *Let $V=\mathbb{P}^N$. Then a point of $V=(K_n)$ is given by homogeneous coordinates $[x_0,\ldots,x_N]$ with all $x_i,\ i=1,\ldots,N$ not zero. Two multiples $[x_0,\ldots,x_N],[x'_0,\ldots,x'_N]$ are equivalent iff $\exists\lambda\in K_n^*$, such that $[x_n,\ldots,x_N] = [\lambda x'_0,\ldots,\lambda x'_N]$. Hence*

$$\#V(K_n) = \sum_{i=0}^{N} q^{ni} = \frac{q^{n(N+1)}-1}{q^n-1}\,, \tag{13.20}$$

so

$$\log Z(V/K,t) = \sum_{n=1}^{\infty}\left(\sum_{i=0}^{N} q^{ni}\right)\frac{t^n}{n} = -\sum_{i=0}^{N}\log\left(1-q^i t\right)\,. \tag{13.21}$$

Thus

$$Z\left(\mathbb{P}^N/K,t\right) = \frac{1}{(1-t)(1-qt)\cdots(1-qNt)}\,. \tag{13.22}$$

In this case $Z\left(\mathbb{P}^N/K,t\right)\in\mathbb{Q}(T)$ obviously.

Theorem 22. *(Weil conjectures) Let K be a field with q–elements and V/K a smooth projective variety, $dim_K V = n$.*

(1) Rationality
$$Z\,(V/K,t) \in \mathbb{Q}(t)\,. \tag{13.23}$$

(2) Functional equation
There is an integer ϵ (Euler characteristic of $V(\mathbb{C})$) so that
$$Z\left(V/K, \frac{1}{q^n t}\right) = \pm q^{\frac{n\epsilon}{2}} t^{\epsilon} Z\,(V/K,t)\;. \tag{13.24}$$

(3) Riemann hypothesis
There is a factorization
$$Z\,(V/K,t) = \frac{P_1(t)P_3(t)\ldots P_{2n-1}(t)}{P_0(t)P_2(t)\ldots P_{2n}(t)} \tag{13.25}$$
with each $P_i(t) \in \mathbb{Z}[t]$. Further $P_0(t) = 1-t$, $P_{2n}(t) = 1-q^n t$, and for each $1 \le i \le 2n-1$, $P_i(t)$ factors over $\mathbb{C}$ as
$$P_i(t) = \prod_j (1-\alpha_{ij}t), \quad |\alpha_{ij}| = q^{i/2} \quad \forall i,j\,. \tag{13.26}$$

Proof: The large part Theorem has been proved on the course of algebraic geometry.

■

This Theorem takes a special form for elliptic curves.

Corollary 11. *Let K be a finite field with q–elements and E/K an elliptic curve. Then there is an $a \in \mathbb{Z}$ so that*
$$Z\,(E/K,T) = \frac{1-aT+qT^2}{(1-T)(1-qT)}\,. \tag{13.27}$$

Further
$$Z\left(E/K, \frac{1}{qT}\right) = Z\,(E/K,T) \quad \textit{(functional equation)}\,, \tag{13.28}$$

and
$$1-aT+qT^2 = (1-\alpha T)(1-\beta T), \quad |\alpha| = |\beta| = q^{1/2}\,. \tag{13.29}$$

Chapter 14

Elliptic Functions

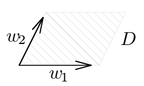
Let $\Lambda \in \mathbb{C}$ be a lattice, i.e. a discrete abelian subgroup $\Lambda \subset \mathbb{C} : \Lambda \underset{\mathbb{Z}}{\otimes} \mathbb{R} \xrightarrow{\sim} \mathbb{C}$ (as $\mathbb{R}$-mod). We shall study meromorphic functions on $\mathbb{C}/\Lambda$.

Definition 30. *An elliptic function (relative to the lattice $\Lambda \subset \mathbb{C}$) is a meromorphic function $f : \mathbb{C} \to \mathbb{C}$ satisfying $f(\omega + z) = f(z)\ \forall \omega \in \Lambda,\ z \in \mathbb{C}$.*

The set of all elliptic functions, denoted $\mathbb{C}(\Lambda)$, is a field.

Definition 31. *A fundamental parallelogram for Λ is the set*

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



where $a \in \mathbb{C}$, ω_1, ω_2 is a basis of Λ. We have the bijection $D \xrightarrow{\sim} \mathbb{C}/\Lambda$ of sets. The closure of D in $\mathbb{C}$ will be denoted $\overline{D}$.

Theorem 23. *An elliptic function with no poles is constant. An elliptic function with no zeros is constant.*

Proof: Suppose $f(z) \in \mathbb{C}(\Lambda)$ is holomorphic. Then the periodicity condition gives $\sup_{z\in\mathbb{C}} |f(z)| = \sup_{z\in\overline{D}} |f(z)|$. Because f is continuous on $\mathbb{C}$ and $\overline{D}$ is compact, so $|f(z)|$ is bounded on $\overline{D}\ \Rightarrow\ |f(z)|$ is bounded on $\mathbb{C}$. Then the Liouville theorem implies f is constant map.
In the second case (f has no zeros), use the previous procedure for $\frac{1}{f}$. ■

Let f be an elliptic function, let $w \in \mathbb{C}$. Then we define

- $\operatorname{ord}_w(f)$:= the order of vanishing of f at w, and

- $\operatorname{res}_w(f)$:= the residue of f at w (i.e. a_{-1} of the Laurent expansion of f).

Since f is elliptic, both $\operatorname{ord}_w(f)$ and $\operatorname{res}_w(f)$ remain the same if w is replaced by $w+\omega$ $\forall\omega\in\Lambda$.

Convention: By $\sum_{w\in\mathbb{C}/\Lambda}$ we understand $\sum_{w\in D}$, D being a fundamental parallelogram for Λ (the resulting sum is independent of the choice of D). Because we study meromorphic functions, the sum $\sum_{w\in D}$ always reduces to the finite sum, i.e. there is no problem with its convergence in next theorem.

Theorem 24. *Let $f\in\mathbb{C}(\Lambda)$. Then*

1. $\displaystyle\sum_{w\in\mathbb{C}/\Lambda}\operatorname{res}_w(f)=0$

2. $\displaystyle\sum_{w\in\mathbb{C}/\Lambda}\operatorname{ord}_w(f)=0$

3. $\displaystyle\sum_{w\in\mathbb{C}/\Lambda}\operatorname{ord}_w(f)w\in\Lambda$

Proof: Let D be a fundamental parallelogram for Λ, such that $f(z)$ has no poles and zeros on the boundary ∂D of D. The proofs are based on application of the residue theorem.

1. $\sum_{w\in\mathbb{C}/\Lambda}\operatorname{res}_w(f)=\frac{1}{2\pi i}\int_{\partial D}f(z)\mathrm{d}z$ and so the periodicity of f implies $\int_{\partial D}f(z)\mathrm{d}z=0$, i.e. $\sum_{w\in\mathbb{C}/\Lambda}\operatorname{res}_w(f)=0$.

2. The periodicity of $f(z)$ implies the periodicity of $f'(z)$ $\big($Note $f'(z):=\lim\limits_{\epsilon\to0}\frac{f(z+\epsilon)-f(z)}{\epsilon}$, i.e. $f'(z+\omega):=\lim\limits_{\epsilon\to0}\frac{f(z+\omega+\epsilon)-f(z+\omega)}{\epsilon}=\lim\limits_{\epsilon\to0}\frac{f(z+\epsilon)-f(z)}{\epsilon}=f'(z)\big)$, so the application of 1. to elliptic function $\frac{f'(z)}{f(z)}$ gives $\sum_{w\in\mathbb{C}/\Lambda}\operatorname{ord}_w(f)=\sum_{w\in\mathbb{C}/\Lambda}\operatorname{res}_w(\frac{f'}{f}(w))=\frac{1}{2\pi i}\int_{\partial D}\frac{f'(z)}{f(z)}\mathrm{d}z=\int_{\partial D}\mathrm{d}\log(f(z))=0$.
   Note that we used
   $$\left.\begin{array}{l} f(z)=c_m(z-a)^m+\cdots \\ f'(z)=m\,c_m(z-a)^{m-1}+\cdots \end{array}\right\}\frac{f'(z)}{f(z)}=m(z-a)^{-1}+O(1).$$

3. We use the residue theorem for the function $\frac{zf'(z)}{f(z)}$:

   - The Laurent expansion of $\frac{f'(z)}{f(z)}$ near a zero of f at a of order m : $\left.\frac{f'}{f}\right|_a(z)=\frac{m}{z-a}+O(1)$,

   - The Laurent expansion of $\frac{f'(z)}{f(z)}$ near a pole of f at a of order m : $\left.\frac{f'}{f}\right|_a(z)=-\frac{m}{z-a}+O(1)$.

Writing $z = a + (z-a)$, we get the Laurent expansion around $a \in \mathbb{C}$: $z\frac{f'}{f}(z) = \frac{am}{z-a} + O(1)$, and the residue theorem gives

$$\begin{aligned}\sum_{w \in \mathbb{C}/\Lambda} \operatorname{ord}_w(f)w &= \frac{1}{2\pi i}\int_{\partial \overline{D}} z\frac{f'}{f}(z)\mathrm{d}z \\ &= \frac{1}{2\pi i}\left(\int_{\alpha}^{\alpha+\omega_1} + \int_{\alpha+\omega_1}^{\alpha+\omega_1+\omega_2} + \int_{\alpha+\omega_1+\omega_2}^{\alpha+\omega_2} + \int_{\alpha+\omega_2}^{\alpha}\right) z\frac{f'}{f}(z)\mathrm{d}z.\end{aligned}$$

Changing the variable $z \mapsto z - \omega_1$ (resp. $z \mapsto z - \omega_2$) in the second (resp. third) integral and using the periodicity of $\frac{f'}{f}(z)$, we get

$$\sum_{w \in \mathbb{C}/\Lambda} \operatorname{ord}_w(f)w = -\frac{\omega_2}{2\pi i}\int_{\alpha}^{\alpha+\omega_1} \frac{f'}{f}(z)\mathrm{d}z + \frac{\omega_1}{2\pi i}\int_{\alpha}^{\alpha+\omega_2} \frac{f'}{f}(z)\mathrm{d}z$$

The change of variables $z \mapsto u = f(z)$ gives $\frac{f'(z)}{f(z)}\mathrm{d}z = \frac{\mathrm{d}u}{u}$. Let C_1 be the closed path from $f(\alpha)$ to $f(\alpha+\omega_1) = f(\alpha)$ traced by $u = f(z)$ as z goes from α to $\alpha+\omega_1$. Then $\int_{\alpha}^{\alpha+\omega_1} \frac{f'}{f}(z)\mathrm{d}z = \int_{C_1} \frac{\mathrm{d}u}{u} \in 2\pi i\mathbb{Z}$, which proves the theorem. ■

Definition 32. *The order of an elliptic function is its number of poles (counted with multiplicity) in any fundamental parallelogram. Note that the number of poles is equal to the number of zeros.*

Lemma 20. *A non-constant elliptic function has order at least* 2.

Proof: If $f(z)$ would have a single simple pole, then from 1. of the Theorem 24 it follows that the residue at that point is zero, so $f(z)$ is holomorphic and so it is a constant function. ■

Define a divisor group $\operatorname{Div}(\mathbb{C}/\Lambda)$ to be the group of formal linear combinations $\sum_{w \in \mathbb{C}/\Lambda} n_w(w)$, $n_w \in \mathbb{Z}$ and $n_w = 0$ for all but finitely many $w \in \mathbb{C}/\Lambda$. For $D = \sum n_w(w) \in \operatorname{Div}(\mathbb{C}/\Lambda)$, we define

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

The divisors of degree zero,

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

form a subgroup of $\operatorname{Div}(\mathbb{C}/\Lambda)$.
Let $f \in \mathbb{C}(\Lambda)^*$. Then the principal divisor $f \mapsto \operatorname{Div}(f) \in \operatorname{Div}^0(\mathbb{C}/\Lambda)$ is defined by

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

The map $\mathrm{Div}\ : \mathbb{C}(\Lambda)^* \mapsto \mathrm{Div}^{\,0}(\mathbb{C}/\Lambda)$ is an injective homomorphism ($\forall\, w$ is $\mathrm{ord}_{\,w}$ a valuation). We also define

$$\begin{aligned} \sum : \mathrm{Div}^{\,0}(\mathbb{C}/\Lambda) \quad &\longrightarrow \quad \mathbb{C}/\Lambda \\ \sum n_w(w) \quad &\longrightarrow \quad \sum n_w w \bmod \Lambda. \end{aligned}$$

Theorem 25. *The sequence*

$$1 \longrightarrow \mathbb{C}^* \longrightarrow \mathbb{C}(\Lambda)^* \xrightarrow{\mathrm{Div}} \mathrm{Div}^{\,0}(\mathbb{C}/\Lambda) \xrightarrow{\Sigma} \mathbb{C}/\Lambda \longrightarrow 0$$

is exact.

Proof: The fact that it is a complex easily follows from 1., 2., 3., of the previous Theorem 24. The exactness follows from Lemma 22 ■

Chapter 15

Explicit Construction of Elliptic Functions

We know that any non-constant elliptic function has order at least two.

Definition 33. *Let $\Lambda \subset \mathbb{C}$ be a lattice. The Weierstrass $\mathcal{P}$-function, relative to the lattice Λ, is defined by the series*

$$\mathcal{P}(z, \Lambda) = \frac{1}{z^2} + \sum_{\substack{\omega \in \Lambda \\ \omega \neq 0}} \left(\frac{1}{(z-\omega)^2} - \frac{1}{\omega^2} \right).$$

The Eisenstein series of weight $2k$ (for Λ) is the series

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

Theorem 26. *Let $\Lambda \subset \mathbb{C}$ be a lattice.*

1. *The Eisenstein series G_{2k} for $\Lambda \subset \mathbb{C}$ is absolutely convergent for all $k > 1$.*
2. *The power series defining Weierstrass function converges absolutely and uniformly on every compact subset of $\mathbb{C} \setminus \Lambda$. It defines a meromorphic function on $\mathbb{C}$ with a double pole with residue 0 at each lattice point and no other poles.*
3. *The Weierstrass $\mathcal{P}$-function is an even elliptic function.*

Proof:

1. Since $\Lambda \subset \mathbb{C}$ is discrete and it is a lattice, there is a constant $C(\Lambda)$ such that $\forall N \in \mathbb{N}$ the number of lattice points in an annulus satisfies

$$\#\{\omega \in \Lambda : N \leq |\omega| < N+1\} < C(\Lambda)N.$$

Then
$\sum_{\substack{\omega\in\Lambda\\ \omega\neq 0}} \frac{1}{|\omega|^{2k}} = \sum_{\substack{\omega\in\Lambda\\ |\omega|\geq 1}} \frac{1}{|\omega|^{2k}} + C'(\Lambda) \leq \sum_{N=1}^{\infty} \frac{\#\{\omega\in\Lambda:\ N\leq|\omega|<N+1\}}{N^{2k}} + C'(\Lambda) < \sum_{N=1}^{\infty} \frac{C(\Lambda)}{N^{2k-1}} + C'(\Lambda) < \infty$

for $C'(\Lambda)$ a finite constant and $k \geq 1$.

2. Let $|\omega| > 2|z|$. Then

$$\left|\frac{1}{(z-\omega)^2} - \frac{1}{\omega^2}\right| = \left|\frac{z(2\omega - z)}{\omega^2(z-\omega)^2}\right| \leq \frac{4|z||2\omega - z|}{|\omega|^4} \leq \frac{10|z|}{|\omega|^3},$$

because $|\omega - z| > |\frac{\omega}{2}| = \frac{1}{2}|\omega|$, $|2\omega - z| \leq |2\omega| + |z| \leq 2|\omega| + \frac{1}{2}|\omega| = \frac{5}{2}|\omega|$. Let us choose $R \in \mathbb{R}_+$. Then for $z \in U(0,R) \smallsetminus \Lambda$

$$\sum_{\substack{\omega\in\Lambda\\ \omega\neq 0}} = \sum_{|\omega|\leq 2R} + \sum_{|\omega|>2R}$$

where the first sum is finite (and bounded) and the second sum is (see 1.) uniformly (and locally) convergent on $U(0,R)\smallsetminus\Lambda$. This implies that $\mathcal{P}(z)$ is a holomorphic function on $\mathbb{C}\smallsetminus\Lambda$ with double pole at each $z \in \Lambda$ (with residue 0).

3. The Weierstrass function is even, i.e. $\mathcal{P}(-z) = \mathcal{P}(z)$. The uniform convergence gives

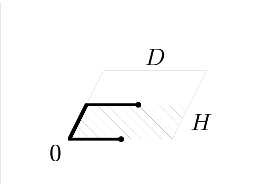
$$\mathcal{P}'(z) = \sum_{\omega\in\Lambda} \frac{-2}{(z-\omega)^3},$$

which is an elliptic function, i.e. $\mathcal{P}'(z+\omega) = \mathcal{P}'(z)\ \forall\,\omega\in\Lambda$.
We have

$$\frac{d}{dz}\left(\mathcal{P}(z+\omega) - \mathcal{P}(z)\right) = 0,$$

i.e. $\mathcal{P}(z+\omega) = \mathcal{P}(z) + c(\omega)\ \forall\,\omega\in\Lambda,\ \forall\,z\in\mathbb{C}\smallsetminus\Lambda$. Taking $z = -\frac{1}{2}\omega$, we get $\mathcal{P}(\frac{\omega}{2}) = \mathcal{P}(-\frac{\omega}{2}) + c(\omega)$ and so $c(\omega) = 0$ due to the evenness of $\mathcal{P}$. ■

Theorem 27. *Let $\Lambda \subset \mathbb{C}$ be a lattice. $\mathbb{C}(\Lambda) = \mathbb{C}(\mathcal{P}(z), \mathcal{P}'(z))$.*



Proof: Let $f(z) \in \mathbb{C}(\Lambda)$. We have $f(z) = \frac{1}{2}(f(z) + f(-z)) + \frac{1}{2}\mathcal{P}'(z)\frac{(f(z)-f(-z))}{\mathcal{P}'(z)}$, where $f(z)+f(-z)$ and $\frac{f(z)-f(-z)}{\mathcal{P}'(z)}$ are even elliptic functions. Thus it is sufficient to prove that the subfield $\mathbb{C}^+(\Lambda)$ of even functions is generated by $\mathcal{P}(z)$, i.e. $\mathbb{C}^+(\Lambda) = \mathbb{C}(\mathcal{P}(z))$.
If f is even, we have $\mathrm{ord}_w f = \mathrm{ord}_{-w} f\ \forall\,w\in\mathbb{C}$. If moreover $2w \in \Lambda$, then $\mathrm{ord}_w f$ is even: differentiate $f(z) = f(-z)$ repeatedly to obtain $f^{(i)}(z) = (-1)^{(i)} f^{(i)}(-z)$. Now if $2w \in \Lambda$, i.e. $w = -w \bmod \Lambda$ and

so $f^{(i)}(w) = f^{(i)}(-w)$, which implies $f^{(i)}(w) = 0 \; \forall\, i \in (2\mathbb{N}+1)$ and so finally $\mathrm{ord}_w f$ must be even.
Let D be a fundamental parallelogram for Λ, and let H be a fundamental domain for $(\mathbb{C}/\Lambda)/\{\pm 1\}$, i.e. $\mathbb{C} \simeq (H+\Lambda) \cup (-H+\Lambda)$ (see the picture).
The above implies

$$\mathrm{Div}\,(f) = \sum_{w \in H} n_w\big((w) + (-w)\big),\ n_w \in \mathbb{Z}.$$

Consider the function

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

We have

$$\mathrm{Div}\ (\mathcal{P}(z) - \mathcal{P}(w)) = (w) + (-w) - 2(0)$$

i.e.

$$\mathrm{Div}\,(f) = \mathrm{Div}\,(g),\ w \in H \setminus 0$$

and 2. of the Theorem 26 $\big(\sum_{w \in \mathbb{C}/\Lambda} \mathrm{ord}_w(f) = 0 = \sum_{w \in \mathbb{C}/\Lambda} \mathrm{ord}_w(g)\big)$ implies that $\mathrm{Div}\,(f) = \mathrm{Div}\,(g)$. Therefore $f(z)/g(z)$ is a holomorphic elliptic function, hence is a constant $c \in \mathbb{C}$. This proves that $f(z) = c\,g(z) \in \mathbb{C}(\mathcal{P}(z), \mathcal{P}'(z))$. ■

Definition 34. *The Weierstrass σ-function (relative to Λ) is the function defined by the product*

$$\sigma(z) = \sigma(z,\Lambda) = z \prod_{\substack{\omega \in \Lambda \\ \omega \neq 0}} \left(1 - \frac{z}{\omega}\right) e^{\frac{z}{\omega} + \left(\frac{z}{\omega}\right)^2 \frac{1}{2}}.$$

Lemma 21.

1. *The infinite product for $\sigma(z)$ defines a holomorphic function on all of $\mathbb{C}$. It has simple zeros at each $z \in \Lambda$, and there are no other (zeros).*
2. $\frac{\mathrm{d}^2}{\mathrm{d}z^2} \log(\sigma(z)) = -\mathcal{P}(z)\ \forall z \in \mathbb{C} \setminus \Lambda$
3. $\forall\, \omega \in \Lambda\ \exists\, a, b \in \mathbb{C}$ *constants:*

$$\sigma(z+\omega) = e^{az+b}\sigma(z)\ \forall z \in \mathbb{C}.$$

Proof:

1. Morally, "$\sigma(z) = \prod_{\omega \in \Lambda}(z-\omega)$", but this infinite product doesn't converge $\forall z \in \mathbb{C}$. We know that $\sum_{\substack{\omega \in \Lambda \\ \omega \neq 0}} \frac{1}{|\omega|^s} < \infty \Leftrightarrow \mathrm{Re}(s) > 2$ $(s \in \mathbb{C})$. Now the equality $-\log(1-\frac{z}{\omega}) = \frac{z}{\omega} + \frac{1}{2}(\frac{z}{\omega})^2 + \frac{1}{3}(\frac{z}{\omega})^3 + \cdots$ and the standard results on convergence of infinite products (see the Theorem 28) imply the absolute and uniform convergence on $\mathbb{C}$.

2. It follows from 1. that we can term-wise differentiate

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

and the result follows.

3. We know $\mathcal{P}(z+\omega) = \mathcal{P}(z)\ \forall \omega \in \Lambda$, *i.e.* $\frac{\mathrm{d}^2}{\mathrm{d}z^2} \log \sigma(z+\omega) = \frac{\mathrm{d}^2}{\mathrm{d}z^2} \log \sigma(z)\ \forall \omega \in \Lambda$. Two times integration yields

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

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

The following Theorem 28 is well-known, see [1].

Theorem 28. *Let us denote by $\mathcal{O}(\Omega)$ ($\Omega \subset \mathbb{C}$:= an open domain in $\mathbb{C}$) the ring of non-zero holomorphic functions on Ω. Suppose $f_n \in \mathcal{O}^*(\Omega)$, $n = 1, 2, \ldots$. Then $\sum_{n=1}^{\infty} |1 - f_n(z)|$ converges uniformly on compact subsets of Ω iff the product $f(z) = \prod_{n=1}^{\infty} f_n(z)$ converges uniformly on compact subsets of Ω. Moreover $m(f, z) = \sum_{n=1}^{\infty} m(f_n, z)$, $z \in \Omega$, where $m(f, z)$ (resp. $m(f_n, z)$) is defined to be the multiplicity of the zero of f (resp. f_n) at z.*

Lemma 22. *Let $n_1, \ldots, n_r \in \mathbb{Z}$ and $z_1, \ldots, z_r \in \mathbb{C}$ satisfy $\sum_{i=1}^{r} n_i = 0$ and $\sum_{i=1}^{r} n_i z_i \in \Lambda$. Then there $\exists$ an elliptic function $f(z) \in \mathbb{C}(\Lambda)$ satisfying* $\operatorname{Div}(f) = \sum_{i=1}^{r} n_i z_i$. *If we normalize the divisor in such a way that $\sum_{i=1}^{r} n_i z_i = 0$, then $f(z) = \prod_{i=1}^{r} \sigma(z - z_i)^{n_i}$.*

Proof: Let $\omega = \sum_{i=1}^{r} n_i z_i \in \Lambda$. Replacing $n_1(z_1) + \cdots + n_r(z_r)$ by $n_1(z_1) + \cdots + n_r(z_r) + (0) - (\omega)$, we can assume $\sum_{i=1}^{r} n_i z_i = 0$. Then 1. of the previous Lemma 21 implies that

$$f(z) = \prod_{i=1}^{r} \sigma(z - z_i)^{n_i}$$

has the correct zeros and poles. The previous Lemma 21, 3., gives

$$\frac{f(z+\omega)}{f(z)} = \prod_{i=1}^{r} e^{(a(z-z_i)+b)n_i} = e^{(az+b)\sum_{i=1}^{r} n_i} e^{-a\sum_{i=1}^{r} n_i z_i} = 1,$$

and so $f(z) \in \mathbb{C}(\Lambda)$. ■

In the next Lemma we shall work out Laurent series expansion of $\mathcal{P}(z), \mathcal{P}'(z)$ which will lead to the fundamental **algebraic** relation satisfied by them.

Theorem 29.

1. *The Laurent series for $\mathcal{P}(z)$ around $z = 0$ is of the form*

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

2. $\forall z \in \mathbb{C} \setminus \Lambda$,
$$\mathcal{P}'^2(z) = 4\mathcal{P}^3(z) - 60G_4\mathcal{P}(z) - 140G_6.$$

Proof:

1. Let $|z| < |\omega|$. Then
$$(z-\omega)^{-2} - \omega^{-2} = \omega^{-2}\left[\left(1-\frac{z}{\omega}\right)^{-2} - 1\right] = \sum_{n=1}^{\infty}(n+1)\frac{z^n}{\omega^{n+2}}$$
Substituting this into the series for $\mathcal{P}(z)$ and reversing (due to the uniform convergence) the order of summation gives the result.

2. The Laurent expansions are
$$\begin{array}{rcl} \mathcal{P}(z) & = & z^{-2} + 3G_4z^2 + 5G_6z^4 + 7G_8z^6 + \cdots, \\ \mathcal{P}'^2(z) & = & 4z^{-6} - 24G_4z^{-2} - 80G_6 + \cdots, \\ \mathcal{P}^3(z) & = & z^{-6} + 9G_4z^{-2} + 15G_6 + (21G_8 + 27G_9^2)z^2 + \cdots \end{array}$$

The comparison reveals that
$$f(z) = \mathcal{P}'^2(z) - 4\mathcal{P}^3(z) + 60G_4\mathcal{P}(z) + 140G_6$$
is holomorphic at $z = 0$ and vanishes at $z = 0$. Since it is also elliptic function relative to $\Lambda \subset \mathbb{C}$, it is constant function in $\mathbb{C}$ and hence trivial ($f(z) = 0\ \forall z \in \mathbb{C}$). ■

Remark 6. *We set* $g_2 \equiv g_2(\Lambda) = 60G_4$,
$g_3 \equiv g_3(\Lambda) = 140G_6$.

Let $E/\mathbb{C}$ be an elliptic curve $\mathcal{P}'^2(z) = 4\mathcal{P}^3(z) - g_2\mathcal{P}(z) - g_3$. The set of complex points of $E/\mathbb{C}$, $E(\mathbb{C})$, is a complex manifold with group law $E/\mathbb{C}\times E/\mathbb{C} \to E/\mathbb{C}$ given by everywhere locally defined rational functions. In particular, $E/\mathbb{C}$ is a complex Lie group. Similarly, $\mathbb{C}/\Lambda$ is a complex Lie group. We show that $\mathbb{C}/\Lambda$ is always complex analytically isomorphic to an elliptic curve.

Theorem 30. *Let* $\Lambda \subset \mathbb{C}$ *be a lattice and* $g_2 = g_2(\Lambda) = 60G_4$, $g_3 = g_3(\Lambda) = 140G_6$ *Eisenstein series.*

1. *The polynomial*
$$f(x) = 4x^3 - g_2x - g_3$$
has distinct roots. Its discriminant is thus non-zero.

2. *Let* $E/\mathbb{C}$ *be the affine curve*
$$E = \{(x,y) \in \mathbb{C}^2 |\ y^2 - 4x^3 - g_2x - g_3 = 0\} \subset \mathbb{C}^2,$$

or its projectivization (denoted by the same letter)

$$E = \{(x, y, z) \in \mathbb{C}^3 |\ y^2z - 4x^3 + g_2xz^2 + g_3z^3 = 0\} \subset \mathbb{P}^2(\mathbb{C}).$$

which is an elliptic curve associated to the cubic polynomial defined in 1. Then the map

$$\begin{array}{rcl} \varphi : \mathbb{C}/\Lambda & \longmapsto & E \subset \mathbb{P}^2(\mathbb{C}), \\ z & \longmapsto & [\mathcal{P}(z), \mathcal{P}'(z), 1],\ z \in (\mathbb{C}/\Lambda) \smallsetminus \Lambda, \\ z & \longmapsto & [0,\ 1,\ 0],\ z \in \Lambda \end{array}$$

is a complex analytic isomorphism of complex Lie groups (i.e. the isomorphism of Riemann surfaces which is a group homomorphism).

Proof:

1. Let $\{\omega_1, \omega_2\}$ be a basis of $L \subset \mathbb{C}$, and $\omega_3 = \omega_1 + \omega_2$. Since $\mathcal{P}'$ is an odd elliptic function, we see that

   $$\mathcal{P}'\left(\frac{\omega_i}{2}\right) = -\mathcal{P}'\left(-\frac{\omega_i}{2}\right) = -\mathcal{P}'\left(-\frac{\omega_i}{2} + \omega_i\right) = -\mathcal{P}'\left(-\frac{\omega_i}{2}\right) \quad i = 1, 2, 3$$

   i.e. $\mathcal{P}'\left(\frac{\omega_i}{2}\right) = 0$. This means that $f(x) = 0$ for $\mathcal{P}\left(\frac{\omega_i}{2}\right)$, $i = 1, 2, 3$ and so it is sufficient to prove that $\mathcal{P}\left(\frac{\omega_i}{2}\right)$ are distinct complex numbers.
   The function $\mathcal{P}(z) - \mathcal{P}\left(\frac{\omega_i}{2}\right)$ is even, i.e. it has at least a double zero at $z = \frac{\omega_i}{2}$, $i = 1, 2, 3$. But since it has order 2, these are the only zeros and so $\mathcal{P}\left(\frac{\omega_i}{2}\right) \neq \mathcal{P}\left(\frac{\omega_j}{2}\right)$ for $i \neq j,\ i, j = 1, 2, 3$.

2. It follows from 2. of the previous Theorem 29 that $\varphi(\mathbb{C}/\Lambda) \subset E/\mathbb{C}$. To prove that φ is surjective, let $(x, y) \in E(\mathbb{C})$. Then $\mathcal{P}(z) - x$ is a non-constant elliptic function, and so it has a zero, say for $z = a$, i.e. $\mathcal{P}(a) = x$. Then $\mathcal{P}'^2(a) = y^2$, so replacing $a \to -a$ if necessary, we obtain $\mathcal{P}'(a) = y$. Then $\varphi(a) = (x, y)$.
   To prove the injectivity, assume $\varphi(z_1) = \varphi(z_2)$. Assume first that $2z_1 \notin \Lambda$. Then the function $\mathcal{P}(z) - \mathcal{P}(z_1)$ has order 2 and zeros $z_1, -z_1, z_2$. It follows $z_2 = \pm z_1 \bmod \Lambda$, and

   $$\mathcal{P}'(z_1) = \mathcal{P}'(z_2) = \mathcal{P}'(\pm z_1) = \pm\mathcal{P}'(z_1)$$

   implies, due to $\mathcal{P}'(z_1) \neq 0$ (see 1.), $z_2 = z_1 \bmod \Lambda$. Now if instead $2z_1 \in \Lambda$, then $\mathcal{P}(z) - \mathcal{P}(z_1)$ has a double zero at z_1 and vanishes at z_2 and we again conclude that $z_2 = z_1 \bmod \Lambda$.
   To show that φ is an analytic isomorphism, we compute its effect on the cotangent space. We know that $\forall (x, y) \in E(\mathbb{C})$, $\frac{\mathrm{d}x}{y}$ is a non-vanishing holomorphic differential, since

   $$\varphi^*\left(\frac{\mathrm{d}x}{y}\right) = \frac{\mathrm{d}\mathcal{P}(z)}{\mathcal{P}'(z)} = \mathrm{d}z$$

is non-vanishing and holomorphic $\forall z \in \mathbb{C}/\Lambda$, φ is a local isomorphism. But the bijectivity proved above implies that it is a global isomorphism. Let $z_1, z_2 \in \mathbb{C}$. There is a function $f \in \mathbb{C}(\Lambda)$ with divisor

$$\mathrm{Div}\,(f) = (z_1 + z_2) - (z_1) - (z_2) - (0).$$

Because $f(z) = F(\mathcal{P}(z), \mathcal{P}'(z))$ for some rational function $F(x, y) \in \mathbb{C}(x, y)/I = \mathbb{C}(E(\mathbb{C}))$, we have

$$\mathrm{Div}\,(F) = (\varphi(z_1 + z_2) - \varphi(z_1) - \varphi(z_2) + \varphi(0))\,.$$

But the principality of this divisor $\mathrm{Div}\,(F)$ implies $\varphi(z_1 + z_2) - \varphi(z_1) - \varphi(z_2) - \varphi(0) = \varphi(z_1 + z_2) - \varphi(z_1) - \varphi(z_2) = 0$, i.e. $\varphi(z_1 + z_2) = \varphi(z_1) + \varphi(z_2)$, which proves the property of group homomorphism. ■

Chapter 16

Kleinian groups and modular forms

16.1 Möbius transformations

An element $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{PSL}(2, \mathbb{C})$ acts on the Riemann sphere $\overline{\mathbb{C}} = \mathbb{C} \cup \{\infty\}$ as the Möbius transformation $z \mapsto \frac{az+b}{cz+d}$. We consider $\mathrm{SL}(2, \mathbb{C})$ as the closed subset of complex Euclidean $4-$space defined by the equation

$$(a, b, c, d) \in \mathbb{C}^4 : \, ad - bc = 1,$$

and give $\mathrm{PSL}(2, \mathbb{C}) := \mathrm{SL}(2, \mathbb{C}) / \{\pm I\}$ the quotient topology y.

Let $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{PSL}(2, \mathbb{C})$, $A \neq I$. Then

$$\begin{aligned} \text{A is parabolic} &\iff \mathrm{Tr}^2(A) = (a+d)^2 = 4, \\ \text{A is elliptic} &\iff 0 \leq \mathrm{Tr}^2(A) < 4, \\ \text{A is hyperbolic} &\iff \mathrm{Tr}^2(A) > 4, \\ \text{A is loxodromic} &\iff \mathrm{Tr}^2(A) \notin [0, 4]. \end{aligned}$$

Note that hyperbolic is only special case of loxodromic. The map $A \mapsto \mathrm{Tr}^2(A)$ is $\mathrm{PSL}(2, \mathbb{C})$ conjugacy invariant, i.e.

$$A = CBC^{-1} \in \mathrm{PSL}(2, \mathbb{C}) \iff \mathrm{Tr}^2(A) = \mathrm{Tr}^2(B) \, .$$

The map $z \mapsto \frac{az+b}{cz+d}$ has either one or two fixed points in $\overline{\mathbb{C}}$:

$$\begin{aligned} \{\alpha, \beta\} &= \left\{ \frac{1}{2c} \left((a-c) \pm \sqrt{\mathrm{Tr}^2(A) - 4} \right) \right\} \text{ if } c \neq 0, \\ \{\alpha, \beta\} &= \left\{ \infty, -\frac{b}{a - a^{-1}} \right\} \text{ if } c = 0. \end{aligned} \tag{16.1}$$

Then A is parabolic iff A has one fixed point in $\overline{\mathbb{C}}$ iff A is conjugate in $\mathrm{PSL}(2,\mathbb{C})$ to $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$. In all other cases $A \neq I$ has to fixed points and is hence conjugate in $\mathrm{PSL}(2,\mathbb{C})$ to $\begin{pmatrix} \lambda & 0 \\ 0 & \lambda^{-1} \end{pmatrix}$ with $\lambda \in \mathbb{C} \setminus \{0,-1,1\}$. In this case A is

- elliptic $\Longleftrightarrow |\lambda| = 1$
- hyperbolic $\Longleftrightarrow \lambda \in \mathbb{R}$
- loxodromic $\Longleftrightarrow |\lambda| \neq 1$

The number $\lambda^2 = \lambda^2(A)$ is called the multiplier of A (λ^2 and λ^{-2} are multipliers of the same Möbius transformation. For A parabolic or $A = I$ we set $\lambda^2(A) = 1$. Note that $\lambda^2(A^n) = \big(\lambda^2(A)\big)^n$, $A \in \mathrm{PSL}(2,\mathbb{C})$. A Möbius transformation is of finite order n iff n is the smallest integer such that $\lambda^{2n}(A) = 1$.

A parabolic transformation A with a finite fixed point a and translation length α can be written in the normal form as a motion of the sphere as

$$\frac{1}{A(z)-a} = \frac{1}{z-a} + \alpha, \quad \alpha \in \mathbb{C}^*,$$

or as an element of $\mathrm{PSL}(2,\mathbb{C})$ as

$$A = \begin{bmatrix} 1+a\alpha & -a^2\alpha \\ \alpha & 1-a\alpha \end{bmatrix}, \quad \big(\mathrm{Tr}\,(A) = 2\big).$$

Question

What about the case of the fixed point $\big(\overline{\mathbb{C}} \setminus \mathbb{C}\big)$?

The transformation A with fixed point a, b and multiplier λ^2 is given in normal form by

$$\frac{A(z)-a}{A(z)-b} = \lambda^2 \frac{z-a}{z-b},$$

and as element of $\mathrm{PSL}(2,\mathbb{C})$ as

$$A = \frac{1}{\lambda(a-b)} \begin{pmatrix} a-\lambda^2 b & ab(\lambda^2-1) \\ 1-\lambda^2 & \lambda^2 a - b \end{pmatrix}.$$

It is easy to verify that for parabolic transformation A holds

$$\left.\frac{\mathrm{d}}{\mathrm{d}\,z}\right|_{z=a} A(z) = 1.$$

For loxodromic A, we call a

$$\begin{aligned} \text{attractive} &\Longleftrightarrow |A'(a)| < 1, \\ \text{repulsive} &\Longleftrightarrow |A'(a)| > 1. \end{aligned} \tag{16.2}$$

16.2 Kleinian groups

The reader is warned that not all claims are easily verifiable.

Let X be a subset of the sphere $\mathbb{CP}^1$. Consider an inclusion of groups $G \subset \Gamma \subset \mathrm{PSL}(2,\mathbb{C})$. We say that X is precisely invariant under G in Γ provided

$$g(X) = X\ (\forall g \in G) \text{ and } \gamma(X) \cap X = \{\emptyset\}\ (\forall \gamma \in \Gamma \setminus G).$$

We say that Γ acts discontinuously at the point $z \in \overline{\mathbb{C}}$ provided the stabilizer Γ_z of z in Γ is finite, i.e. $\#\Gamma_z = \#\{\gamma \in \Gamma \mid \gamma z = z\} < \infty$, and there is a neighborhood U of z such that $\Gamma_z U \subseteq U$. The region of discontinuity $\Omega = \Omega(\Gamma)$ is the largest ($\Rightarrow$ open) set on which the group Γ acts discontinuously. Its complement $\Lambda = \Lambda(\Gamma)$ is the limit set of Λ. The group Γ is called Kleinian group provided $\Omega \neq \{\emptyset\}$.

Remark 7. *If $\Gamma \subseteq PSL(2,\mathbb{C})$ and Γ acts discontinuously somewhere on $\overline{\mathbb{C}}$, then Γ is automatically discrete. Hence every Kleinian group is commutable. Discreteness does not imply discontinuity. The discrete group $PSL(2,\mathbb{Z}[i])$, for example, does not act discontinuously on $\overline{\mathbb{C}}$.*

Definition 35. *Let G be a group of homeomorphisms of topological space X. The group generates an equivalence relation on X: two points $x, y \in X$ are equivalent (modulo G) if there is $g \in G$ such that $g(x) = y$. The set of equivalence classes is the quotient space X/G. Let $\pi : G \to X/G$ ($x \mapsto Gx$) be the quotient map such that X/G is equipped with the weakest topology for which π is continuous map.*

The factor space $\Omega(\Gamma)/\Gamma$ is a union of at most countably many Riemann surfaces whenever the group Γ is Kleinian. If Γ is Kleinian group, then for each $z \in \Omega(\Gamma)$, the stabilizer $\Gamma_z = \{\gamma \in \Gamma \mid \gamma(z) = z\}$ is a finite cyclic group. If $A \in \mathrm{PSL}(2,\mathbb{C})$, then the conjugate group

$$A\Gamma A^{-1} = \left\{A \circ \gamma \circ A^{-1} \mid \gamma \in \Gamma\right\}$$

is also Kleinian and

- $\Omega\left(A\Gamma A^{-1}\right) = A\left(\Omega(\Gamma)\right)$,
- $\Lambda\left(A\Gamma A^{-1}\right) = A\left(\Lambda(\Gamma)\right)$,
- $\Omega\left(A\Gamma A^{-1}\right)/A\Gamma A^{-1} \simeq \Omega(\Gamma)/\Gamma$.

Definition 36. *Let G be a group of Möbius transformations operating on a set $D \subset \overline{\mathbb{C}}$. A fundamental domain for the action of G on D is a connected open set $O = O(G)$ bounded by analytic areas $\bigcup_{i\in I}\left(c_i^+ \cup c_i^-\right)$ satisfying:*

1/ $\forall x \in D$, there is a $z \in \overline{O}$ and a $g \in G$ such that $g(x) = z$, *2/ if* $z_1, z_2 \in O$ *and* $g(z_1) = z_2$ *for some* $g \in G$*, then* $g = Id$*,*

3/ for each $i \in I$*, there exists a* $g_i \in G$ *with* $g_i\left(c_i^+\right) = c_i^-$*.*

A fundamental set for the action of G on D is a set conatining exactly one point for each $G-$orbit. Roughly, Ω/Γ is obtained by boundary identifications on the closure of a fundamental domain for the action of Γ on Ω. We let

$$\Delta_1, \ldots, \Delta_i, \ldots$$

be a maximal set of $\Gamma-$inequivalent components of Ω, and we let

$$\Gamma_i = \{\gamma \in \Gamma \mid \gamma(\Delta_i) = \Delta_i\}$$

be the stabilizer of Δ_i in Γ. If Γ is finitely generated then Γ_i have also this property. Moreover,

$$\Omega/\Gamma \simeq \bigcup_i \Delta_i/\Gamma_i$$

and the union is finite whenever Γ is finitely generated.

16.3 Fundamental domain for congruence subgroups

Let $\mathbb{H}^2 = \{\tau \in \mathbb{C} \mid \mathrm{Im}(\tau) > 0\}$. A point τ determines a free abelian group $\tilde{G} = \tilde{G}_\tau$, generated by the two translations T_1, T_2:

$$T_1 : \mathbb{C} \longrightarrow \mathbb{C}, \quad z \longmapsto z+1, \qquad T_2 : \mathbb{C} \longrightarrow \mathbb{C}, \quad z \longmapsto z+\tau.$$

The complex plane $\mathbb{C}$ quotiened by this equivalence relation defined by T_1, T_2 is topologically a torus T_τ, $T_\tau \simeq \mathbb{C}/\tilde{G}$. A fundamental domain for $\tilde{G}$ is defined by

$$D = D\left(\tilde{G}\right) = \{a + t_1 + t_2\tau \mid 0 < t_1 < 1, 0 < t_2 < 1\}, \, a \in \mathbb{C}.$$

The Abel's theorem tells us that for any (compact) Riemann surface with fundamental group $\mathbb{Z} \oplus \mathbb{Z}$ there is a $\tau \in D$ such that this Riemann surface is conformally equivalent to T_τ.

The previous definition of T_τ as a complex analytic manifold comes from the approach of factorization of $\mathbb{C}$ by a discontinuous group $\tilde{G}$. The lattice points of $\tilde{G}$,

$$L = L\left(\tilde{G}\right) = \{n + m\tau \mid m, n \in \mathbb{Z}\}$$

from a normal subgroup of the additive group $\tilde{G}$, hence $T_\tau = \mathbb{C}/L$ is a $1-$dimensional Lie group (a complex analytic manifold with commutative group structure).

Theorem 31. *Two points $\tau_1, \tau_2 \in \mathbb{H}^2$ determine conformally equivalent tori iff there exists a Möbius transformation $M \in PSL(2, \mathbb{Z}[i]) = SL(2, \mathbb{Z})/\{\pm Id\}$ with $\tau_2 = M\tau_1$.*

Proof:

The following is the standard result from complex analysis on $\mathbb{C}$. Let $f : T_{\tau_1} \to T_{\tau_2}$ be a conformal group. Then there exists a conformal map $F : \mathbb{C} \to \mathbb{C}$ such that the diagram

$$\begin{array}{ccc} \mathbb{C} & \xrightarrow{F} & \mathbb{C} \\ \Pi_1 \big\downarrow & & \big\downarrow \Pi_2 \\ T_{\tau_1} & \xrightarrow{f} & T_{\tau_2} \end{array}$$

is commutative, where Π_1, Π_2 are the canonical projections. Since F is conformal, we get

$$\begin{aligned} F : \mathbb{C} &\longrightarrow \mathbb{C} \\ z &\longmapsto az + b, \quad a \in \mathbb{C}^*, b \in \mathbb{C}. \end{aligned} \tag{16.3}$$

The translation map $T_b : \mathbb{C} \to \mathbb{C}, z \mapsto z+b$ is conformal self-map of T_{τ_2}, hence we assume $b = 0$. The commutativity of the diagram implies $F\, \tilde{G}_{\tau_1} F^{-1} = \tilde{G}_{\tau_2}$. Let us call this conjugation θ. Identifying the translation $z \mapsto z + b$ with $b \in \mathbb{C}$, we see

$$\theta(1) = F(1) = a,\ \theta(\tau_1) = F(\tau_1) a\tau_1$$

must be generators for $\tilde{G}_{\tau_2}$. Thus there exists an $A = \begin{bmatrix} \alpha & \beta \\ \gamma & \delta \end{bmatrix} \in \mathrm{GL}(2, \mathbb{Z})$ so that $a = \alpha + \beta\tau_2, a\tau_1 = \gamma + \delta\tau_2$. Hence $\tau_1 = \frac{\gamma+\delta\tau_2}{\alpha+\beta\tau_2}$. Since $\tau_1, \tau_2 \in \mathbb{H}^2$, A must belong to $\mathrm{SL}(2, \mathbb{Z})$, and $M = \begin{bmatrix} \alpha & -\gamma \\ -\beta & \delta \end{bmatrix}$. Conversely, if $\tau_2 = M(\tau_1)$ with M as above, then we define

$$F(z) := (\alpha + \beta\tau_2)\, z, \quad z \in \mathbb{C}.$$

It follows that

$$F(z + 1) = F(z) + (\alpha + \beta\tau_2)\,, F(z + \tau_1) = F(z) + (\gamma + \delta\tau_2)$$

for all $z \in \mathbb{C}$. This means that F defines a conformal map of T_{τ_1} onto T_{τ_2}. ■

Let G be a group of Möbius transformations. Assume that G is discontinuous and consists in addition to the identity of only parabolic transformations. Then G is either cyclic and hence conjugate to the group generated by

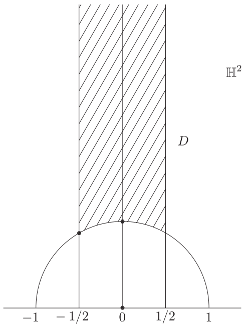
$$T_1 : \overline{\mathbb{C}} \longrightarrow \overline{\mathbb{C}}, \quad z \longmapsto z + 1 \,\left(z \in \overline{\mathbb{C}}\right),$$

or G is conjugate to $\tilde{G}_\tau$ for some $\tau \in \mathbb{H}^2$.

Theorem 32. *A fundamental domain for the action of* $\Gamma = PSL(2, \mathbb{Z}[i])$ *on* $\mathbb{H}^2$ *is the open region* $D = D\,(PSL(2, \mathbb{Z}[i]))$ *in* $\mathbb{H}^2$ *bounded by the lines* $\mathrm{Re}\,(\tau) = -\frac{1}{2}$, $\mathrm{Re}\,(\tau) = \frac{1}{2}$ *and semi-circle* $|\tau| = 1$. *A fundamental set for this action can be obtained by adjoining the circular arc from* i *to* $\frac{1}{2}\left(1 + i\sqrt{3}\right)$ *(including both end points) and the vertical line segment from* $\frac{1}{2}\left(1 + i\sqrt{3}\right)$ *to* $i\infty$.

Proof:

The fundamental set is of the form on this picture.



First of all, we shall show that no two points of D are Γ−equivalent. Assume that $\tau_1\tau_2 \in \mathbb{H}^2$ are equivalent under Γ, and $\mathrm{Im}\,(\tau_2) \geq \mathrm{Im}\,(\tau_1)$. Let $\tau_2 = \frac{a\tau_1 + b}{c\tau_1 + d}$, $C = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \mathrm{SL}(2, \mathbb{Z})$. Since $\mathrm{Im}\,(\tau_2) = \frac{\mathrm{Im}(\tau_1)}{|c\tau_1 + d|^2}$, we must have $|c\tau_1 + d| \leq 1$.

If $c = 0$, then $ad = 1$ and so both $a = \pm 1, d = \pm 1$. Without loss of generality we may assume $a = 1 = d$. It follows that $\tau_2 = \tau_1 + b$, hence

$$|b| = |\mathrm{Re}\,(\tau_2) - \mathrm{Re}\,(\tau_1)| = 0 \implies b = 0.$$

Assume now that $c \neq 0$. The condition $\left|\tau_1 + \frac{d}{c}\right| \leq \frac{1}{|c|}$ implies that $|c| = 1$. For if $|c| \geq 2$, then τ_1 would be at a distance at most $\frac{1}{2}$ from real axis $\mathbb{R}$, which is impossible since the point in D nearest to $\mathbb{R}$ is $\frac{1}{2}\left(1 + i\sqrt{3}\right)$. Without loss of generality we may assume $c = 1$ and hence $|\tau_1 + d| \leq 1$. The geometric shape of D tells us that this is possible only for $|d| \leq 1$. The inequality $|\tau_1 + 1| \leq 1$ ($d = 1$) is never satisfied for points $\tau_1 \in D$ since $\exp\,(2\pi i/3) \notin D$. The inequality $|\tau_1 - 1| \leq 1$ ($d = -1$) is satisfied only by the point $\exp\,(2\pi i/3) \in D$. For this point we have

$$|c\tau_1 + d| = \left|\exp\left(\frac{2\pi i}{3}\right) - 1\right| = 1,$$

hence $\mathrm{Im}\,(\tau_2) = \mathrm{Im}\,(\tau_1)$ and by the geometric shape of D, $\tau_1 = \tau_2$. It remains to consider the case $c = 1, d = 0$. This implies $b = -1$, and since $|\tau_1| \leq 1$ and $|\tau_1| \geq 1$ ($\tau_1 \in D$), we conclude that $|\tau_1| = 1$ and $\tau_2 = a - \frac{1}{\tau_1} = a - \overline{\tau_1}$. Hence $\mathrm{Re}\,(\tau_1 + \tau_2) = a$, and this is possible only when $a = 0$ $\left(|\mathrm{Re}\,(\tau_1)| < \frac{1}{2} \wedge |\mathrm{Re}\,(\tau_2)| < \frac{1}{2} \text{ for } \tau_1, \tau_2 \in D\right)$. Thus $\tau_2 = -\frac{1}{\tau_1}$, which tells us that $\tau_1 = i = \tau_2$ (see on the picture of $\overline{D}$ how the map $\tau \to -\overline{\tau}$ works). It remains to show that every $\tau \in \mathbb{H}^2$ is Γ−equivalent to at least one point in the closure $\overline{D}$ of D. This is easy to see using the composition of the maps

1/ $C = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} \in \mathrm{SL}(2, \mathbb{Z}), \quad b \in \mathbb{Z},$

2/ $C' = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix} \in \mathrm{SL}(2, \mathbb{Z}).$

This completes the proof. ■

Chapter 17

Heights on algebraic varieties

The height measures the size of a rational point on an elliptic curve by counting the number of digits necessary to write down the coordinates of the point (or just its $x-$ coordinate). Numerical experiments of calculation the coordinates of the multiples $[n]P$ of a non-torsion rational point P real parabolic shape - the number of digits necessary to write $[n]P$ grows quadratically with n. This quadratic behavior is the ingredient used in the proof of the Mordell-Weil theorem.

Consider the $n-$dimensional projective space $\mathbb{P}^n_{\mathbb{Q}}$ over $\mathbb{Q}$ with a fixed homogeneous coordinate system. Given a rational point $x \in \mathbb{P}^n_{\mathbb{Q}}$, we can write $x = (x_1, \ldots, x_n)$, with $x_j \in \mathbb{Z}$ and $\gcd(x_0, \ldots, x_n) = 1$. This determines the values of the homogenous coordinates (up to a units $\{\pm 1\} \in \mathbb{Z}^*$).

Definition 37. *The height H of $x \in \mathbb{P}^n_{\mathbb{Q}}$ resp. the logarithmic height h of $x \in \mathbb{P}^n_{\mathbb{Q}}$ are defined by*

$$\begin{aligned} H(x) &= \max\left(|x_1|, \ldots, |x_n|\right) \geq 1, \\ h(x) &= \log\left(H(x)\right) \geq 0. \end{aligned} \tag{17.1}$$

In particular, a rational number $x - \frac{a}{b}$ $(a, b \in \mathbb{Z},\ gcd(a, b) = 1)$ is naturally a point of $\mathbb{P}^1_{\mathbb{Q}}$. Its height is equal to

$$\begin{aligned} H\left(\frac{a}{b}\right) &= \max\left(|a|, |b|\right), \\ h\left(\frac{a}{b}\right) &= \log\left(\max\left(|a|, |b|\right)\right). \end{aligned} \tag{17.2}$$

If one works over number fields, one needs to use the normalized valuations on K, which are defined as follows ($x \in K^*$):

$$||x||_v = \begin{cases} (Nv)^{-\operatorname{ord}_v(x)}, & v \in M_K^f \\ |x|^{[K_v:\mathbb{R}]}, & v \mid M_K^\infty \end{cases}$$

where $N_v = \#k(v)$ is the norm of $v \in M_K^f$. The normalized valuations satisfy the product formula

$$\prod_{v \in M_K} ||x||_v = 1, \quad \forall x \in K^*,\ M_K = M_K^+ \cup M_K^\infty.$$

For $x \in \mathbb{P}^n(K)$, we choose any homogeneous coordinates $x = (x_0, \ldots, x_n)$ of x ($x_j \in K$) and put

$$H_K(x) = \prod_{v \in M_K} \max\left(\| x_0 \|_v, \ldots, \| x_n \|_v\right) \geq 1,$$

which is a finite product, independent of the choice of the homogeneous coordinates (thanks to the product formula). The quantities

$$H(x) = H_K(x)^{\frac{1}{[K:\mathbb{Q}]}},\ h(x) = \log\left(H(x)\right) \geq 0$$

are then independent on the number field K and define the function

$$h : \mathbb{P}^n\left(\overline{\mathbb{Q}}\right) \longrightarrow \mathbb{R}_{\geq 0},$$

which coincides on $\mathbb{P}^n(\mathbb{Q})$ with the height **??**.

Lemma 23. *Two real-valued functions $f, f' : S \to \mathbb{R}$ on a set S are equivalent (notation: $f \sim f'$) if the function $|f(x) - f'(x)|$ is bounded on S. If $h' : \mathbb{P}^n\left(\overline{\mathbb{Q}}\right) \to \mathbb{R}_{\geq 0}$ is the height defined by another system of homogeneous coordinates, $h' \sim h$.*

Proof (sketch)**:**

The change of homogeneous coordinates is given by $g \in \mathrm{GL}_{n+1}(K)$. For every $v \in M_K^f$,

$$\max_i \left(\| \sum_j g_{ij} x_j \|_v \right) \leq \left(\max_{i,j} \left(\| g_{ij} \|_v\right) \right) \max_j \left(\| x_j \|_v\right) = C_v(g) \max_j \left(\| x_j \|_v\right),$$

where $C_v(g) = 1$ for all but finitely many v. Similar bounds exist for $v \in M_K^\infty$. ■

Proposition 10. *For every $C, D > 0$, the set*

$$\left\{x \in \mathbb{P}^n\left(\overline{\mathbb{Q}}\right) \mid h(x) \leq C,\ [k(x) : \mathbb{Q}] \leq D \right\}$$

is finite. We denote by $k(x)$ the field of definition of x.

Proof:

It is enough to consider the points $x \in \mathbb{P}^n\left(\overline{\mathbb{Q}}\right)$ of fixed degree $[k(x) : \mathbb{Q}] = d$. If $d = 1$, then the statement follows from definition **??**. The general case $d > 0$ follows by induction using the map

$$f : \left\{x \in \mathbb{P}^n\left(\overline{\mathbb{Q}}\right) \mid h(x) \leq C,\ [k(x) : \mathbb{Q}] = d \right\} \longrightarrow \left\{y \in \mathbb{P}^N\left(\mathbb{Q}\right)\right\}$$

defined by sending $x = (x_0, \ldots, x_n)$ to the coefficient $y = (y_0, \ldots, y_N)$ of the norm form

$$N_{k(x)/\mathbb{Q}}\left(x_0 T_0 + \ldots + x_n T_n\right) = \sum_\alpha y_\alpha T^\alpha,$$

where α is a multiindex. The map has finite fibres $\left(\# f^{-1}(y) \le d\,(\forall y)\right)$ and

$$h(f(x)) \le d h(x) + c(n,d),$$

where $c(n,d)$ is a constant depending only on n, d. ■

Let $E : y^2 = x^3 + Ax + B$ be an elliptic curve over a number field K. Then the $x-$coordinate defines a morphism $x : E \to \mathbb{P}^1_K$, $\deg x = 2$. We fix a coordinate system on $\mathbb{P}^1$ and define

$$\begin{aligned} h_x : E\left(\overline{K}\right) &\longrightarrow \mathbb{R}_{\ge 0}, \\ P &\longmapsto h(x(P)). \end{aligned} \tag{17.3}$$

This function is even, i.e. $h_x(-P) = h_x(P)$ $(P \boxplus (-P) = 0)$.

Theorem 33 (Quadraticity of height). *The function h_x is almost quadratic in the sense that the function*

$$\mathrm{Cube}(h_x) : (E \times_k E \times_k E)\left(\overline{K}\right) \longrightarrow \mathbb{R},$$

$$\begin{aligned} (P,Q,R) \longmapsto\, & h_x(P \boxplus Q \boxplus R) - h_x(P \boxplus Q) - h_x(P \boxplus R) - h_x(Q \boxplus R) + \\ & h_x(P) + h_x(Q) + h_x(R) \end{aligned} \tag{17.4}$$

is bounded, i.e. $\mathrm{Cube}\,(h_x) \sim 0$.

Corollary 12.

1/ *For each point $P \in E\left(\overline{K}\right)$, the limit*

$$\hat{h}(P) = \frac{1}{2} \lim_{N \to \infty} \frac{h_x\left([mN]P\right)}{m^{2N}} \ge 0$$

exists and does not depend on the choice of $m \ge 2$ ($\hat{h}$ is called canonical or the Néron-Tate height).

2/ $\hat{h} \sim \frac{1}{2} h_x$, $\hat{h}(-P) = \hat{h}(P)$.

3/ $\mathrm{Cube}\left(\hat{h}\right) = 0$, *i.e. $\hat{h}$ is quadratic.*

4/ $\langle P, Q \rangle := \frac{1}{2}\left(\hat{h}(P \boxplus Q) - \hat{h}(P) - \hat{h}(Q)\right)$ *is a bilinear symmetric form*

$$\langle , \rangle : E\left(\overline{K}\right) \times E\left(\overline{K}\right) \longrightarrow \mathbb{R},$$

satisfying $\langle P, P \rangle \ge 0$ $\forall P \in E\left(\overline{K}\right)$.

5/ A point $P \in E\left(\overline{K}\right)$ *satisfies* $\langle P, P\rangle = 0 \iff P \in E\left(\overline{K}\right)_{tors.}$.

There are some useful (weak) properties of the height:

1/ For every $P_0 \in E(K)$ *there is a constant* $C_1 = C_1(E, K, P_0)$ *such that*

$$h_x(P \boxplus P_0) \leq 2h_x(P) + C_1, \quad \forall P \in E(K).$$

2/ There is a constant $C_2 = C_2(E, K)$ *such that*

$$h_x([2]P) \geq 4h_x(P) - C_2, \quad \forall P \in E(K).$$

3/ For every $C > 0$*, the set* $\{P \in E(K) \mid h_x(P) < C\}$ *is finite.*

Chapter 18

Galois cohomology, homogeneous spaces, Selmer and Tate-Shafarevich groups

The aim is to reformulate weak Mordell-Weil theorem and analyze it in terms of cohomologues of Galois groups. Let us first motivate the technical definition of cohomology group.

Question - Classification of twists.

Let X_0/K be an algebro-geometric structure (an algebra, a variety,a quadratic form, etc.) defined over a field K. Classify the set of $k-$isomorphism classes of objects X/k with the property that $X_0 \times_k \overline{k} \xrightarrow{\sim} X \times_k \overline{k}$. The objects X are called twists of X_0/k.

Ex. 18. *If X_0/k is a curve, then the twists of X_0 are curves defined over k such that they are isomorphic to $X_0/\overline{k}$. Let us consider the plane cubic curves*

$$X_{a,b,c} : ax^3 + by^3 + cz^3 = 0, \quad a, b, c \in k^*$$

The curves are all twists of one another, since by

$$\begin{aligned} [x, y, z] &\longrightarrow [a^{-1/3}x, b^{-1/3}y, c^{-1/3}z], \\ X_{a,b,c}/\overline{k} &\xrightarrow{\sim} X_{1,1,1}/\overline{k} \end{aligned} \tag{18.1}$$

for all a, b, c. However, it is a much more difficult question to determine isomorphism classes of $X_{a,b,c}$ over k.

Ex. 19. *Consider two varieties*

$$\begin{aligned}\mathbb{V}_1/\mathbb{Q} &: x^2+y^2=z^2,\\ \mathbb{V}_2/\mathbb{Q} &: x^2+y^2=3z^2.\end{aligned} \tag{18.2}$$

Concerning $\mathbb{V}_1/\mathbb{Q}$, *consider the natural map* $\varphi : \mathbb{V} \to \mathbb{P}^1$, $(x,y,z) \mapsto [x+y,z]$. *Clearly* φ *is regular at every point of* $\mathbb{V}_1$ *except possibly* $[1,0,-1]$ *(i.e. where* $x+z=0=y$*). But using*

$$(x+z)(x-z) \equiv -y^2 (mod\, I_{\mathbb{V}_1})$$

we have

$$\varphi(x,y,z) = [x+z,y] = [x^2-z^2, y(x-z)] = [-y^2, y(x-z)] = [-y, x-z].$$

Thus

$$\varphi([1,0,-1]) = [0,2] = [0,1],$$

so φ *is regular at every point of* $\mathbb{V}_1$ *(and is a isomorphism). One easily checks that the map*

$$\begin{aligned}\varphi' : \mathbb{P}^1 &\longrightarrow \mathbb{V}_1,\\ [s,t] &\longrightarrow [s^2-t^2, 2st, s^2+t^2].\end{aligned} \tag{18.3}$$

is a morphism (i.e. a rational map which is regular at every point). In particular $\mathbb{V}_1$ *has lot of rational points. Concerning* $\mathbb{V}_2/\mathbb{Q}$, $\mathbb{V}_2(\mathbb{Q}) = \{0\}$. *To see this, suppose* $[x,y,z] \in \mathbb{V}_2(\mathbb{Q})$ *with* $x,y,z \in \mathbb{Z}$ *and* $gcd(x,y,z)=1$. *Then*

$$x^2+y^2 \equiv 0\, mod 3,$$

so

$$x \equiv 0 \equiv y\, mod 3.$$

Hence x^2, y^2 are divisible by 3^2, so from the equation for $\mathbb{V}_2$ it follows that $3 \mid z$, which contradicts the assumption $\gcd(x,y,z)=1$.
By the way, this illustrates one of the fundamental tools used in the study of Diophantine equations: $\mathbb{V}(\mathbb{Q}) \neq \{\emptyset\} \Rightarrow \mathbb{V}(\mathbb{Q}_p) \neq \{\emptyset\}\, \forall p \in \mathbb{Z}$, p prime. The opposite implication is highly non-trivial and is the content of so called Hasse principle.
In conclusion, $\mathbb{V}_1/\mathbb{Q}(\mathbb{Q}) \simeq \mathbb{P}_1(\mathbb{Q})$ and $\mathbb{V}_2/\mathbb{Q}(\mathbb{Q}) = \{\emptyset\}$ are not isomorphic over $\mathbb{Q}$. However $\mathbb{V}_1/\mathbb{Q}$ and $\mathbb{V}_2/\mathbb{Q}$ are isomorphic over $\mathbb{Q}(\sqrt{3})$, an isomorphism being given by

$$\begin{aligned}\varphi : \mathbb{V}_2 &\longrightarrow \mathbb{V}_2\\ [x,y,z] &\longmapsto \left[x, y, \frac{z}{\sqrt{3}}\right]\end{aligned} \tag{18.4}$$

Let X be a twist of X_0, and fix a $\overline{k}-$isomorphism $f: X \to X_0$. Then for each $\sigma \in \mathrm{Gal}(\overline{k}/k)$ we obtain an automorphism of X_0 via the composition

$$X_0 \xrightarrow{f^{-1}} X \xrightarrow{f^{\sigma}} X_0.$$

Thus we obtain a map

$$\begin{aligned} \varphi: G &\longrightarrow \mathrm{Aut}(X_0) \\ \sigma &\longmapsto \varphi(\sigma) := f^{\sigma} \circ f^{-1}. \end{aligned} \tag{18.5}$$

This map φ is not a homomorphism, but rather "twisted homomorphism" (by the action of G):

$$\varphi(\sigma\tau) = f^{\sigma\tau} \circ f^{-1} = f^{\sigma\tau} \circ (f^{\tau})^{-1} \circ f^{\tau} \circ f^{-1} = \left(f^{\sigma} f^{-1}\right)^{\tau} f^{\tau} f^{-1} = \varphi(\sigma)^{\tau} \sigma(\tau),$$

where the middle equality follows from

$$f^{\tau} = \tau^{-1} f \tau,\ (f^{\tau})^{-1} = \tau^{-1} f^{-1} \tau \quad \left(f^{\tau} \left(f^{\tau}\right)^{-1} = 1 = \left(f^{\tau}\right)^{-1} f^{\tau}\right)$$

$$\Downarrow$$

$$\begin{aligned} \left(f^{\tau} f^{-1}\right)^{\tau} &= \tau^{-1} f^{\sigma} f^{-1} \tau = \tau^{-1} \sigma^{-1} f \sigma f^{-1} \tau = (\sigma\tau)^{-1} f \sigma \tau \tau^{-1} f^{-1} \tau = \\ &= f^{\sigma\tau} \tau^{-1} f^{-1} \tau = f^{\sigma\tau} \left(f^{\tau}\right)^{-1}. \end{aligned} \tag{18.6}$$

The map φ is called 1-cocycle on G with values in $\mathrm{Aut}(X_0)$. In most situations, the 1-cocycle φ will have the property that there will exists a finite Galois extension K/k such that φ is trivial on the subgroup $\mathrm{Gal}(\overline{k}/K)$. This is true because typical algebro-geometric objects and maps (such as varities and rational maps between them) are determined by a finite number of polynomials that have a finite number of coefficients. A 1-cocycle φ with this property is called to be continuous, because it is continuous with respect to the Krull topology on G and the discrete topology on $\mathrm{Aut}(X_0)$.

Now suppose that $f_1: X \to X_0$ is another $\overline{k}-$isomorphism and define $\varphi_1(\sigma) := f_1^{\sigma} f_1^{-1}$. Then

$$\begin{aligned} \left(f_1 f^{-1}\right)^{\sigma} \varphi(\sigma) &= \left(f_1 f^{-1}\right)^{\sigma} \left(f^{\sigma} f_1\right) = f_1^{\sigma} \left(f^{-1}\right)^{\sigma} f^{\sigma} f^{-1} = f_1^{\sigma} \left(f^{\sigma}\right)^{-1} f^{\sigma} f^{-1} \\ &= f_1^{\sigma} f_1^{-1} f_1 f^{-1} = \varphi_1(\sigma) \left(f_1 f^{-1}\right). \end{aligned} \tag{18.7}$$

So if $a := f^{-1} f_1 \in \mathrm{Aut}(X_0)$, then φ, φ_1 are related by

$$a^{\sigma} \varphi(\sigma) = \varphi_1(\sigma) a,\ \forall \sigma \in G.$$

Thus a twist of X_0 leads to a 1-cocycle φ in the set

$$\begin{aligned} H := \{\, \varphi: G \longrightarrow \mathrm{Aut}(X_0) \mid \varphi(\sigma\tau) = \varphi(\sigma)^{\tau} \varphi(\tau) \,\} / \sim, \\ \varphi \sim \varphi' \Leftrightarrow \exists a \in \mathrm{Aut}(X_0) : a^{\sigma} \varphi(\sigma) = \varphi'(\sigma) a. \end{aligned} \tag{18.8}$$

Suppose that X, X' are twists of X_0 that give the same element of H. This means that we fix $\overline{k}-$isomorphism $f : X \to X_0$, $f' : X' \to X_0$, then there is an element $a \in \mathrm{Aut}(X_0) : a^\sigma \varphi(\sigma) = \varphi'(\sigma) a$, where $\varphi(\sigma) = f^\sigma f^{-1}$, $\varphi'(\sigma) = f'^\sigma f'^{-1}$. Rearranging yields

$$\left(f'^{-1} a f\right)^\sigma = \left(f'^{-1} a f\right) \forall \sigma \in G.$$

In other words, the isomorphism $f'^{-1} a f : X \to X'$ is defined over k, and X, X' are the same twists of X_0. This shows that the set of twists of X_0 to the set H is injective.

In order to show this map is bijective, we need to know that every element of H corresponds to an actual twist of X_0. The basic idea is to take $\varphi \in H$, use it to construct an object X_φ, and to show that X_φ is

1/ $\overline{k}-$isomorphic to X_0,

2/ defined over k.

Let us illustrate this idea on a quasi-projective variety X_0/k. For $\varphi : G \to \mathrm{Aut}(X_0)$ a continuous 1-cocycle representing an element of H, choose a finite Galois extension K/k such that $\varphi|_{G_K} = 0$, i.e. φ factors through $G_{K/k} := \mathrm{Gal}(K/k)$.

We let $G_{K/k}$ act on $X_0 \times_k K$ by twisting the natural action via φ. Then the quotient $(X_0 \times_k K) / G_{K/k}$ is the desired object X_φ provided this quotient object does exist in the desired category. We shall indicate how to construct this quotient in the case of affine variety X_0. So suppose that X_0/k is an affine variety, $X_0 = \mathrm{Spec}(A_0)$. Thus A_0 is a $k-$algebra, and we let $A = A_0 \otimes_k K$ be the $K-$ algebra (obtained by extending scalars of A_0/K). Note that $K-$automorphisms of X_0 are in bijection with $K-$algebra automorphisms of A_0/K. In particular,

$$\varphi(\sigma) \in \mathrm{Aut}(X_0) \longleftrightarrow \varphi^*(\sigma) : A \longrightarrow A.$$

Define the ring $A_\varphi = A$ (as the sets), but we twist the action of $G_{K/k}$ on A_φ according to the following formula:

$$\sigma \in G_{K/k} \times \alpha \in A_\varphi \longrightarrow \sigma.\alpha := \varphi(\sigma)^* \alpha^\sigma,$$

where $\sigma.\alpha$ denotes the action σ on $\alpha \in A_\varphi$ and α^σ denotes the action of σ on $\alpha \in A$. Let $A_\varphi^{G_{K/k}}$ be the subalgebra of A_φ of fixed elements via the action of $G_{K/k}$. Then B is an integral $k-$algebra and by Hilbert theorem it is finitely generated, hence $X_\varphi = \mathrm{Spec}(B)$ is an affine $k-$variety. Since

$$\begin{aligned} B &= A \cap K\left(X_0\right)^{G_{K/k}}, \\ K\left(X_0\right) &= k\left(X_0\right) \otimes_k K, \end{aligned} \tag{18.9}$$

we see that

$$A \simeq K \otimes_k B. \tag{18.10}$$

In other words, X_φ is $K-$isomorphic to X_0/K. Finally, we can check that the $K-$isomorphism $X \simeq X_0$ is associated to the 1-cocycle φ. This discussion leads to

Definition 38. *Let G be a (finite or topological) group acting on another (not necessarily abelian) group A. Denote the action by*

$$\begin{aligned} G \times A &\longrightarrow A, \\ (\sigma, a) &\longmapsto a^\sigma. \end{aligned} \tag{18.11}$$

The 0-th cohomology group of G acting on A is the group

$$H^0(G, A) = A^G = \{\alpha \in A \mid \alpha^\sigma = \alpha \ \textit{ for all } \sigma \in G\}$$

of elements of A fixed by every element of G. A map $\varphi : G \to A$ is called 1-cocycle from G to A if it satisfies

$$\varphi(\sigma\tau) = \varphi(\sigma)^\tau \varphi(\tau), \, \forall \sigma, \tau \in G.$$

Two 1-cycles φ, φ' are said to be cohomologous if there exists an $a \in A$ such that

$$a^\sigma \varphi(\sigma) = \varphi_1(\sigma) a, \, \forall \sigma \in G.$$

The set of cohomology classes under this equivalence relation is denoted $H^1(G, A)$ and called the first cohomology set of G acting on A. If G is a topological group, for example the Galois group of infinite extension, we will add the requirement that the cocycles should be continuous when A is given discrete topology.

Ex. 20. *Let X_0 be an quasiprojective variety defined over k. The there is a natural bijection between the $k-$twists of X_0 and the cohomology set $H^1\left(Gal(\overline{k}/k), \, Aut(X_0)\right)$.*

The cohomology set $H^1(G, A)$ is an example of a pointed set because it has distinguished element $\emptyset$, i.e. 0-cocycle. If the group A is abelian, $H^1(G, A)$ becomes cohomology group. More precisely, if A is abelian, $\varphi_1, \varphi_2 : G \to A$ are 1-cocycles, we define their sum

$$(\varphi_1 + \varphi_2)(\sigma) := \varphi_1(\sigma) + \varphi_2(\sigma), \, \forall \sigma \in G.$$

Clearly $\varphi_1 + \varphi_2$ is again a cocycle, i.e. the set of cocycles forms a group, often denoted by $Z^1(G, A)$ The group of coboundaries, denoted by $B^1(G, A)$, is the set of maps of the form

$$\begin{aligned} \delta : G &\longrightarrow A, \\ \sigma &\longmapsto a^\sigma - a, \text{ for all } a \in A. \end{aligned} \tag{18.12}$$

The sum of two coboundaries is coboundary and every coboundary is a cocycle, i.e. $B^1(G, A) \subseteq Z^1(G, A)$. Then

$$H^1(G, A) = Z^1(G, A)/B^1(G, A).$$

The following proposition summarizes basic properties of H^0, H^1.

Proposition 11. *Let G be a group, and let A, A' be groups on which G acts.*

1/ *Functionality: Let $f : A \to A'$ be a G homomorphism, i.e. the diagram*

$$\begin{array}{ccc} A & \longrightarrow & A' \\ \big\downarrow G & & \big\downarrow G \\ A & \longrightarrow & A' \end{array}$$

is commutative. Then f induces a natural map

$$\begin{aligned} H^1(G,A) &\longrightarrow H^1(G,A'), \\ [\varphi] &\longmapsto [f \circ \varphi]. \end{aligned} \tag{18.13}$$

If A, A' are abelian, this map is a homomorphism. Let $F : G' \to G$ be a homomorphism. Then G' acts on A via F and induces a natural map

$$\begin{aligned} H^1(G,A) &\longrightarrow H^1(G',A), \\ [\varphi] &\longmapsto [\varphi \circ F]. \end{aligned} \tag{18.14}$$

If A is abelian, this map is a homomorphism.

2/ *Inflation-restriction sequence: Let $H \subseteq G$ be a subgroup of G. Then the map $H^1(G,A) \to H^1(G,A)$ from 1/ is called restriction map. If further H is a normal subgroup of G, then G/H acts on A^H. In this case $\pi : G \to G/H$, $i : A^H \hookrightarrow A$ induces the inflation map defined by*

$$\begin{aligned} H^1(G/H, A^H) &\longrightarrow H^1(G,A), \\ [\varphi] &\longmapsto [i \circ \varphi \circ \pi]. \end{aligned} \tag{18.15}$$

The following sequence, called the inflation-restriction sequence, is exact:

$$0 \longrightarrow H^1\left(G/H, A^H\right) \xrightarrow{inf} H^1(G,A) \xrightarrow{res} H^1(H,A)$$

3/ *Long exact sequence: Let*

$$0 \longrightarrow A \xrightarrow{f} B \xrightarrow{g} C \longrightarrow 0$$

be a short exact sequence of $G-$modules, where f, g are $G-$homomorphisms. Then there is a canonical long exact sequence

$$\begin{aligned} 0 \longrightarrow H^0(G,A) &\xrightarrow{f} H^0(G,B) \longrightarrow H^0(G,C) \xrightarrow{\delta} H^1(G,A) \\ &\xrightarrow{f} H^1(G,B) \xrightarrow{g} H^1(G,C), \end{aligned} \tag{18.16}$$

where the connecting homomorphism δ is defined as follows: Let $c \in H^0(G,C)$. Choose some $b \in B : g(b) = c$. Then for any $\sigma \in G$, we have

$$g(b^\sigma - b) = g(b)^\sigma - g(b) = c^\sigma - c = 0$$

since $c \in C^G$. *Thus* $b^\sigma - b \in Ker(g) = Im(f)$, $b^\sigma - b \in B^1(G,B)$ *and the injectivity of* f *on* $B^1(G,B)$ *means that we obtain a well defined element* $f^{-1}(b^\sigma - b) \in A$. *The map*

$$\begin{aligned} G &\longrightarrow A, \\ \sigma &\longmapsto f^{-1}(b^\sigma - b), \end{aligned} \tag{18.17}$$

is a cocycle representing the cohomology class of $\delta(c)$.
If A, B, C *are abelian, the long exact sequence reduces to the short exact sequence*

$$0 \longrightarrow C^G/g(B^G) \xrightarrow{\delta} H^1(G,A) \xrightarrow{f} H^1(G,B)[g] \longrightarrow 0.$$

Ex. 21. *(Kummer sequence) Let* $G_k = Gal(\overline{k}/k)$ *and let* $\mu_m \subset \overline{k}^*$ *be the group of* $m-$*th roots of unity. The short exact sequence of* G_k-*modules*

$$\begin{aligned} 0 \longrightarrow \mu_m \longrightarrow \overline{k}^* &\xrightarrow{m} \overline{k}^* \longrightarrow 0 \\ a &\longrightarrow a^m \end{aligned} \tag{18.18}$$

induces the long exact sequence

$$0 \longrightarrow \mu_m(k) \longrightarrow k^* \xrightarrow{m} k^* \xrightarrow{\delta} H^1\left(G_k, \mu_m\right) \longrightarrow H^1\left(G_k, \overline{k}^*\right).$$

Hilbert's Theorem90 says that the last group $H^1\left(G_k, \overline{k}^*\right)$ *is trivial. This implies*

$$\delta : H^1\left(G_k, \mu_m\right) \xrightarrow{\sim} k^*/\left(k^*\right)^m$$

is an isomorphism. In particular because $\mu_m \subset k^*$, G *acts trivially on* μ_m, *so* $k^*/\left(k^*\right)^m \xrightarrow{\sim} Hom(G, \mu_m)$. *It is known that the group* $Hom(G,\mu_m)$ *classifies abelian extensions of* k *of exponent* m *via* $(f : G \to \mu_m) \to \overline{k}^{Ker\ f}$. *The isomorphism* $\delta : k^*/\left(k^*\right)^m \to Hom(G,\mu_m)$ *from* **??** *is given by*

$$\begin{aligned} \delta : a &\longrightarrow \delta a, \\ (\delta a)(\sigma) &= \frac{\alpha^\sigma}{\alpha},\ \alpha^m = a. \end{aligned} \tag{18.19}$$

Hence if $\mu_m \subset k^*$ *and if* K/k *is an abelian extension of* k *of exponent* m, *then there always exists an element* $a \in k$ *such that* $K = k\left(\sqrt[m]{a}\right)$.

Let A/k be an abelian variety. Within $\mathrm{Aut}(A)/\overline{k}$ we can identify two important subgroups:

1/ The subgroup of translations, which we identify with $A\left(\overline{k}\right)$.

2/ The subgroup of automorphisms, $\mathrm{Aut}(A,e)$, that fix the natural element $e \in A(k)$.

If A is an elliptic curve, $\mathrm{Aut}(A)$ is finite. The group $H^1\left(G_k, A\left(\overline{k}\right)\right) \subseteq H^1\left(G_k, \mathrm{Aut}(A)\right)$ naturally appears in the cohomological proof of Mordell-Weil theorem, which justify our treatment of the group of twists $H^1\left(G_k, \mathrm{Aut}(A)\right)$.

Chapter 19

Rational points on Abelian varieties

Let us recall the definition of Abelian variety.

Definition 39. *An algebraic group defined over k is a variety V/k , a point $e \in V(k)$, and a morphisms*

$$\begin{array}{ccccc} m & : & V \times V & \to & V \\ i & : & V & \to & V \end{array}$$

satisfying axioms for the group law:

(1) $m(e,x) = m(x,e) = x \quad \forall x \in V(k)\,,$

(2) $m(i(x),x) = m(x,i(x)) = e \quad \forall x \in V(k)\,,$

(3) $m(m(x,y),z) = m(x,m(y,z)) \quad \forall x,y,z \in V(k)\,.$

Definition 40. *An abelian variety is a projective variety that is also algebraic group.*

Principal goal of this section:

Theorem 34. *(Mordell–Weil) Let A/k be an abelian variety defined over a number field k. Then the group $A(k)$ of k-rational points of A is finitely generated.*

For elliptic curves this does mean – "These exists a finite set of k-rational points such that all rational points may be obtained from them by the tangent and chord process."

Theorem 3 $\iff \exists P_1, \ldots, P_r \in A(k),\ r \in \mathbb{N}_0 : A(k) = A(k)_{tors} \oplus \mathbb{Z}P_1 \oplus \cdots \oplus \mathbb{Z}P_r$.
The number $r \in \mathbb{N}_0$ is called the *rank* of abelian variety A/k, $A(k)$ is called the Mordell–Weil group. Note that $A(k)_{tors}$ is a finite abelian group, i.e. can be written as

$$\begin{aligned} A(k)_{tors} \simeq\ & (\mathbb{Z}/m_1\mathbb{Z}) \oplus \cdots \oplus (\mathbb{Z}/m_s\mathbb{Z})\ , \\ & m_i \in \mathbb{N}\, \forall i \in \{1, \ldots, s\} : m_i \,|\, m_{i+1}\, \forall i, s \leq 2 \dim A\,. \end{aligned} \tag{19.1}$$

Theorem 35. *("Weak" Mordell–Weil) Let $A(k)$ be an abelian variety defined over a number field k, let $A(k)$ be the group of k-rational points of A, and let $m \geq 2$ be an integer. Then the group $A(k)/mA(k)$ is finite.*

Proof: The proof "*Theorem* 4 $\Rightarrow$ *Theorem* 1" is based on the existence of so called Néron–Tate height $\widehat{h}$ on $A(k)$. Recall that $\widehat{h}$ is a nonnegative quadratic form $\widehat{h} : A(k) \times A(k) \to \mathbb{R}$ with the property

$$\forall C \in \mathbb{R}_+ : \{x \in A(k) \,|\, \widehat{h}(x) \leq C\} \text{ is finite.}$$

The following lemma axiomatizes the situation and completes the proof of the implication. ■

Lemma 24. *(Descent lemma) Let G be an abelian group equipped with a quadratic form $q : G \to \mathbb{R}$ such that for all $C \in \mathbb{R}_+$, the set*

$$\{x \in G \,|\, q(x) \leq C\} \textit{ is finite.}$$

Assume that for some $m \geq 2$, the group G/mG is finite. Then G is finitely generated (a G, group).

In particular, let $g_1, \ldots, g_s$ be a set of representatives for G/mG, and let $C_0 := max_i\, q(g_i)$. Then G is generated by the finite set

$$\{x \in G \,|\, q(x) \leq C_0\}\,.$$

Proof: (of Descent lemma) Observe that for all $x \in G : q(x) \geq 0$, since otherwise we would have infinitely many points with $q(x) < 0$.

$$\begin{aligned} & [\ q(x+x) = q(2x) = 4q(x) \Longrightarrow \\ & \big(q(x) < 0 \Longleftrightarrow q(2x) < 0\big),\ \text{i.e. } q(nx) < 0\ \forall n \in \mathbb{Z}\ ] \end{aligned} \tag{19.2}$$

To case notation, put

$$\begin{aligned} |x| &:= \sqrt{q(x)}\ , \\ c_0 &:= \max\nolimits_i |g_i|\,, \\ S &:= \{x \in G \,|\ |x| \leq C_0\} \end{aligned} \tag{19.3}$$

and we prove that the finite set S generates G.

Let $x_0 \in G$. If $x_0 \in S$, we are done. Otherwise, $|x_0| > c_0$, so we consider the image of x_0 in G/mG a nd choose a coset representative g_i for x_0. This means

$$x_0 = g_i + mx_1 \quad \text{for some } x_1 \in G\,. \tag{19.4}$$

We use the triangle inequality to compute

$$m|x_1| = |x_0 - g_i| \leq |x_0| + |g_i| \leq |x_0| + c_0 < 2|x_0|\,. \tag{19.5}$$

Since $m \geq 2$ by assumption, we find $|x_1| < |x_0|$.

If $x_1 \in S$, then $x_0 = g_i + mx_1$ is in the subgroup generated by S, and we are done. Otherwise we can write $x_1 = g_j + mx_2$, the same computation as above we reals $|x_2| < |x_1|$. Continuing in this way, we obtain a sequence $x_0, x_1, x_2, \dots,$ satisfying

$$|x_0| > |x_1| > |x_2| > \cdots \tag{19.6}$$

and with the property that x_0 is a (linear) combination of x_t and $g_1, \dots, g_s$. Since G has only finitely many elements of bounded size, eventually the sequence terminates with an element that is in S, which completes the proof that x_0 is a linear combination of the elements of S. Therefore, S generates G. ■

Remark 8. *The term "descent" comes from Fermat's famous "descente infinie". For example, the proof that integral solutions to $x^2 - dy^2 = 1$ are generated by one fundamental solution and $x^4 + y^4 = z^2$ has no nontrivial integral solutions can be written along the same lines of the previous proof.*

Note that $A/k\,(\mathbb{C})$, the set of complex points of abelian variety defined over k, forms a complex torus, i.e. $A/k\,(\mathbb{C}) \simeq \mathbb{C}^q/\Lambda$ for some lattice $\Lambda \subset \mathbb{C}^g$. The number $g \in \mathbb{N}_0$ is called the dimension of abelian variety. As an example, the complex points of an an elliptic curve form a torus $\mathbb{C}/\mathbb{Z}\omega_1 + \mathbb{Z}\omega_2$. Note, however, that not all complex tori are, for $g \geq 2$, abelian varieties. Because $\mathbb{Z} \in End(A/k\,(\mathbb{C}))$, the multiplication by integer $m \in \mathbb{N}$ gives an endomorphism $[m]$ (surjective):

$$\begin{aligned} \underbrace{A/k\,(\mathbb{C}) \times \cdots \times A/k\,(\mathbb{C})}_{n\times} &\longrightarrow A/k\,(\mathbb{C}) \\ \underbrace{P + P + \cdots + P}_{m\times} &\longrightarrow mP\,. \end{aligned} \tag{19.7}$$

The kernel of multiplication by m, denoted by $Ker[m]$, is a free $\mathbb{Z}/m\mathbb{Z}$–mod of rank $2\dim(A/k) = 2g : Ker[m] = \left(\frac{1}{m}\Lambda\right)/\Lambda \xrightarrow{\sim} (\mathbb{Z}/m\mathbb{Z})^{2g}$.

It follows from algebraicity of the group law that $[m] : A(\bar{k}) \to A(\bar{k})$ is surjective with finite kernel $Ker[m] =: A_m \xrightarrow{\sim} (\mathbb{Z}/m\mathbb{Z})^{2g}$. For each $x \in A(k)$, we select a point $y \in A(\bar{k}) : [m](y) = x$. Then $\forall \sigma \in Gal\left(\bar{k}/k\right)$, the point $\sigma(y) - y \in A_m$, because

$$[m]\left(\sigma(y) - y\right) = \sigma\left([m]y\right) - [m]y = \sigma(x) - x = 0\,. \tag{19.8}$$

Lemma 25. *For any finite extension k'/k, the kernel of the (natural) map $A(k)/mA(k) \to A(k')/mA(k')$ is finite.*

Proof: For k' a Galois extension over k, $G = \mathrm{Gal}\,(k'/k)$, the kernel of the map $A(k)/mA(k) \to A(k')/mA(k')$ will be denoted

$$B := (A(k) \cap mA(k'))\,/mA(k)\,. \tag{19.9}$$

For any (x mod $mA(k)$) $\in B$, we fix an element $y \in A(k')$ such that $[m]y = x$. Let us consider a map

$$\begin{aligned} f_x : G &\longrightarrow A_m(k') \\ \sigma &\longrightarrow y^\sigma - y\,, \end{aligned} \tag{19.10}$$

which is not a homomorphism (just a map of sets). We have thus defined a map

$$\begin{aligned} B &\longrightarrow SetMaps\,(G, A_m) \\ x &\longmapsto f_x \end{aligned} \tag{19.11}$$

Since G, A_m are finite sets, B is finite on the condition that this map is injective. Suppose $f_x = f_{x'}$, and let $y, y' \in A(k')$ be the points used to define $f_x, f_{x'}$. Then $f_x(\sigma) = \sigma(y) - y = \sigma(y') - y' = f_{x'}(\sigma)\ \forall \sigma \in G$, and so $\sigma(y - y') = y - y'\ \forall \sigma \in G$. This implies $y - y' \in A(k)$, i.e.

$$x - x' = [m]y - [m]y' = [m](y - y') \in mA(k)\,. \tag{19.12}$$

This means that x and x' represent the same element of B, which completes the proof. ■

Remark 9. *The previous considerations can be rephrased in terms of Galois group cohomology. In particular, $f_x : G \to A_x$ is a group 1–cocycle and it is well defined element of $H^1(k, A_m)$.*

For a fixed m, let us consider a field k such that

- A_m is contained in $A(k)$,
- μ_m (the m–th roots of unity) are contained in k (this follows, in fact, from the first point using Weil's pairing).

Definition 41. *For each $x \in A(k)$ and each $\sigma \in Gal(\bar{k}/k)$, choose some $y \in A(\bar{k})$ satisfying $[m](y) = x$ and define*

$$t\,(\sigma, x) := \sigma(y) - y\,. \tag{19.13}$$

We verify below (under the assumption $A_m \subset A(k)$) that the value $t\,(\sigma, x)$ depends on x and not on the choice of φ. The resulting map

$$t :\ Gal\left(\bar{k}/k\right) \times A\,(k) \longrightarrow A_m \tag{19.14}$$

is called Kummer pairing on A/k.

Notice the analogy with the classical Kummer pairing,

$$\begin{aligned} \mathrm{Gal}\left(\bar{k}/k\right) \times k^* &\longrightarrow \mu_m \\ (\sigma, a) &\longrightarrow \sigma(\alpha)_{\alpha^{-1}} \left(\alpha = a^{\frac{1}{m}}\right) , \end{aligned} \tag{19.15}$$

where $\sigma \mapsto (\alpha \to \sigma(\alpha))$ is a representation given by cyclotomic character. The most important properties of Kummer pairing are summarized in the following.

Theorem 36. *Assume $A_m \subset A(k)$.*

(1) The function $t(\sigma, x) = \sigma(y) - y$ described above is well–defined and gives a bilinear map $t : Gal\left(\bar{k}/k\right) \times A(k) \to A_m$.

(2) Let L be the extension of k obtained by adjoining to k the coordinates of points $y \in A\left(\bar{k}\right) : [m]y \in A(k)$. Then t induces a non–degenerate pairing

$$t : \ Gal(L/k) \times A(k)/mA(k) \to A_m\,. \tag{19.16}$$

In particular, $A(k)/mA(k)$ is finite iff L is finite extension of k.

Proof: We begin by checking that $t(\sigma, x)$ does not depend on the choice of y. So suppose that $[m]y' = [m]y = x$. Then $y' - y \in A_m \subset A(k)$, i.e.

$$(\sigma(y) - y) - (\sigma(y') - y') = \sigma(y - y') - (y - y') = 0\,. \tag{19.17}$$

Therefore, the value of $t(\sigma, x)$ depends only on σ, x and t is well–defined. The verification of bilinearity is also straightforward, so for the first variable

$$\begin{aligned} t(\sigma\sigma', x) &= y^{\sigma\sigma'} - y = y^{\sigma\sigma'} - y^{\sigma'} + y^{\sigma'} - y = (y^\sigma - y)^{\sigma'} + \left(y^{\sigma'} - y\right) \\ &= (t(\sigma, x))^{\sigma'} + t(\sigma', x) = t(\sigma, x) + t(\sigma', x)\ . \end{aligned} \tag{19.18}$$

The last equality $(t(\sigma, x))^{\sigma'} = t(\sigma, x)$ is true because $t(\sigma, x) \in A_m \subset A(k)$, i.e. $t(\sigma, x)$ is Galois–invariant.

The linearity in the second variable follows from

$$\begin{aligned} t(\sigma, x + x') &= (y + y')^\sigma - (y + y') = (y^\sigma - y) + (y'^\sigma - y') \\ &= t(\sigma, x) + t(\sigma, x') \end{aligned} \tag{19.19}$$

The non-degeneracy follows from the following arguments. Since Am has exponent m, the kernel in the second variable contains $mA(k)$. Now suppose that $x \in A(k)$ is in the left kernel, i.e. $\sigma(y) = y$ for all $\sigma \in Gal\left(\bar{k}/k\right)$, and hence that $y \in A(k)$ and so $x = [m]y \in mA(k)$. Therefore, the left kernel is exactly $mA(k)$. Next we observe that an element σ is in the right kernel iff for every $y \in A\left(\bar{k}\right)$ satisfying $[m]y \in A(k)$ we have $\sigma(y) = y$. From the definition of L, this is equivalent to saying that $\sigma \in Gal\left(\bar{k}/L\right)$. Hence the right kernel is $Gal\left(\bar{k}/L\right)$, i.e. the bilinear form quotient in the first variable through $Gal\left(\bar{k}/k\right)/Gal\left(\bar{k}/L\right) \xrightarrow{\sim} Gal\left(\bar{k}/L\right)$, as stated. ■

We thus need to understand the ramification properties of field extensions of the form $k(y)/k$, where $[m]y = x \in A(k)$. Under the assumption that $A_m \subset A(k)$, the extension $k(y)$ depends only on x and is independent of y, so to simplify notation we will denote such an extension by $k\left(\frac{1}{m}x\right)$.

Lemma 26. *Assume $A_m \subset A(k)$ and $x \in A(k)$. Then the extension $k\left(\frac{1}{m}x\right)$ is Galois over k, and its Galois group is canonically isomorphic to a subgroup of A_m.*

Proof: Fix a point $y \in A\left(\bar{k}\right)$ with $[m]y = x$. We have proved that the Galois conjugates of y differ by elements of A_m, so the assumption that $A_m \subset A(k)$ implies that all of the Galois conjugates of y are already contained in $k(y)$. Thus $k(y)$ is Galois over k. Further, the map

$$\begin{aligned} Gal\,(k(y)/k) &\longrightarrow A_m \\ \sigma &\longmapsto t\,(\sigma, x) - \sigma(y) - y \end{aligned} \tag{19.20}$$

is a group homomorphism (Theorem 36, (1)), and it is injective, since σ is determined by its action on y. By this, we mean $\left(\forall y \in A\left(\bar{k}\right),\ \sigma, \sigma' \in\ Gal\,(k(y)/k)\right)$:

$$\begin{aligned} \sigma(y) - y &= \sigma'(y) - y \Rightarrow \sigma(y) = \sigma'(y) \\ &\Rightarrow \left(\sigma'^{-1}\sigma\right)(y) = y \Rightarrow \tilde{\sigma}\,(y) = y \Rightarrow \tilde{\sigma} = 1 \\ &\Rightarrow \sigma = \sigma',\ \forall \tilde{\sigma} \in Gal\,(k(y)/k)\,,\ \forall y \in A\left(\bar{k}\right) \end{aligned} \tag{19.21}$$

Note the independence of the result on the choice of $y \in A\left(\bar{k}\right)$. Hence $Gal\,(k(y)/k)$ is isomorphic to a subgroup of A_m. ■

Classical Kummer theory now tells us that $k\left(\frac{1}{m}x\right)$ is obtained by adjoining to k some m–th roots of elements of k (commutativity of $Gal\,(k(y)/k)$).

The following Theorem, which completes the arguments leading to the proof of the weak Mordell–Weil theorem, will be only stated and not proved. The reason is that it brings into the play the machinery of integral models for abelian varieties.

Theorem 37. *Let $m \geq 1$ be an integer, and let S be the (finite) set of places (valuation) of k which A has bad reduction, together with the places (valuations) that divide m. Then for all (rational) points $x \in A(k)$, the extension $k\left(\frac{1}{m}x\right)/k$, is unramified outside S. In particular, the fields described in Theorem 36, (2), is unramified outside $S \subset \mathbb{P}_k,\ \#S < \infty$.*

19.1 Models and good reduction

Let X/K be a variety defined over a field K, which is quotient field of the ring R_k. Let $S := Spec\,(R_k)$.

Definition 42. *Let K, S, X be as above. A model for (X, S) is a scheme $\mathcal{X} \to S$ whose generic fiber is isomorphic to X.*

Note that generic fiber of $\mathcal{X} \to S$ means the fiber over $(0) \in Spec\,(R_k)$. In particular for X affine, we can proceed very explicitly. Suppose the ideal defining $X/\mathbb{Q}$ in $\mathbb{A}^n/\mathbb{Q}$ is generated by polynomials $P_1/\mathbb{Q}, \cdots, P_r/\mathbb{Q}$. Clearing denominators, we may assume that $P_i \in \mathbb{Z}[T_1, \ldots, T_n]$. Then

$$Spec\,(\mathbb{Z}[T_1, \ldots, T_n] \,/\, (P_1, \ldots, P_r)) \to Spec\,(\mathbb{Z}) \tag{19.22}$$

gives a model for X whose special fiber at $(p) \in Spec\,(\mathbb{Z})$ is the scheme over $\mathbb{F}_p$, $Spec\left(\mathbb{F}_p[T_1, \ldots, T_n]/\left(\bar{P}_1, \ldots, \bar{P}_r\right)\right)$, defined by the equations $\bar{P}_1/\mathbb{F}_p = \cdots = \bar{P}_r/\mathbb{F}_p = 0$ in $\mathbb{A}^n/\mathbb{F}_p$. This illustrates that taking special fibers of a model makes precise the motion of "reducing a variety mod p". Of course, the structure of special fibers depends on the choice of the model $\mathcal{X}$.

Let $s \in S$ and let us denote by $\mathcal{O}_S \subset K$ the local ring obtained by localization of R_k in the ideal $I_S \subset R_k$.

Definition 43. *A smooth projective variety X/K has good reduction at $s \in S$ if there exists a projective model of $X/\mathcal{O}_S$ whose special fiber is smooth. If such a model $\mathcal{X}$ doesn't exists, we say that X has bad reduction at $s \in S$.*

Let us finally summarize all steps in the proof of the (weak) Mordell-Weil theorem.

(A) Let L be the field obtained by adjoining to k the coordinates of the point $Q \in A\left(\bar{k}\right)$ satisfying $mQ \in A(k)$ ("division" the points in $A(k)$ by m). Then a general argument of Galois theory, which works over any field, shows that $A(k)/mA(k)$ is finite iff the fields L is a finite extension of k.

(B) If we assume, as we may, that all of the m–torsion pints of A are k–rational, then L/k will be an abelian extension of k of exponent m, that is $Gal\,(L/k)$ is abelian and every element of $Gal\,(L/k)$ has order dividing m. Using Kummer theory or Hermite's theorem, we realize that an abelian extension of exponent m is a finite extension iff it is unramified outside a finite set of primes.

(C) The proof is reduced to the study of ramified primes in the extension L/k. The result is that L/k is unramified outside the places of bad reduction of abelian variety A and the places dividing m.

This completes the strategy of the proof.

Chapter 20

Effective computation of the Mordell-Weil group

All (classical) statements of Diophantine geometry, e.g. Mordell-Weil theorem, Roth's theorem, Siegel's and Falting's theorems etc., are purely qualitative. That is, they merely assert that certain sets, e.g. of generators, numbers, valuations, are finite. A challenge is to make these statements effective, which means to give an effective procedure for computing all of the elements in the finite set.

Let A/k be an abelian variety of dimension g, i.e. $\dim_k A/k = g$. There is an effective upper bound for the rank of $A(k), A(k) \simeq A(k)_{\text{tors.}} \oplus \mathbb{Z}^{\text{rank}\{A(k)\}}$, in terms of k, g and the places of bad reduction of A, but there is no effective procedure for computing the rank exactly. The torsion subgroup of $A(k)$ is much easier to deal with, and there is an effective algorithm to compute it.

Ex. 22. *$E/\mathbb{Q} : y^2 = x^2 + Ax + B$, $A, B \in \mathbb{Z}$. The Luts-Nagel theorem asserts that every torsion point $P = (x, y) \in E(\mathbb{Q})_{tors.}$ has $x, y \in \mathbb{Z}$ and moreover, either $y = 0$ or $y^2 \mid (4A^3 + 27B^2)$.*
Let E/k be an elliptic curve defined over a number field k. We write C_m for a cyclic group of order m.

(1) Let $k = \mathbb{Q}$. Then $E(\mathbb{Q})_{tors.}$ is isomorphic to C_m with $1 \leq m \leq 10$ or 12, or to $C_2 \times C_2$ with $1 \leq m \leq 4$.

(2) For every $d \geq 1$ there is a constant C_d such that $\forall k$, $[k : \mathbb{Q}] \leq d$ and every elliptic curve E/k, we have $\#E(k)_{tors.} \leq C_d$. In particular, for each d, there are only a finite number of possible group structures for $E(k)_{tors.}$.

The proof of this theorem is modular.

We define cannonical regulator of A/k as follows. Let $\hat{A}$ be the dual abelian variety, and choose a bases $P_1, \ldots, P_r$ for $A(k)/A(k)_{\text{tors.}}$ resp. $P'_1, \ldots, P'_r$ for

$\hat{A}(k)/\hat{A}(k)_{\text{tors.}}$ (note $A, \hat{A}$ are isogenous, i.e. they have the same rank). Let $\mathcal{P}$ be a Poincare divisor on $A \times \hat{A}$, and let

$$\langle P, P' \rangle_{\mathcal{P}} = \hat{h}_{\mathcal{P}}(P, P') \text{ for } (P, P') \in A \times \hat{A},$$

be the cannonical height on $A \times \hat{A}$ w.r. to $\mathcal{P}$. Then the cannonical regulator of A/k is

$$\operatorname{Reg}(A/k) := \left| \det \left(\langle P_i, P_j' \rangle_{\mathcal{P}} \right)_{1 \leq i,j \leq r} \right|.$$

Note that we have a lattice $A(k)/A(k)_{\text{tors.}}$ inside Euclidean space $A(k) \otimes \mathbb{R} \simeq \mathbb{R}^{\text{rank}(A(k))}$ with inner product $\langle , \rangle_{\mathcal{P}}$.

It is intuitively clear that we can bound the norm of some basis of the lattice if we know the upper bound on the volume of a fundamental cell of the lattice and the lower bound for the smallest nonzero vector in the lattice. The following theorem makes it precise:

Theorem 38 (Hermite). *Let $\mathbb{V}$ be a real vector space of dimension r with Euclidean norm $\| \, . \, \|$, let $L \subseteq \mathbb{V}$ be a lattice and $Vol(L)$ be the volume of a fundamental cell for L. Then there is a basis $\{u_1, \ldots, u_r\}$ of L, $L \simeq \mathbb{Z}u_1 \oplus \ldots \oplus \mathbb{Z}u_r$, satisfying*

$$Vol(L) \leq ||u_1|| \ldots ||u_r|| \leq \left(\frac{4}{3}\right)^{\frac{r(r-1)}{2}} Vol(L).$$

Hence if the u_i's are order in increasing length, $||u_1|| \leq ||u_2|| \leq \ldots \leq ||u_r||$, then

$$||u_i|| \leq \left(\frac{4}{3}\right)^{\frac{r(r-1)}{2(r-i+1)}} \left(\frac{Vol(L)}{||u_1||}\right)^{\frac{1}{(r-i+1)}} \quad \text{for } 1 \leq i \leq r.$$

In particular, an upper bound on $Vol(L)$ and a nonzero lower bound for $||u||$ for non-zero vectors $u \in L$ gives an upper bound for the length of a basis of L.

Thus we need a lower bound for $\hat{h}_{\mathcal{P}}(P)$ and an upper bound for $\operatorname{Reg}_{\mathcal{P}}(A/k)$. The first bound is manageable, but there is no proven algorithm to compute an upper bound for the regulator $\operatorname{Reg}(A/k)$. However, there is a conjectural approach via zeta functions and related analytic techniques.

Let $A/\mathbb{Q}$ be an abelian variety of dimension g. For each prime p, choose a prime $l \neq p$, and define the Tate module of A by

$$T_l(A) = \lim_{\substack{\longleftarrow \\ n}} A[l^n]$$

relative to the maps $A[l^{n+1}] \xrightarrow{[l]} A[l^n]$. Let $V_l(A) = T_l(A) \otimes_{\mathbb{Z}_l} \mathbb{Q}_l$. Then $T_l(A) \simeq \mathbb{Z}_l^{2g}$, $V_l(A) \simeq \mathbb{Q}_l^{2g}$. Moreover, there is natural action of the Galois group $\operatorname{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ on these sets (induced by $l \neq p$):

$$\rho_l : \operatorname{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \longrightarrow \operatorname{Aut}_{\mathbb{Q}_l}(V_l(A)) \xrightarrow{\sim} \operatorname{GL}(2g, \mathbb{Q}_l).$$

The map ρ_l is the $l-$adic representation attached to $A/\mathbb{Q}$. For any prime β over p, i.e. $p\mathcal{O}_k = \beta_1^{e_1} \dots \beta_k^{e_k}$ for some $[K:\mathbb{Q}] < \infty$, we let D_p resp. I_p denote the decomposition and inertia groups of p. Up to conjugation in $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$, D_p and I_p are independent of the choice of β. Thus

$$D_p := \left\{\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}),\, \sigma(\beta) = \beta\right\},\; I_p := \mathrm{Ker}\left(D_p \longrightarrow \mathrm{Gal}\left(\overline{\mathbb{F}}_p/\mathbb{F}_p\right)\right).$$

The reduction map $D_p \longrightarrow \mathrm{Gal}\left(\overline{\mathbb{F}}_p/\mathbb{F}_p\right)$ is surjective, and we let Frob_p denote $\geq n$ elements of D_p that maps to the Frobenius element $\mathrm{Fr}_p : \alpha \mapsto \alpha^p$, $\alpha \in \overline{\mathbb{F}}_p$. In other words, Fr_p topologically generates $\mathrm{Gal}\left(\overline{\mathbb{F}}_p/\mathbb{F}_p\right)$ and Frob_p is well defined up to an element of I_p and up to conjugation.

Let $V_l(A)^{I_p} \subseteq V_l(A)$ be the subspace of $V_l(A)$ fixed by all elements of I_p. Then the action of Frob_p on $V_l(A)^{I_p}$ is well defined up to conjugation, i.e. its characteristic polynomial

$$Q_p(t) := \det\left(1 - \rho_l(\mathrm{Frob}_p)|_{V_l(A)^{I_p}}\, t\right)$$

is independent of all choices involved.

The $L-$series of $A/\mathbb{Q}$ is the Dirichlet series given by the product

$$L(A/\mathbb{Q}, s) = \sum_{n=1}^{\infty} a_n n^{-s} = \prod_p Q_p\left(p^{-s}\right)^{-1}.$$

We remark that if A has good reduction at p, then the action of I_p on $V_l(A)$ is trivial, thus for all but finite number of primes p we have $V_l(A)^{I_p} = V_l(A)$, $\deg Q_p(t) = 2g$. This follows from the fact that if A has good reduction at p, then the reduction map $A[l^n] \to A(\mathbb{F}_\beta)$ is injective. It is also not at all obvious that $Q_p(t)$ is independent of the choice of auxiliary prime $l \neq p$. In the case of good reduction of A at p the Weil's estimate says that $Q_p(t)$ factors over $\mathbb{C}$ as $Q_p(t) = \prod_{i=1}^{2g}(1 - \alpha_i t)$, $|\alpha_i| = \sqrt{p}$. This implies that the product defining $L(A/\mathbb{Q}, s)$ converges for $\mathrm{Re}(s) > \frac{3}{2}$. Conjecturally, more is true:

Conjecture 1.

1/ The $L-$series $L(A/\mathbb{Q}, s)$ has an analytic continuation to all $s \in \mathbb{C}$.

2 There is an integer N, called conductor of A and divisible by exactly the primes of bad reduction of A, such that

$$\bigwedge(A/\mathbb{Q}, s) := N^{\frac{s}{2}}\left((2\pi)^{-s}\,\Gamma(s)\right)^g L(A/\mathbb{Q}, s)$$

satisfies the functional equation

$$\bigwedge(A/\mathbb{Q}, 2-s) := \epsilon \bigwedge(A/\mathbb{Q}, s)$$

for some $\epsilon = \pm 1$ called the sign.

We will ask for analytic behavior of $L(A/\mathbb{Q},s)$ near some special value of s, for example $s=1$. First some notation. The real period of A is the integral $\Omega_A := \left|\int_{A(\mathbb{R})} \eta_A\right|$ of a Néron's differential η_A, i.e. differential normalized to have finite non-zero reduction on every fiber of the Néron model of A. For each prime p, let $A^0(\mathbb{Q}_p) \subseteq A(\mathbb{Q}_p)$ denote the subgroup of $A(\mathbb{Q}_p)$ that reduces to the identity component of the Néron model of A, and let c_p be the index of $A^0(\mathbb{Q}_p)$ in $A(\mathbb{Q}_p)$. In particular, $c_p = 1$ for primes of good reduction, so $c_p = 1$ for all but finitely many primes. We assume that $Ш(A(\mathbb{Q}))$, the Tate-Shafarevich group of $A/\mathbb{Q}$, is finite.

Conjecture 2. *(Birch+Schwinnerton-Dyer) Assume that $L(A/\mathbb{Q},s)$ admits an analytic continuation to $\mathbb{C}$.*

1/ The order of vanishing of $L(A/\mathbb{Q},s)$ at $s=1$ is $ord_{s=1} L(A/\mathbb{Q},s) = rank(A(\mathbb{Q}))$.

2/ Let $r = rank(A(\mathbb{Q}))$. Then the leading coefficient of the Taylor expansion of $L(A/\mathbb{Q},s)$ around $s=1$ is

$$L^*(A/\mathbb{Q},1) := \lim_{s\to 1} \frac{L(A,s)}{(s-1)^r} = \Omega_A \Big(\prod_p c_p\Big) \frac{\#Ш(A/\mathbb{Q}) Reg(A/\mathbb{Q})}{\#A(\mathbb{Q})_{tors.} \#\hat{A}(\mathbb{Q})_{tors.}}.$$

The sign of the functional equation **??** *is then $\epsilon = (-1)^{rank(A(\mathbb{Q}))}$, giving a comparatively easy (conjectural) analytic way to decide the parit of the rank.*

The conjecture of Birch+Schwinnerton-Dyer may be viewed as an analogue of the classical formula for the residue of the Dedekind zeta function $\zeta_k(s)$ of a number field k, $[k:Q] < \infty$. Let H_k be the class group of k, D_k the absolute value of the discriminant of k, let r_1 resp. r_2 be the number of real resp. pairs of complex conjugate embeddings of k, and μ_k be the group of roots of unity in k. Then

$$\lim_{s\to 1} (s-1)\zeta_k(s) = \frac{2^{r_1}(2\pi)^{r_2}}{\sqrt{D_k}} \frac{\#H_k \mathrm{Reg}_k}{\#\mu_k}.$$

There is the following list of (not perfect) associations:

Number field	$\longleftrightarrow$	Abelian variety
R_k^*	$\longleftrightarrow$	$A(k)$
$\mu_k = (R_k^*)_{\text{tors.}}$	$\longleftrightarrow$	$A(k)_{\text{tors.}}$
Reg_k	$\longleftrightarrow$	$\mathrm{Reg}(A/k)$
H_k	$\longleftrightarrow$	$Ш(A/k)$

(20.1)

Chapter 21

Riemann surfaces

A Riemann surfaces is a geometric object X locally isomorphic to an open subset of $\mathbb{C}$. These local pieces are glued together so that one can work with holomorphic resp. meromorphic functions and (1–)differential globally on X. The standard examples of Riemann surfaces are $\mathbb{P}^{-1}(\mathbb{C}), C(\mathbb{C})$ (= complex points of the circle), $\mathbb{C}/2\pi i\mathbb{Z}$ (= a cylinder), $\mathbb{C}/\mathbb{Z}+\mathbb{Z}i$ (= a torus). Here is the standard definition.

Definition 44. *A Riemann surface X is a connected Hausdorff topological space with countable basis of open sets, equipped with an equivalence class of holomorphic atlases. An atlas on X consists of a set of local charts $(U_\alpha, \varphi_\alpha)$, where*

(A) $\{U_\alpha\}_\alpha$ *is an open covering of* X,

(B) $\varphi_\alpha : U_\alpha \xrightarrow{\sim} \varphi_\alpha(U_\alpha)$ *is a homeomorphism between* U_α *and a domain* $\varphi_\alpha(U_\alpha) \subset \mathbb{C}$.

The local charts are required to be compatible in the sense that $\forall$ pair of local charts $(U_\alpha, \varphi_\alpha), (U_\beta, \varphi_\beta)$, the transition function

$$\varphi_\beta \circ \varphi_\alpha^{-1} : \varphi_\alpha(U_\alpha \cap \varphi_\beta) \longrightarrow \varphi_\beta(U_\alpha \cap \varphi_\beta) \tag{21.1}$$

is holomorphic. Two atlases are equivalent if their union is also an a atlas.

Definition 45. *Let X be a Riemann surface. A local coordinante at a point $x \in X$ is a local chart (U_α, z_α) satisfying*

(A) $x \in U_\alpha$,

(B) $z_\alpha(x) = 0, \quad dz_\alpha(x) \neq 0.$

Ex. 23. *(1) One can replace $\mathbb{C}$ by $\mathbb{C}^n$. Then the geometric object is called a complex manifold of dimension n.*

(2) If Z_α is a local coordinate at $x \in X$, any other local coordinate is given by power series $\sum_{n\geq 1} c_n z_\alpha^n$ with non–zero radius of convergence and $c_1 \neq 0$.

(3) An open connected subset $U \subseteq \mathbb{C}$ is a Riemann surface, with one chart $U \hookrightarrow \mathbb{C}$ given by inclusion. For each $a \in U$, $z_\alpha(z) = z - a$ is a local coordinate at $a \in U$.

(4) $X = \mathbb{P}^1(\mathbb{C})$ is a compact Riemann surface, with two charts (U_1, φ_1), (U_2, φ_2) :

$$\begin{array}{ll} U_1 = X\backslash\{\infty\}, & \varphi_1 : \; U_1 \xrightarrow{\sim} \mathbb{C}\,, \\ U_2 = X\backslash\{0\} & \qquad\; z \mapsto z\,. \\ & \varphi_2 : \; U_2 \xrightarrow{\sim} \mathbb{C}\,, \\ & \qquad\; z \mapsto \frac{1}{z}\,. \end{array} \tag{21.2}$$

The intersection $U_1 \cap U_2 = \mathbb{C}^*$, which means that X is obtained from two copies of $\mathbb{C}$ glued along $\mathbb{C}^*$ by $z \mapsto \frac{1}{z}$. For $x = a \in \mathbb{C}$ resp. $x = \infty$, $z_\alpha(z) = z - a$ resp. $z_\alpha(z) = \frac{1}{z}$ is a local coordinate at x.

21.1 Maps between Riemann surfaces

Definition 46. *A map $f : X \to Y$ between Riemann surfaces X, Y is holomorphic at a point $x \in X$ if there exist local charts $(U_\alpha, \varphi_\alpha)$, $x \in U_\alpha$ on X and (V_β, ψ_β), $f(x) \in V_\beta$ on Y such that the function*

$$\psi_\beta \circ f \circ \varphi_\alpha^{-1} : \; \varphi_\alpha(U_\alpha) \longrightarrow \psi_\beta(V_\beta) \tag{21.3}$$

is holomorphic at $\varphi_\alpha(x)$. The map f is holomorphic if it is holomorphic at all points $x \in X$.

Remark 10. *Note that f is holomorphic (at x) $\Rightarrow$ it is continuous (at x).*

Definition 47. *A holomorphic function on a Riemann surface X is a holomorphic map $f : X \to \mathbb{C}$. Denote by $\mathcal{O}(x)$ the set of holomorphic functions on X (it is a commutative ring containing $\mathbb{C}$).*

Note that if Y is a Riemann surface, X a topological space and $f : X \to Y$ an unramified covering, then there exists a unique structure of Riemann surface on X for which f is a holomorphic map. Similarly, if Y is a Riemann surface and G a group of holomorphic automorphisms of Y satisfying

$$(\forall y \in Y)\,(\exists U \ni y \text{ open})\,(\forall g \in G\backslash\{e\}) : \; g(U) \cap U = \{0\}\,, \tag{21.4}$$

then the projection $f : Y \to G\backslash Y = X$ is an unramified covering and there exists a unique structure of a Riemann surface on X, equipped with the quotient topology, for which f is a holomorphic map.

Ex. 24. *This applies, in particular, to quotients $f : \mathbb{C} \to \mathbb{C}/L$ of $\mathbb{C}$ by discrete additive subgroups, i.e. by $L = \mathbb{Z}u$ or $L = \mathbb{Z}u + \mathbb{Z}v$, $u, v \in \mathbb{C}$ linearly independent over $\mathbb{R}$.*

Definition 48. *A meromorphic function on a Riemann surface X is a holomorphic map $f : X \to \mathbb{P}^1(\mathbb{C})$ such that $f(X) \neq \{\infty\}$. Denote by $\mathcal{U}(X)$ the set of meromorphic functions on X (it is a field containing $\mathbb{C}$).*

If $X \subset \mathbb{C}$ is a domain, this definition is equivalent to the usual one. If (U_α, z_α) is a local coordinate at $x \in X$ and $f \in \mathcal{U}(X)$, then $f \circ z_\alpha^{-1}$ has a Laurent expansion

$$\left(f \circ z_\alpha^{-1}\right)(z) = \sum_{n \geq n_0,\ n \in \mathbb{Z}} a_n z^n\,, \tag{21.5}$$

converging in a punctured disc $\{z \in \mathbb{C} \,|\, 0 < |z| < r\}$.

Definition 49. *The order of vanishing a non–zero meromorphic function $f \in \mathcal{U}(X) \backslash \{0\}$ at $x \in X$ is defined as*

$$ord_x(f) = \min\{n \in \mathbb{Z} \,|\, a_n \neq 0\} \in \mathbb{Z}\,. \tag{21.6}$$

The integer $ord_x(f)$ does not depend on the choice of a local coordinate; f is holomorphic at $x \Leftrightarrow ord_x(f) \geq 0$.

Ex. 25. *Let $X = \mathbb{P}^1(\mathbb{C})$, $f(z) = \prod_j (z - a_j)^{n_j}$, where $a_j \in \mathbb{C}$ are distinct and $n_j \in \mathbb{Z}$. The description of local coordinates on X together with*

$$f(z) = \left(\frac{1}{z}\right)^{-\sum_j n_j} \prod_j \left(1 - \frac{a_j}{z}\right)^{n_j} \tag{21.7}$$

imply that

$$ord_{a_j} = n_j\,, \quad ord_\infty(f) = -\sum_j n_j\,. \tag{21.8}$$

Note that ord_x is a discrete valuation: if $f, g \in \mathcal{U}(X) \backslash \{0\}$, then

$$\begin{aligned} ord_x(fg) &= ord_x(f) + ord_x(g)\,, \\ ord_x(f+g) &= \min(ord_x(f), ord_x(g))\,. \end{aligned} \tag{21.9}$$

If $f \in \mathcal{U}(X) \backslash \{0\}$, then the set $Z(f) = \{x \in X \,|\, ord_x(f) \neq 0\}$ is a closed discrete (= the induced topology on $Z(f)$ is discrete) subset of X. In particular, if X is compact, then $Z(f)$ is finite. If $g, h \in \mathcal{U}(X)$ satisfy $g(x) = h(x)$ for all $x \in A$, $A \subseteq X$ is closed non–discrete subset of X, then $g = h$ (apply the previous remark to $f = g - h$). If $f : X \to Y$ is a non–constant holomorphic map and $g : Y \to \mathbb{P}^1(\mathbb{C})$ a meromorphic function on Y, then $f^*(g) = g \circ f : X \to \mathbb{P}^1(\mathbb{C})$ is a meromorphic function on X. The map $f^* : \mathcal{U}(Y) \to \mathcal{U}(X)$ is an embedding of fields (over $\mathbb{C}$).

Definition 50. *Let $f : X \to Y$ be a non-constant holomorphic map between Riemann surfaces and $x \in X$. Then there exist local coordinates z_α (resp. z_β) at x (resp. $f(x) \in Y$) such that*

$$\left(z_\beta \circ f \circ z_\alpha^{-1}\right)(z) = z^e\,, \tag{21.10}$$

where $e = e_x \geq 1$ is an integer, called ramification index of f at x (it does not depend on any choices). The ramification points of f are the points $x \in X$ with $e_x > 1$. They form a discrete subset of X.

Lemma 27. *A non–constant holomorphic map between Riemann surfaces i open.*

Lemma 28. *If X is a compact Riemann surface, then $\mathcal{O}(x) = \mathbb{C}$.*

Proof: If not, then there is a non–constant holomorphic map $f : X \to \mathbb{C}$; its image $f(X) \subset \mathbb{C}$ is both compact and open, which is imposible. ■

As a corollary we get that $f : X \to Y$ is bijective, then $e_x = 1$ for every $x \in X$ and $f^{-1} : Y \to X$ is holomorphic.

Lemma 29. *Let $f : X \to Y$ a non–constant holomorphic map between Riemann surfaces. Assume, in addition, that f i proper, i.e. $f^{-1}(K) \subset X$ is compact for every compact subset $K \subset Y$ (this folds, for example, if both X, Y are compact). Then there is an integer $deg(f) \geq 1$ ("the degree of f") such that*

$$(\forall y \in Y) \sum_{x \in f^{-1}(y)} e_x = deg(f)\,. \tag{21.11}$$

If $e_x = 1$ for all $x \in X$, then f is an unramified covering.

Ex. 26. *If $X = Y = \mathbb{C}$ and $f(z) = z^2$, then $e_x = 1$ resp. $e_x = 2$ for $z \neq 0$ resp. $z = 0$, and $deg(f) = 2$.*

Ex. 27. *If X is compact, $f : X \to \mathbb{P}^1(\mathbb{C})$ is a non–constant meromorphic function and $y = 0$ (resp. $y = \infty$), then $e_x = ord_x(f)$ (resp. $e_x = -ord_x(f)$) for each $x \in f^{-1}(y)$. In particular,*

$$deg(f) = \sum_{f(x)=0} ord_x(f) = -\sum_{f(x)=\infty} ord_x(f)\,. \tag{21.12}$$

21.2 Holomorphic and meromorphic differentials

Let X be a Riemann surface with an atlas $\{(U_\alpha, \varphi_\alpha)\}$. A holomorphic function $f : X \to \mathbb{C}$ defines, for each α, a holomorphic function $f_\alpha = f \circ \varphi_\alpha^{-1} \in \mathcal{O}(\varphi_\alpha(U_\alpha))$. On $\varphi_\alpha(U_\alpha \cap U_\beta)$ they satisfy the compatibility condition

$$f_\beta \circ \psi_{\alpha\beta} = f_\alpha\,, \tag{21.13}$$

where $\psi_{\alpha\beta} = \varphi_\beta \circ \varphi_\alpha^{-1}$ denotes the transition function. Writing z_α for the standard coordinate on $\mathbb{C} \supset \varphi_\alpha(U_\alpha)$, the compatibility condition reads

$$f_\alpha(z_\alpha) = f_\beta(z_\beta) = f_\beta(\psi_{\alpha\beta}(z_\alpha)) \,. \tag{21.14}$$

Meromorphic functions on X admit an analogous description with $f_\alpha \in \mathcal{U}(\varphi_\alpha(U_\alpha))$.

Definition 51. *A holomorphic differential ω on X is defined by a collection of holomorphic functions $g_\alpha \in \mathcal{O}(\varphi_\alpha(U_\alpha))$ such that the formal expressions $\omega_\alpha = g_\alpha(z_\alpha)dz_\alpha$ are compatible on $\varphi_\alpha(U_\alpha \cap U_\beta)$ as follows:*

$$\begin{aligned} g_\alpha(z_\alpha)dz_\alpha &= g_\beta(\psi_{\alpha\beta}(z_\alpha))dz_\beta \\ &= g_\beta(\psi_{\alpha\beta}(z_\alpha))\psi'_{\alpha\beta}(z_\alpha)dz_\alpha \,, \end{aligned} \tag{21.15}$$

i.e. $g_\alpha = (g_\beta \circ \psi_{\alpha\beta})\, \psi'_{\alpha\beta}$. The set of holomorphic differentials on X will be denoted by $\Omega^1(X)$ (it is an $\mathcal{O}(X)$–module).

Definition 52. *A meromorphic differential (form) on X is defined by a collection of meromorphic functions $g_\alpha \in \mathcal{U}(\varphi_\alpha(U_\alpha))$ satisfying the same compatibility condition as in Eg. (↑???). Meromorphic differentials form a vector space over $\mathcal{U}(X)$, which will be denoted by $\Omega^1_{mer}(X)$.*

Ex. 28. *If $f \in \mathcal{O}(X)$ resp. $f \in \mathcal{U}(X)$ is given by the collection $f_\alpha(z_\alpha)$ as in Eq.(↑???), then the collection of functions $g_\alpha = f'_\alpha(z_\alpha)$ defines a differential (form) $df \in \Omega^1(X)$ resp. $\Omega^1_{mer}(X)$, for which $(df)_\alpha = f'_\alpha(z_\alpha dz_\alpha) = df_\alpha$*

Ex. 29. *If $f : X \to X$ is a holomorphic map and $\omega \in \Omega^1(X)$, one can pull-back $f^*(\omega) \in \Omega^1(Y)$ as follows: let $\{(U_\alpha, \varphi_\alpha)\}_\alpha$ be an atlas of X and assume that ω is given by a collection $g_\alpha \in \mathcal{O}(\varphi_\alpha(U_\alpha))$ as in Eq. (↑???). Choose an atlas $\{(U_\beta, \varphi_\beta)\}_\beta$ of Y such that, for each β, $f(V_\beta) \subset U_\alpha$ for some $\alpha = j(\beta)$. In terms of the standard coordinates z_β on V_β (resp. $z_\beta = z_{j(\beta)}$) on $U_\alpha = U_{j(\beta)}$, the map f is defined by the formula $z_\alpha = f_\beta(z_\beta)$, where $f_\beta = \varphi_\alpha \circ f \circ \psi_\beta^{-1}$. The differential $f^*(\omega)$ is then given by the collection of functions $\left(g_{j(\beta)} \circ f_\beta\right) f'_\beta \in \mathcal{O}\left(\psi_\beta(U_\beta)\right)$. The same construction works for meromorphic differentials as well. In particular, $f^*(dh) = d(h \circ f)$ for any $h \in \mathcal{U}(X)$.*

Definition 53. *Let $\omega \in \Omega^1_{mer}(X)\backslash\{0\}$ and $x \in X$. Choose a local coordinate (U_α, z_α) at x and write $\omega_\alpha = f_\alpha(z_\alpha)dz_\alpha$,*

$$f_\alpha(z_\alpha) = \sum_{n \geq n_0}^{\infty} a_n z_\alpha^n \,. \tag{21.16}$$

The order of zero of ω and its residue are defined as

$$ord_x(\omega) = ord_x(f_\alpha), \quad res_x(\omega) = a_{-1} \,. \tag{21.17}$$

It is easy to see that both $ord_x(\omega)$, $res_x(\omega)$ are independent of the choice of a local coordinate.

Ex. 30. *For $X = \mathbb{P}^1(\mathbb{C})$ and $\omega = dz$ (where z is the standard coordinate on $\mathbb{C} \simeq X \backslash \{\infty\}$), $\omega = d(z-a)$ for every $a \in \mathbb{C}$, hence $ord_a(dz) = 0$. Taking $u = \frac{1}{z}$ as a local coordinate at $\infty \in X$, the identity $dz = -u^{-2}du$ shows that $ord_\infty(dz) = -2$.*

Lemma 30. *If $f \in \mathcal{U}(X)\backslash\{0\}$ and $ord_x(f) \neq 0$, then $ord_x(df) = ord_x(f) - 1$.*

Proof: In local chart with local coordinate z_α at x, we have $f_\alpha(z_\alpha) = \sum_{n \geq m} a_n z_\alpha^n$, where $m = ord_x(f) \neq 0$ and $a_m \neq 0$. Then $(df)_\alpha = \sum_{n\geq m} n a_n z_\alpha^{n-1} dz_\alpha$, hence $ord_x(df) = m - 1$. ∎

Theorem 39. *(Residue Theorem) If X is a compact Riemann surface and $\omega \in \Omega^1_{mer}(X)\backslash\{0\}$, then $\sum_{x\in X} res_x \omega = 0$.*

Corollary 13. *If X is a compact Riemann surface and $f \in \mathcal{U}(X)\backslash\{0\}$, then*

$$\sum_{x\in X} ord_x(f) = 0\,. \tag{21.18}$$

Proof: The meromorphic differential $\omega = \frac{df}{f}$ satisfies $res_x(\omega) = ord_x(f)\ \forall x \in X$. ∎

Lemma 31. *If $f : X \to Y$ is a non–constant holomorphic map between Riemann surfaces, $x \in X$ and z_β a local coordinates at $f(x) \in Y$, then $ord_x\left(f^*(dz_\beta)\right) = e_x - 1$.*

Proof: If f is given in a local chart by $z_\beta = z_\alpha^{e_x}$, where z_α is a local coordinate at x and z_β a local coordinate at $f(x)$. Hence

$$ord_x\left(f^*(dz_\beta)\right) = ord_x\left(d(z_\alpha^{e_x})\right) = ord_x\left(e_x z_\alpha^{e_x - 1} dz_\alpha\right) = e_x - 1 \tag{21.19}$$

∎

Lemma 32. *Let X be a Riemann surface. If $\omega_1, \omega_2 \in \Omega^1_{mer}(X)\backslash\{0\}$, then there exists a meromorphic function $f \in \mathcal{U}(X)\backslash\{0\}$ such that $\omega_1 = f\omega_2$.*

Proof: If ω_1, ω_2 ar given locally by (non–zero) meromorphic functions $g_{1,\alpha}, g_{2,\alpha}$ satisfying the compatibility condition. Then the quotients $\left(\frac{g_{1,\alpha}}{g_{2,\alpha}}\right)_\alpha$ define a non–zero meromorphic function f. Thus $\omega_1 = f\omega_2$. ∎

Theorem 40. *Let X be a Riemann surface. Then $\mathcal{U}(X) \neq \mathbb{C}$ and $\Omega^1_{mer}(X) \neq \{0\}$. For every Riemann surface X, the vector space $\Omega^1_{mer}(X)$ is 1–dim $\mathcal{U}(X)$–module.*

Let X be a compact Riemann surface. The dimension of the space of holomorphic differentials

$$g_{an}(X) := \dim_{\mathbb{C}} \Omega^1(X) \tag{21.20}$$

is referred to as the analytic genus of X. It follows from Riemann–Roch theorem that

$$deg(\dim(\omega)) = 2g_{an}(X) - 2 \quad \forall \omega \in \Omega^1_{mer}(X)\backslash\{0\}\,. \tag{21.21}$$

21.3 Implicit function theorem

Ex. 31. *Consider the circle $C : f(x,y) = x^2 + y^2 - 1 = 0$. As $\frac{\partial f}{\partial x}(0,1) = 0$, the tangent to C at (0,1) is zero. Moreover, for every open U, $(0,1) \in U$ (either in $\mathbb{R}^2$ or $\mathbb{C}^2$), $U \cap C$ ($C = C(\mathbb{R}), C(\mathbb{C})$) is not a graph of any function $y \mapsto (x(y))$, because there are two possible values of x for y arbitrarily close 1. On the other hand, it is given by a graph of a function $x \mapsto y(x)$ (for sufficiently small U). This is special case of the following result.*

Theorem 41. *(Theorem on implicit function – holomorphic version) Let $U \subset \mathbb{C}^2$ be an open set, $f \in \mathcal{O}(U)$ a holomorphic function of $(x,y) \in U$ and $Z = \{(x,y) \in U \,|\, f(x,y) = 0\}$ its set of zeroes. Assume that $P = (x_P, y_P) \in Z$ is a point satisfying $\frac{\partial f}{\partial x}(P) \neq 0$. Then there exists an open set $V \subseteq U$, $P \in V$, such that $\frac{\partial f}{\partial x}(Q) \neq 0$ $\forall Q \in Z \cap V$, the horizontal projection*

$$\begin{aligned} p_2 : Z \cap V &\longrightarrow p_2\,(Z \cap V) \\ (x,y) &\longmapsto y, \quad y_P \in p_2\,(Z \cap V)\,. \end{aligned} \tag{21.22}$$

is a homeomorphism and its inverse is given by $y \mapsto (x(y), y)$, where $x(y)$ is a holomorphic function on the open set $p_2\,(Z \cap V) \ni y_P$.

This theorem can be generalized to a system of holomorphic equations

$$f_1(z_1, \ldots, z_n) = \quad \ldots \quad = f_m(z_1, \ldots, z_n) = 0 \quad (m < n)\,. \tag{21.23}$$

21.4 Orientation of Riemann surfaces

Let V be a real vector space, $\dim V < \infty$. The set $F(V)$ of (ordered) bases of V is a principal homogeneous space of $GL(V)$, i.e. $\forall u, v \in F(V)$ $\exists! g \in GL(V)$ satisfying $g(u) = v$. This equips $F(V)$ with natural topology. By definition, two bases u, v define the same orientation of V iff u, v lie in the same connected component of $F(V)$, i.e. iff $v = g(u)$ with $g \in GL(V)^0$ contained in the connected component of the identity of $GL(V)$, i.e. iff $det(g) > 0$. Equivalently we can fix a volume element ω on V, i.e. $\omega \in \Lambda^{TOP} V^*$, $\omega \neq 0$. Then $u = \{u_1, \ldots, u_n\} = v\{v_1, \ldots, v_n\}$ define the same orientation of V iff $\omega(u_1, \ldots, u_n) = \omega(v_1, \ldots, v_n)$ have the some sign.

The standard orientation of $\mathbb{C}(= \mathbb{R}^2)$ is given by the ordered basis $\{1, i\}$. Let x, y be the real and imaginary part of the canonical coordinate $z = x + iy$ on $\mathbb{C}$. Then the standard volume element $\omega = x \wedge y$ satisfies $\omega(1, i) > 0$. Note, however, that there is not canonical choice of the orientation of $\mathbb{C}$.

If $\{(U_\alpha, \varphi_\alpha)\}_\alpha$ is an atlas of X, one can use the local charts to transport the standard orientation of $\mathbb{C}$ to X, at least infinitesimally, i.e. to the tangent spaces of X. We must check that these orientations agree on the intersections $U_\alpha \cap U_\beta$. Let us decompose the local coordinates z_α, z_β (at the same point

$x \in X$) into their real and imaginary parts $z_\alpha = x_\alpha + iy_\alpha$, $z_\beta = x_\beta + iy_\beta$. For small $\epsilon > 0$, the vectors $\epsilon, i\epsilon$ based at $0 = z_\alpha(x)$ are mapped by the transition function $\psi_{\alpha\beta} = z_\beta \circ z_\alpha^{-1}$ to

$$\begin{aligned} \epsilon &\longmapsto \left(\frac{\partial x_\beta}{\partial x_\alpha} + i\frac{\partial y_\beta}{\partial x_\alpha}\right)\epsilon + O(\epsilon^2)\,, \\ i\epsilon &\longmapsto \left(\frac{\partial x_\beta}{\partial x_\alpha} + i\frac{\partial y_\beta}{\partial x_\alpha}\right)\epsilon + O(\epsilon^2)\,. \end{aligned} \tag{21.24}$$

This implies that the infinitesimal change of orientation is given by the sign of the determinant of the non–singular Jacobian matrix

$$M = \begin{pmatrix} \frac{\partial x_\beta}{\partial x_\alpha} & \frac{\partial y_\beta}{\partial x_\alpha} \\ \frac{\partial x_\beta}{\partial y_\alpha} & \frac{\partial y_\beta}{\partial y_\alpha} \end{pmatrix}. \tag{21.25}$$

The Cauchy–Riemann equations tell us that

$$M = \begin{pmatrix} \frac{\partial x_\beta}{\partial x_\alpha} & \frac{-\partial x_\beta}{\partial y_\alpha} \\ \frac{\partial x_\beta}{\partial y_\alpha} & \frac{\partial x_\beta}{\partial y_\alpha} \end{pmatrix} \Longrightarrow \det(M) = \frac{\partial^2 x_\beta}{\partial x_\alpha^2} + \frac{\partial^2 x_\beta}{\partial y_\alpha^2} > 0\,. \tag{21.26}$$

and so two orientations are compatible. In particular, let (U_α, z_α) be a local coordinate on $X, V \subset U_\alpha$ an open subset and $f : V \to \mathbb{R}_{\geq 0}$ a non–negative (differentiable) function for which $f^{-1}(0) \subset V$ is discrete set, then $\frac{i}{2}\int_V f dz_\alpha \wedge d\overline{z}_\alpha > 0$ as $\frac{i}{2}d(x+iy) \wedge d(x-iy) = dx \wedge dy$. For $\omega \in \Omega^1(V)\backslash\{0\}$ $(\omega_\alpha = f_\alpha(z_\alpha)dz_\alpha)$, then

$$\frac{i}{2}\int_V \omega \wedge \bar{\omega} = \frac{i}{2}\int_V |f_\alpha(z_\alpha)|^2\, dz_\alpha \wedge d\overline{z}_\alpha\,. \tag{21.27}$$

21.5 Genus and the Riemann–Hurwitz formula

Let X be a compact Riemann surface. Because X is orientable, it is homeomorphic to a sphere with g handles. The integer $g = g(x)$ is called the (topological) genus of X. For every triangulation of X, denote by s_i the number of simplices of dimension $i = 0, 1, 2$ in the triangulation. Then $s_0 - s_1 + s_2 = 2 - 2g(x)$. Using suitably compatible triangulations on X and Y, it is easy to prove the following theorem.

Theorem 42. *(Riemann–Hurwitz formula) Let $f : X \to Y$ be a non–constant holomorphic map between compact Riemann surfaces. Then*

$$2g(X) - 2 = (2g(Y) - 2)\ deg(f) + \sum_{x \in X}(e_x - 1)\,. \tag{21.28}$$

Ex. 32. *If X is a compact Riemann surface and $f : X \to \mathbb{P}^1(\mathbb{C})$ is a holomorphic map of degree $deg(f) = 2$, then*

$$2g(x) - 2 = -4 + |s|, \quad s = \{x \in X \,|\, e_x = 2\} = \{x \in X \,|\, e_x \neq 1\}\,. \tag{21.29}$$

Thus there are $|s| = 2n,\ n \geq 1$, ramification points of f and $g(x) = n - 1$.

21.6 Smooth plane curves as Riemann surfaces

An affine plane curve over a field K is a polynomial equation $V : f(x,y) = 0$, where $f \in K[x,y]$.

Definition 54. *Let $L \supset K$ be a field and $P = (x_P, y_P) \in V(L)$ a point on V with coordinates in L. We say that P is a smooth point on V if*

$$\left(\frac{\partial f}{\partial x}(P), \frac{\partial f}{\partial y}(P)\right) \neq (0,0)\,. \tag{21.30}$$

Ex. 33. *(i) Each point of $V_1 : y = 0$ is smooth.*

(ii) No point of $V_2 : y^2 = 0$ is smooth.

(iii) The point $(0,0)$ is not smooth on either of the curves

$$V_3 : \; y^2 - x^3 = 0, \quad V_4 : \; y^2 - x^2(x+1)\,. \tag{21.31}$$

All other points on V_3, V_4 are smooth.

Definition 55. *V/K is a smooth affine plane curve over K if every point $P \in V(\bar{K})$ is smooth on V/K (where $\bar{K}$ is an algebraic closure of K).*

21.7 Divisors on Riemann surfaces

Definition 56. *A divisor on X is a locally finite formal sum $D = \sum_{P\in X} n_P(P)$, $n_P \in \mathbb{Z}$, where locally finite means that denoting by $supp(D) = \{P \in X \,|\, n_P \neq 0\}$ the support of D, we require that, for each compact subset $K \subset X$, the intersection $K \cap supp(D)$ be finite. In particular for X compact, locally finite = finite. The set $Div(X)$ of all divisors on X is an abelian group w.r. to addition. The divisor D is effective ($D \geq 0$) if all coefficients $n_P \geq$ are non–negative.*

Definition 57. *The divisor of a meromorphic function $f \in \mathcal{U}(X)^*$ (resp. the divisor of a meromorphic differential $\omega \in \Omega^1_{mer}(X)\backslash\{0\}$) is*

$$dif(f) = \sum_{P\in X} ord_P(f)(P), \quad div(\omega) = \sum_{P\in X} ord_P(\omega)(P)\,. \tag{21.32}$$

Note that the sums are locally finite. The divisors of the form $div(f)$, $f \in \mathcal{U}(X)^*$, are called principal divisors. They form a subgroup $P(X) \subseteq Div(X)$.

Definition 58. *If X is compact, then the degree of a divisor $D = \sum_P(P) \in Div(X)$ is $deg(D) = \sum_P n_P \in \mathbb{Z}$, a finite sum. Denote by $Div^0(X) = Ker(deg : Div(X) \longrightarrow \mathbb{Z})$ the subgroup of divisors of degree zero. It is clear that $P(X) \subseteq Div^0(X)$.*

Definition 59. *The divisor class group of X is the quotient abelian group $Cl(X) := Div(X)/P(X)$. If X is compact, then the subgroup of divisor classes of degree zero is denoted by $Cl^0(X) = Div^0(X)/P(X)$.*

If X is not compact, then every divisor on X is principal, i.e. $Cl(X) = 0$. To sum up, if X is compact, then there are exact sequences

$$\begin{aligned}
&0 \longrightarrow C^* \longrightarrow \mathcal{U}(X)^* \xrightarrow{div} Div(X) \longrightarrow Cl(X) \longrightarrow 0\,,\\
&0 \longrightarrow C^* \longrightarrow \mathcal{U}(X)^* \xrightarrow{div} Div^0(X) \longrightarrow Cl^0(X) \longrightarrow 0\,,\\
&0 \longrightarrow Cl^0(X) \longrightarrow Cl(X) \xrightarrow{deg} \mathbb{Z} \longrightarrow 0\,.
\end{aligned} \tag{21.33}$$

Let $f : X \to Y$ be a non–constant proper holomorphic map between Riemann surfaces. Then the map

$$f^* :\ \sum_{y\in Y} n_y(y) \longmapsto \sum_{x\in X} e_x n_{f(x)}(x) \tag{21.34}$$

defines a homomorphism of abelian groups

$$f^* :\ Div(Y) \longrightarrow Div(X) \tag{21.35}$$

satisfying

$$\begin{aligned}
&f^*(div(g)) = div(g\circ f) \quad (\forall g \in \mathcal{U}(Y)^*)\ ,\\
&deg\,(f^*(D)) = deg(f)\,deg(D) \quad (\forall D \in Div(Y))\,,\ \text{X is compact.}
\end{aligned} \tag{21.36}$$

21.8 Line bundles on Riemann surfaces

Recall that a theta function (w.r. to a lattice $L \subset \mathbb{C}$) is a holomorphic function $F(z) \in \mathcal{O}(\mathbb{C})$ satisfying the functional equations

$$F(z+\omega) = e^{a(\omega)z+b(\omega)}F(z), \quad z \in \mathbb{C},\ \omega \in L \tag{21.37}$$

for some $a(\omega),\ b(\omega) \in \mathbb{C}$. In particular, if $L = \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2$ then

$$\begin{aligned}
F(z+\omega_1) &= e^{a_1z+b_1}F(z), \quad a_1, b_1 \in \mathbb{C}\\
F(z+\omega_2) &= e^{a_2z+b_2}F(z), \quad a_2, b_2 \in \mathbb{C}\,.
\end{aligned} \tag{21.38}$$

Questions 1. *Theta function is not a function on $\mathbb{C}/L$. So what is a theta function (on $\mathbb{C}/L$)?*

The answer is that theta functions are sections of line bundles on $\mathbb{C}/L$. From the algebraic point of view, a line bundle on a Riemann surface X is a rank 1 projective $\mathcal{O}(X)$–module.

Definition 60. *Let X be a complex manifold, e.g. a Riemann surface. A (holomorphic) line bundle over X is a complex manifold $\mathcal{L}$ equipped with a surjective holomorphic map $p : \mathcal{L} \to X$ such that:*

(1) The fibre $\mathcal{L}_x := p^{-1}(x)$ over each $x \in X$ is a vector space, $dim_{\mathbb{C}}\mathcal{L}_x = 1$.

(2) L is locally isomorphic to the product $X \times \mathbb{C}$ in the following sense: there exists an open covering $\{U_\alpha\}_\alpha$ of X and holomorphic isomorphisms $f_\alpha : p^{-1}(U_\alpha) \xrightarrow{\sim} U_\alpha \times \mathbb{C}$ making the diagram

$$\begin{array}{ll} p^{-1}(U_\alpha) & \xrightarrow{\sim} U_\alpha \times \mathbb{C} \\ \downarrow p & \swarrow pr_1 \\ U_\alpha & \end{array} \tag{21.39}$$

commutative, and inducing linear maps on the fibers over each $x \in U_\alpha$.

A (holomorphic) section of $\mathcal{L}$ is a holomorphic map $s : X \to \mathcal{L}$ such that $p \circ s = Id$. The set $\Gamma(X, \mathcal{L})$ of holomorphic sections of $\mathcal{L}$ is a module over $\mathcal{O}(X)$. An isomorphism between $\mathcal{L}$ and another (holomorphic) line bundle $p' : \mathcal{L}' \to X$ is a holomorphic isomorphism $f : \mathcal{L} \xrightarrow{\sim} \mathcal{L}'$ linear on each fibre $(p')^{-1}(x)$ $(x \in X)$ and making the diagram

$$\begin{array}{ccc} \mathcal{L}' & \xrightarrow{\mathrm{f}} & \mathcal{L} \\ p' \searrow & & \swarrow p \\ & x & \end{array} \tag{21.40}$$

commutative.

Remark 11. *Replacing $\mathbb{C}$ by $\mathbb{C}^N$, $N \in \mathbb{N}$, we obtain the definition of rank N bundle on X. Note that the difference between the cases $N = 1$ resp. $N > 1$ is the commutativity ($GL(1, \mathbb{C}) \xrightarrow{\sim} \mathbb{C}^*$) resp. non–commutativity ($GL(N, \mathbb{C})$) of the group of automorphisms of the fibre.*

Ex. 34. *(1) The trivial line bundle is the product, $pr_1 : X \times \mathbb{C} \to X$. There is a canonical isomorphism*

$$\begin{aligned} \mathcal{O}(X) &\xrightarrow{\sim} \Gamma(X, X \times \mathbb{C}) \\ f &\longmapsto s(x) = (x, f(x)) \,. \end{aligned} \tag{21.41}$$

(2) If $p : \mathcal{L} \to X$ is a holomorphic line bundle, $f : Y \to X$ a holomorphic map. Then the pull–back of $\mathcal{L}$ via f

$$f^*\mathcal{L} = \{(y, l) \in Y \times \mathcal{L} \,|\, f(y) = p(l)\} \tag{21.42}$$

with the map $p'(y, l) = y$ is a holomorphic line bundle over Y.

(3) *By definition of the projective space,* $\mathbb{P}^N(\mathbb{C}) = \{V \subset \mathbb{C}^{N+1} \,|\, dim_{\mathbb{C}}(V) = 1\}$. *The tautological line bundle over* $\mathbb{P}^N(\mathbb{C})$ *is*

$$\mathcal{L} = \{(v, V) \in \mathbb{C}^{N+1} \times \mathbb{P}^N(\mathbb{C}) \,|\, v \in V\}\,, \tag{21.43}$$

together with the map $p(v, V) = V$.

Assume that Y is a complex manifold, G a group acting on Y by holomorphic automorphisms such that the action of each $g \in G \backslash \{e\}$ has no fixed points, i.e. $g_y \neq y, \ \forall y \in Y$. We will be interested in constructing line bundles on the quotient $X = G \backslash Y$ from lifts of the G–action from Y to the trivial line bundle $Y \times \mathbb{C}$ on Y. The prototypes of this construction are

(1) $Y = \mathbb{C},\ G = L$ (a lattice in $\mathbb{C}$), $X = \mathbb{C}/L$.

(2) $Y = \mathbb{C}^{N+1} \backslash \{0\},\ G = \mathbb{C}^*$ (G acting by diagonal multiplication on Y), $X = \mathbb{P}^N(\mathbb{C})$. In order to lift the G–action from Y to the trivial bundle $Y \times \mathbb{C}$ we must construct, for each $g \in G$, a holomorphic map $\tilde{g} : Y \times \mathbb{C} \to Y \times \mathbb{C}$ making the diagram

$$\begin{array}{ccc} Y \times \mathbb{C} & \xrightarrow{\tilde{g}} & Y \times \mathbb{C} \\ \downarrow pr_1 & & \downarrow pr_1 \\ Y & \xrightarrow{g} & Y \end{array} \tag{21.44}$$

commutative, and acting on each fiber $\{y\} \times \mathbb{C}$ by linear automorphism satisfying $\widetilde{g_1 g_2} = \tilde{g}_1 \tilde{g}_2,\ \forall g_1, g_2 \in G$. The linearity on the fibers explicitly amounts to

$$\tilde{g}(y, t) = (gy, \alpha_g(y)t), \quad y \in Y,\ t \in \mathbb{C}\,. \tag{21.45}$$

where $\alpha_g : Y \to \mathbb{C}^*$ is an invertible holomorphic function on Y. Then

$$\widetilde{g_1 g_2} = \tilde{g}_1 \tilde{g}_2 \Longrightarrow \alpha_{g_1 g_2}(y) = \alpha_{g_1}(g_2(y))\, \alpha_{g_2}(y)\,. \tag{21.46}$$

Conversely, if $\alpha_g : Y \to \mathbb{C}^*$ is a set of holomorphic functions satisfying Eq(↑???), then Eq(↑↑???) defines the lift of the G–action from Y to $Y \times \mathbb{C}$.

The identity Eq(↑???) is, essentialy, a 1–cocycle identity for the G–action on the group $\mathcal{O}(Y)^*$ of invertible holomorphic functions on Y. Note that G acts on $\mathcal{O}(Y)^*$ on the right (by $(\alpha * g)(y) = \alpha(gy)$), since we have started with a left G–action on Y. It is more customary to let G act on Y on the right, which then leads to the "usual" 1–cocycle relation for a left G–action on $\mathcal{O}(Y)^*$.

Ex. 35. *If, for each* $g \in G$, $\alpha_g(y) = \alpha_g$ *is a constant function, then*

$$\alpha_{g_1 g_2}(y) = \alpha_{g_1}(g_2(y))\, \alpha_{g_2}(y) = \alpha_{g_1}(y)\, \alpha_{g_2}(y) = (\alpha_{g_1}, \alpha_{g_2})\,(y) \quad (\forall y \in Y) \Longrightarrow$$

$$\begin{aligned} \varrho :\ G &\longrightarrow \mathbb{C}^* \\ g &\longmapsto \varrho(g) = \alpha_g \end{aligned} \tag{21.47}$$

is a group homomorphism. This yields, $\forall d \in \mathbb{Z}$, the lifted action defined by

$$\tilde{g}(y,t) = (gy, g^d t)\,. \tag{21.48}$$

The definition of lifted action via the diagram ↑??? implies that the projection pr_1 induces a map between the quotient spaces

$$\begin{aligned} pr_G:\ \mathcal{L} = G\backslash(Y\times\mathbb{C}) \longrightarrow G\backslash Y\ &=\ X\,,\\ pr_G(\tilde{\pi}_G(y,t))\ &=\ \pi_G(y)\,, \end{aligned} \tag{21.49}$$

where

$$\tilde{\pi}_G:\ Y\times\mathbb{C} \longrightarrow G\backslash(Y\times\mathbb{C}), \quad \pi_G:\ Y \longrightarrow G\backslash Y \tag{21.50}$$

denote canonical projections. In the generality we are considering, $\mathcal{L}$ and X are topological spaces (equipped with the quotient topology) and p is a continuous map. The fact that G acts on Y without fixed points implies that

$$\tilde{\pi}_G(y,t_1) = \tilde{\pi}_G(y,t_2) \Longleftrightarrow t_1 = t_2\,, \tag{21.51}$$

hence each fibre $pr_G^{-1}(\pi_G(y))$ consists of the set of distinct points $\tilde{\pi}_G(y,t),\ t\in\mathbb{C}$. Moreover, the structure of complex vector space on $pr_G^{-1}(\pi_G(y))$ depends only on $\pi_G(y)$.

A side from the question of holomorphic structure, we describe set theoretical sections of $p:\mathcal{L}\to X$, i.e. the maps $s:X\to\mathcal{L}$ satisfying $p\circ s = Id_x$. The commutative diagram

$$\begin{array}{ccc} Y\times\mathbb{C} & \xrightarrow{\tilde{\pi}_G} & G\backslash(Y\times\mathbb{C}) \\ \downarrow pr_1 & & \downarrow pr_G \\ Y & \xrightarrow{\pi_G} & G\backslash Y \end{array} \tag{21.52}$$

together with the equivalence Eq(↑???) imply that there is uniquely determined function $F:Y\to\mathbb{C}$ such that

$$(s\circ\pi)(y) = \tilde{\pi}_G(y,F(y)) \quad \forall y\in Y\,. \tag{21.53}$$

For which functions F does the Eq(↑???) define a (set–theoretical) section s of $\mathcal{L}$? The necessary and sufficient condition is that the RHS of Eq(↑???) should depend only on $\pi_G(y)$, i.e.

$$\tilde{\pi}_G(gy,F(gy)) = \tilde{\pi}_G(y,F(y)) \quad \forall y\in Y,\ \forall g\in G\,. \tag{21.54}$$

which is equivalent to

$$\tilde{\pi}_G(gy,F(gy)) = \tilde{\pi}_G(y,F(y)) = \tilde{\pi}_G(\tilde{g}(y,F(y))) = \tilde{\pi}_G(gy,\alpha_g(y)F(y))\,, \tag{21.55}$$

and hence, via Eq(↑???)

$$F(gy) = \alpha_g(y)F(y) \quad \forall y\in Y,\ \forall g\in G\,. \tag{21.56}$$

Notice the similarity with functional equation of theta functions. In the case that both $\mathcal{L}, X$ are complex manifolds, $p : \mathcal{L} \to X$ is a line bundle and the precious description of the sections of $\mathcal{L}$ also holds in the holomorphic category, inducing a bijection between

$$\Gamma(X, \mathcal{L}) \xrightarrow{\sim} \{\mathcal{F} \in \mathcal{O}(\mathcal{Y}) \,|\, \mathcal{F} \text{ satisfies Eq}(\uparrow)\}\,. \tag{21.57}$$

The line bundles $\mathcal{L}$ on X obtained by this construction are not completely arbitrary: by definition, $\pi_G^*(\mathcal{L}) = Y \times \mathbb{C}$.

Let $pr_1 : Y \times \mathbb{C} \to Y$ be a trivial line bundle. The reparametrization of the (trivial) line bundle $pr_1 : Y \times \mathbb{C} \to Y$ is a holomorphic isomorphism

$$\begin{aligned} \text{Iso: } Y \times \mathbb{C} &\xrightarrow{\sim} Y \times \mathbb{C} \\ (y, t) &\longmapsto (y, \beta(y)t) \end{aligned} \tag{21.58}$$

linear on the fibers via invertible holomorphic function $\beta : Y \to \mathbb{C}^*$. We define two lifts $\tilde{g}, \tilde{g'}$ of g to be equivalence provided the diagram

$$\begin{array}{ccc} Y \times \mathbb{C} & \xrightarrow{\tilde{g}} & Y \times \mathbb{C} \\ \downarrow\wr\ \text{Iso} & & \downarrow\wr\ \text{Iso} \\ Y \times \mathbb{C} & \xrightarrow{\tilde{g'}} & Y \times \mathbb{C} \end{array} \tag{21.59}$$

is commutative. In other words,

$$\begin{aligned} (gy, \alpha_g'(y)\beta(y)t) &= \tilde{g'}(\text{Iso}(y,t)) = \text{Iso}(\tilde{g}(y,t)) = \text{Iso}(gy, \alpha_g(y)t) \\ &= (gy, \beta(gy)\alpha_g(y)t)\,, \end{aligned} \tag{21.60}$$

which is equivalent to

$$\alpha_g'(y) = \frac{\beta(gy)}{\beta(y)}\alpha_g(y), \quad \forall y \in Y,\ \forall g \in G\,, \tag{21.61}$$

i.e. α_g', α_g differ by a 1–coboundary. In this reparametrization, the isomorphism class of $\mathcal{L}$ does not change, but the projection $\tilde{\pi}_G : Y \times \mathbb{C} \to \mathcal{L}$ changes according to $\tilde{\pi}_G' \circ \text{Iso} = \tilde{\pi}_G$. The description of sections of $\mathcal{L}$ still bolds if we replace $F(y)$ by $F'(y) = \beta(y)F(y)$.

All standard constructions of linear algebra can be applied to the case of vector bundles. In particular, given two (holomorphic) vector bundles $\mathcal{L}, \mathcal{L}'$ on X, we can form new line bundles $\mathcal{L} \otimes_{\mathcal{O}(X)} \mathcal{L}'$ and $\mathcal{L}^*$ (the dual of $\mathcal{L}$. If $\mathcal{L}$ is constructed from the functions $\{\alpha_g(y)\}$ (resp. $\mathcal{L}'$ is constructed from the functions $\{\alpha_g'(y)\}$, then $\mathcal{L} \otimes \mathcal{L}$ is defined by $\{\alpha_g(y)\alpha_g'(y)\}$ (resp $\mathcal{L}^*$ is defined using $\{\alpha_g^{-1}(y)\}$. On the level of sections, we have

$$\Gamma(X, \mathcal{L}) \otimes_{\mathbb{C}} \Gamma(X, \mathcal{L}) \longrightarrow \Gamma(X, \mathcal{L} \otimes \mathcal{L}')\,. \tag{21.62}$$

defined as follows: if $s \in \Gamma(X, \mathcal{L})$, $s' \in \Gamma(X, \mathcal{L}')$ correspond to the functions $F : Y \to \mathbb{C}$, $F' : Y \to \mathbb{C}$ satisfying Eq($\uparrow$???), then the tensor product $s \otimes s'$ corresponds to the function $F(y)F'(y)$.

21.9 Theta functions (from the point of view of line bundles)

Let $Y = \mathbb{C},\ G = L$ (a lattice in $\mathbb{C}$), $X = \mathbb{C}/L$. We are looking for holomorphic functions $\alpha_u(z) \in \mathcal{U}(\mathbb{C})$ $(u \in L)$ satisfying

$$\alpha_{u+v}(z) = \alpha_u(z+v)\alpha_v(z), \quad u, v \in L,\ z \in \mathbb{C}\,, \tag{21.63}$$

such that they define an action

$$\tilde{u}(z,t) = (z+u, \alpha_u(z)t), \quad u \in L \tag{21.64}$$

on $\mathbb{C} \times \mathbb{C}$ and its action descends to a holomorphic line bundle

$$\mathcal{L} = L\backslash(\mathbb{C} \times \mathbb{C}) \longrightarrow X = \mathbb{C}/L\,. \tag{21.65}$$

The sections of $\mathcal{L}$ correspond to holomorphic functions $F \in \mathcal{O}(\mathbb{C})$ satisfying

$$F(z+u = \alpha_u(z)F(z), \quad u \in L,\ z \in \mathbb{C}\,. \tag{21.66}$$

If the functions $\alpha_u(z)$ are replaced by equivalent functions

$$\tilde{\alpha}_u(z) = \frac{\beta(z+u)}{\beta(z)}\alpha_u(z)\,, \tag{21.67}$$

where $\beta : \mathbb{C} \to \mathbb{C}^*$ is and invertible holomorphic function, then the line bundle remains the same.

Lemma 33. *(1) Every holomorphic line bundle on $\mathbb{C}/L$ is obtained by the above construction.*

(2) For every solution $\{\alpha_u(z)\}$ of Eq(↑???) there is an equivalent solution via Eq(↑???) of the form

$$\tilde{\alpha}_u(z) = e^{a(u)z+b(u)}, \quad a(u), b(u) \in \mathbb{C}\,. \tag{21.68}$$

We shall not prove the lemma. The first statement is the consequence of the fact that every holomorphic line bundle on $\mathbb{C}$ is trivial. If Y is a non–compact Riemann surface, every (holomorphic) line bundle on Y is trivial. In particular, this applies to $\mathbb{C}$ and the unit disc $\Delta := \{z \in \mathbb{C} \,|\, |z| < 1\}$. If X is a Riemann surface not isomorphic to $\mathbb{P}^1(\mathbb{C})$, the universal covering Y of X is isomorphic either to $\mathbb{C}$ or to Δ, and $X = G\backslash Y$, where $G = \pi_1(X, x_0)$ acts on Y. This implies that every (holomorphic) line bundle on X can be obtained via particular pair $\{Y, G\}$.

Assume that $\mathcal{L}$ is the line bundle on $\mathbb{C}/L$ defined by the collection of functions $\{\alpha_u(z)\}$, $\alpha_u(z) = e^{a(u)z+b(u)}$, $a(u), b(u) \in \mathbb{C}$. The associativity condition Eq(↑???) is then equivalent to

$$\begin{aligned} a(u+v) &= a(u) + a(v) \\ b(u+v) &= b(u) + b(v) + a(u)v \mod 2\pi\mathbb{Z}\,. \end{aligned} \tag{21.69}$$

Interchanging u and v in Eq(↑???) gives the alternating bilinear form on L,

$$(u+v) \longmapsto \begin{vmatrix} u & v \\ a(u) & a(v) \end{vmatrix} \in 2\pi\mathbb{Z}, \quad (u, v \in L) \tag{21.70}$$

has values in $2\pi\mathbb{Z}$. This bilinear form represents the first Chern class of $\mathcal{L}$, i.e.

$$c_1(\mathcal{L}) \in H^2(\mathbb{C}/L, 2\pi\mathbb{Z}) = Hom(\Lambda^2 H_1(\mathbb{C}/L, \mathbb{Z}), 2\pi\mathbb{Z})\,. \tag{21.71}$$

If $L = \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2$, Eq(↑???) determine the constants $a(u), b(u)$ $(u \in L)$ iff we know $a(\omega_1), b(\omega_j) \in \mathbb{C}$ $(j = 1, 2)$, satisfying

$$\begin{vmatrix} \omega_1 & \omega_2 \\ a(\omega_1) & a(\omega_2) \end{vmatrix} \in 2\pi\mathbb{Z}\,. \tag{21.72}$$

Ex. 36. *Assume $\omega_2 = 1, \omega_1 = \tau$ ($Im\,\tau > 0$). After a reparametrization Eq(↑???) with $\beta(z) = \exp(Az^2 + Bz + C)$ (for suitable $A, B, C \in \mathbb{C}$), we can assume $a(1) = b(1) = 0$. The integrability condition Eq(↑???) becomes*

$$-a(\tau) = \begin{vmatrix} \tau & 1 \\ a(\tau) & 0 \end{vmatrix} \in 2\pi\mathbb{Z}\,. \tag{21.73}$$

Consider the case $-a(\tau) = 2\pi i$. The sections of the associated line bundle $\mathcal{L}$ then correspond to holomorphic functions $F \in \mathcal{O}(\mathbb{C})$ satisfying

$$F(z+1) = F(z), \quad F(z+\tau) = e^{-2\pi iz + b(\tau)} F(z)\,. \tag{21.74}$$

The induced map T_c^* of the translation, $T_c : z \mapsto z + c$, amounts to the pull–back $T_c^*\mathcal{L}$ of $\mathcal{L}$, which yields $b(\tau) \mapsto b(\tau) - 2\pi ic$. We choose c in such a way that $F(z) = F(-z)$ (i.e. F is an even holomorphic section). Putting $z = -\frac{\tau}{2}$ we obtain $b(\tau) = -\pi i\tau$.

We denote by $\mathcal{L}$ the line bundle on $\mathbb{C}(\mathbb{Z}\tau + \mathbb{Z})$ corresponding to the values $a(1) = b(1) = 0$, $a(\tau) = -2\pi i$, $b(\tau) = -\pi i\tau$.

A section $s \in \Gamma(\mathbb{C}/(\mathbb{Z}\tau + \mathbb{Z}, \mathcal{L})$ is then given by $F(z) \in \mathcal{O}(\mathbb{C})$ satisfying $F(z+1) = F(z)$, $F(z + \tau = e^{-2\pi i(z+\frac{\tau}{2})} F(z)$.

Proposition 12. *(Basic theta functions).: The space of holomorphic solutions of Eq(↑???) is equal to $\mathbb{C} \cdot \theta(z)$, where*

$$\theta(z) = \theta(z, \tau) = \sum_{n\in\mathbb{Z}} q^{\frac{n^2}{2}} t^n = \sum_{n\in\mathbb{Z}} e^{\pi in^2\tau + 2\pi inz}\,. \tag{21.75}$$

In other words, $\Gamma(\mathbb{C}/(\mathbb{Z}\tau + \mathbb{Z}), \mathcal{L}) = \mathbb{C} \cdot \theta(z)$.

Proof: Assume $F \in \mathcal{O}(\mathbb{C})$ satisfies Eq(↑???). The first relation implies $F(z) = f(e^{2\pi iz})$ for some $f \in \mathcal{O}(\mathbb{C}^*)$, which can be expanded to a convergent tangent series $f(t) = \sum_{n\in\mathbb{Z}} a_n t_n$ $(t = e^{2\pi iz})$. The second relation of Eq(↑???) is equivalent to

$$\sum_{n\in\mathbb{Z}} a_n q^n t^n = f(qt) = t^{-1}q^{-1/2} = \sum_{n\in\mathbb{Z}} a_n q^{-1/2} t^{n-1}$$
$$= \sum_{n\in\mathbb{Z}} a_{n+1} q^{-1/2} t^n \quad \left(q^{1/2} = e^{\pi i\tau}\right), \tag{21.76}$$

hence to

$$a_{n+1} = q^{n+1/2} a_n \ (n \in Z) \Longrightarrow a_n = q^{\frac{n^2}{2}} a_0 \ (n \in Z)$$
$$\Longrightarrow f(t) = a_0 \sum_{n\in\mathbb{Z}} q^{\frac{n^2}{2}} t^n = a_0 \theta(z). \tag{21.77}$$

As $|q| < 1$, the series defining $\theta(z)$ is uniformly convergent for t contained in a compact subset of $\mathbb{C}^*$, and so defines a holomorphic function. Reversing the calculation, we see that $\theta(z)$ satisfies Eq(↑???). ■

For fixed $a, b \in \{0, 1\} = \mathbb{Z}/2\mathbb{Z}$, denote by $\chi_{a,b} : L \to L/2L \to \{\pm 1\}$ the character $\chi_{a,b}(m + n\tau) = (-1)^{ma+nb}$, $L = \mathbb{Z}\tau + \mathbb{Z}$, $m, n \in \mathbb{Z}$. The constant functions $\{\chi_{a,b}(u)\}$ define a line bundle on $\mathbb{C}/\mathbb{Z}\tau+\mathbb{Z}$, which will also be denoted by $\chi_{a,b}$. For each $k \in \mathbb{Z}$, a section $s \in \Gamma(\mathbb{C}/(\mathbb{Z}\tau + \mathbb{Z}), \mathcal{L}^{\otimes k} \otimes \chi_{a,b})$ corresponds to a holomorphic function $F \in \mathcal{O}(\mathbb{C})$ satisfying

$$F(z + 1) = (-1)^a F(z),\ F(z + \tau) = (-1)^b exp^{-2\pi ik(z+\frac{\tau}{2})} F(z). \tag{21.78}$$

Let $k = 1$.

Lemma 34. *For $k = 1$, $a, b \in \{0, 1\}$, the space of holomorphic solutions of Eq(↑???) is equal to $\mathbb{C} \cdot \theta_{ab}(z)$, where*

$$\theta_{ab}(z) = \theta_{ab}(z, \tau) = \sum_{n\in\mathbb{Z}} e^{\pi i(n+\frac{a}{2})^2\tau + 2\pi i(n+\frac{a}{2})(z+\frac{b}{2})} = \theta_{a0}(z + \frac{b}{2}, \tau)$$
$$= e^{\pi ia(z+\frac{b}{2}) + \frac{\pi ia\tau}{4}} \theta_{00}(z + \frac{a\tau + b}{2}, \tau). \tag{21.79}$$

In other words, $\Gamma(\mathbb{C}/(\mathbb{Z}\tau + \mathbb{Z}), \mathcal{L} \otimes \chi_{a,b}) = \mathbb{C} \cdot \theta_{ab}(z)$ $(\theta_{00}(z) = \theta(z))$.

If we let $\mathrm{Im}(\tau) \to +\infty$, then $q = exp(2\pi i\tau) \to 0$. The expansion of $\theta_{ab}(z, \tau)$ then yields the following asymptotics as $\tau \to i\infty$:

$$\theta_{00}(z, \tau) \sim \theta_{01}(z, \tau) \sim 1, \quad \theta_{10}(z, \tau) \sim (t^{1/2} + t^{-1/2})q^{1/8},$$
$$\theta_{11}(z, \tau) \sim i(t^{1/2} - t^{-1/2})q^{1/8}. \tag{21.80}$$

Lemma 35. *(1) The function $\theta(z)$ has simple zeroes at $z = \frac{\tau+1}{2} + \mathbb{Z}\tau + \mathbb{Z}$ (and no other zeroes).*

(2) *For $a, b \in \{0,1\}$, the function $\theta_{ab}(z)$ has simple zeroes at $z \in \frac{(a+1)\tau+(b+1)}{2} + \mathbb{Z}\tau + \mathbb{Z}$ (and no other zeroes).*

It is easy to prove, using functional equations Eq(↑???), that

$$\frac{1}{2\pi i}\int_{\partial D}\frac{\theta'(z)}{\theta(z)}dz = 1 \quad \frac{1}{2\pi i}\int_{\partial D} z\frac{\theta'(z)}{\theta(z)}dz \in \frac{\tau+1}{2} + \mathbb{Z}\tau + \mathbb{Z}\,, \tag{21.81}$$

where $D = \{z = \alpha + t_1\tau + t_2 1 \,|\, 0 \geq t_1, t_2 \geq 1\}$ is the fundamental parallelogram for $L = \mathbb{Z}\tau + \tau$.

It is possible to classify, up to isomorphism, all line bundles on $\mathbb{C}/(\mathbb{Z}\tau + \mathbb{Z})$. Each line bundle $\mathcal{L}'$ is defined, up to isomorphism, by the functions

$$\alpha_1(z) = 1, \quad \alpha_\tau(z) = e^{-2\pi i m(z+\frac{\tau}{2}+c)}, \quad m \in \mathbb{Z},\ c \in \mathbb{C}\,, \tag{21.82}$$

with $\{\alpha_u(z)\}$, $u \in \mathbb{Z}\tau + \tau$, fulfilling associativity condition. In other words, $\mathcal{L}'$ is isomorphic to $(T_c^*\mathcal{L})^{\otimes m}$, where $T_c(z) = z + c$ is the translation by $c \in \mathbb{C}$ (for example, $\Gamma(\mathbb{C}/(\mathbb{Z}\tau + \mathbb{Z}), T_c^*\mathcal{L}) = \mathbb{C}\cdot\theta(z+c)$).

If $c, c' \in \mathbb{C}$ satisfy $m(c - c') \in \mathbb{Z}\tau + \mathbb{Z}$, then Eq(↑???) define (for $c, c' \in \mathbb{C}$) the same line bundles. This means that the isomorphism class of $(T_c^*\mathcal{L})^{\otimes m}$ depends on two invariants: an integer and an element of $\mathbb{C}/(\mathbb{Z}\tau+\mathbb{Z})$, which is reminiscent of the description of divisor class group $Cl\,(\mathbb{C}/(\mathbb{Z}\tau + \mathbb{Z}))$:

$$0 \longrightarrow \mathbb{C}/(\mathbb{Z}\tau + \mathbb{Z}) \longrightarrow Cl\,(\mathbb{C}/(\mathbb{Z}\tau + \mathbb{Z})) \stackrel{deg}{\longrightarrow} \mathbb{Z} \longrightarrow 0\,. \tag{21.83}$$

There is a direct correspondence between isomorphism classes of line bundles on an arbitrary Riemann surface X and divisor classes on X. For a line bundle $p : \mathcal{L} \to X$, one can define meromorphic sections of $\mathcal{L}$. The zeros and poles (including multiplicities) of such a non–zero meromorphic section s are invariant under the action of G, hence come from a divisor $div(s) \in Div(X)$. Non–zero meromorphic sections of $\mathcal{L}$ always exist and form a one–dimensional vector space over $\mathcal{U}(X)$. If $s' = fs$ is another meromorphic section of $\mathcal{L}$ (with $f \in \mathcal{L}(X)\backslash\{0\}$), then $div(s') = div(s) + div(f)$. Thus the class of the divisor $div(s)$ does not depend on the choice of s. We get a homomorphism of abelian groups

$$\begin{array}{ccc} \begin{array}{c}\{\text{isomorphism classes of} \\ \text{line bundles on } X\}\end{array} & \longrightarrow & Cl(X)\,, \\ \mathcal{L} & \longmapsto & [div(s)] \end{array} \tag{21.84}$$

with tensor structure of line bundles on the LHS.

21.10 Relations among theta functions

Theta functions satisfy a large number of interesting identities, based on the following simple fact – the tensor product

$$\begin{aligned} &\Gamma\left(\mathbb{C}/(\mathbb{Z}\tau + \mathbb{Z}), \mathcal{L}^{\otimes m} \otimes \chi_{a,b}\right) \otimes_{\mathbb{C}} \Gamma\left(\mathbb{C}/(\mathbb{Z}\tau + \mathbb{Z}), \mathcal{L}^{\otimes n} \otimes \chi_{c,d}\right) \longrightarrow \\ &\Gamma\left(\mathbb{C}/(\mathbb{Z}\tau + \mathbb{Z}), \mathcal{L}^{\otimes (m+n)} \otimes \chi_{a+c,b+d}\right)\,, \end{aligned} \tag{21.85}$$

base non–trivial kernels, which yield non–trivial linear relations between products of the theta functions.

The four theta functions $\theta_{ab}(z),\ \ a,b\in\{0,1\}$, are linearly independent over $\mathbb{C}$.

Theorem 43. *For $m\in\mathbb{Z},\ \ a,b\in\{0,1\}$,*

$$dim_{\mathbb{C}}\Gamma\left(\mathbb{C}/(\mathbb{Z}\tau+\mathbb{Z}),\mathcal{L}^{\otimes m}\otimes\chi_{a,b}\right)=\begin{cases} m\ if\ m>0\\ 0\ \ if\ m<0\,.\end{cases} \tag{21.86}$$

Proof: If $m>0$, the expansion of a holomorphic solution into a tangent series $\sum_{n\in\mathbb{Z}}a_n t^{n+\frac{a}{2}}$ yields, via the functional equation, recursive relations between a_n and a_{n+m} $(n\in\mathbb{Z})$, which leaves the values of $a_0,\dots,a_{m-1}$ undetermined. Conversely, any choice at these first m coefficients defines a holomorphic solution. If $m<0$, we obtain again recursive relations between a_n,a_{n+m} $(n\in\mathbb{Z})$, but every non–zero choice of $(a_0,\dots,a_{m-1})$ leads to a divergent series. ■

Ex. 37. *The four functions $\theta^2_{ab}(z)$ all lie in the two–dimensional space $\Gamma\left(\mathbb{C}/(\mathbb{Z}\tau+\mathbb{Z}),\mathcal{L}^{\otimes 2}\right)$ and they generate this space. As a result, there exist two linearly independent relations among $\theta^2_{00}(z),\theta^2_{01}(z),\theta^2_{10}(z),\theta^2_{11}(z)$.*

We denote, for $n\geq 0$ and $a,b\in\{0,1\}$,

$$\theta^{(n)}_{ab}(z)=\left(\frac{\partial}{\partial z}\right)^n\theta_{ab}(z),\quad \theta_{ab}=\theta_{ab}(0,\tau),\quad \theta^n_{ab}=\left(\frac{\partial}{\partial z}\right)^n\theta_{ab}(z,\tau)\Big|_{z=0}\,. \tag{21.87}$$

For example,

$$\begin{vmatrix}\theta'_{ab}(z) & \theta'_{cd}(z)\\ \theta_{ab}(z) & \theta_{cd}(z)\end{vmatrix}\in\Gamma\left(\mathbb{C}/(\mathbb{Z}\tau+\mathbb{Z}),\mathcal{L}^{\otimes 2}\otimes\chi_{a+c,b+d}\right)\,. \tag{21.88}$$

Lemma 36. *(Heat equation): For $a,b\in\{0,1\}$,*

$$\left(\frac{\partial^2}{\partial z^2}-4\pi i\frac{\partial}{\partial\tau}\right)\theta_{ab}(z,\tau)=0\,. \tag{21.89}$$

Proof: As

$$\frac{1}{2\pi i}\frac{\partial}{\partial\tau}:\left\{\begin{matrix} q^m\longmapsto mq^m\\ t^m\longmapsto 0\end{matrix}\right\},\quad \frac{1}{2\pi i}\frac{\partial}{\partial z}:\left\{\begin{matrix} q^m\longmapsto 0\\ t^m\longmapsto mt^m\end{matrix}\right\}, \tag{21.90}$$

the operator $\frac{1}{2\pi i}\frac{\partial}{\partial\tau}-\frac{1}{2}\left(\frac{1}{2\pi i}\frac{\partial}{\partial z}\right)^2$annihilates each of the series

$$\theta_{ab}(z)=\sum_{n\in\mathbb{Z}}e^{\pi ib\left(n+\frac{a}{2}\right)}q^{\frac{1}{2}\left(n+\frac{a}{2}\right)^2}t^{n+\frac{a}{2}}\,. \tag{21.91}$$

■

Letting $z \mapsto 0$ (i.e. $t \sim 1 + 2\pi i z$), we obtain

$$\begin{aligned}
\theta_{00}(\tau) &= \prod_{n=1}^{\infty} (1-q^n)\left(1+q^{n-\frac{1}{2}}\right)^2 , \\
\theta_{01}(\tau) &= \prod_{n=1}^{\infty} (1-q^n)\left(1-q^{n-\frac{1}{2}}\right)^2 , \\
\theta_{10}(\tau) &= 2q^{\frac{1}{8}} \prod_{n=1}^{\infty} (1-q^n)(1+q^n)^2 . \qquad (21.92)
\end{aligned}$$

Theorem 44. *(Jacobi's triple product formula)*

$$\sum_{n\in\mathbb{Z}} q^{\frac{n^2}{2}} t^n = \prod_{n=1}^{\infty} (1-q^n)\left(1+q^{n-\frac{1}{2}}t\right)\left(1+q^{n-\frac{1}{2}}t^{-1}\right) . \qquad (21.93)$$

Appendix A

Algebraic Curves, Function Fields

This appendix contains a brief survey of the relations between algebraic curves and algebraic function fields. For details and proofs, we refer to the literature on algebraic geometry, for instance [3], [4], [5], [6].

We assume that K is an algebraically closed field

B.1. Affine Varieties. The n-dimensional *affine space* $\mathbf{A}^n = \mathbf{A}^n(K)$ is the set of all n-tuples of elements of K. An element $P = (a_1, \ldots, a_n) \in \mathbf{A}^n$ is a *point*, and $a_1 \ldots, a_n$ are the *coordinates* of P.

Let $K[X_1, \ldots, X_n]$ be the ring of polynomials in n variables over K. A subset $V \subseteq \mathbf{A}^n$ is an *algebraic set* if there exists a set $M \subseteq K[X_1, \ldots, X_n]$ such that

$$V = \{P \in \mathbf{A}^n \mid F(P) = 0 \text{ for all } F \in M\}\,. \tag{A.1}$$

Given an algebraic set $V \subseteq \mathbf{A}^n$, the set of polynomials

$$I(V) = \{F \in K[X_1, \ldots, X_n] \,|\, F(P) = 0 \text{ for all } P \in V\} \tag{A.2}$$

is called the *ideal* of V. $I(V)$ is obviously an ideal in $K[X_1, \ldots, X_n]$, and it can be generated by finitely many polynomials $F_1, \ldots, F_r \in K[X_1, \ldots, X_n]$. Thus we have

$$V = \{P \in \mathbf{A}^n \mid F_1(P) = \ldots = F_r(P) = 0\}\,. \tag{A.3}$$

An algebraic set $V \subseteq \mathbf{A}^n$ is called *irreducible* if it cannot be written as $V = V_1 \cup V_2$, where V_1 and V_2 are proper algebraic subsets of V. Equivalently, V is irreducible if and only if the corresponding ideal $I(V)$ is a prime ideal. An *affine variety* is an irreducible algebraic set $V \subseteq \mathbf{A}^n$.

The *coordinate ring* of an affine variety V is the residue class ring

$$\Gamma(V) = K[X_1, \dots, X_n]/I(V)\,. \tag{A.4}$$

As $I(V)$ is a prime ideal, $\Gamma(V)$ is an integral domain. Any $f = F + I(V) \in \Gamma(V)$ induces a function $f : V \to K$ by setting $f(P) = F(P)$ for $P \in V$. The quotient field

$$K(V) = \mathit{Quot}\,(\Gamma(V)) \tag{A.5}$$

is called the *field of rational functions* (or the *function field*) of V.

For a point $P \in V$, let

$$\mathcal{O}_P(V) = \{f \in K(V) \,|\, f = g/h \text{ with } g, h \in \Gamma(V) \text{ and } h(P) \neq 0\}\,. \tag{A.6}$$

This is a local ring with quotient field $K(V)$, its unique maximal ideal is

$$M_P(V) = \{f \in K(V) \,|\, f = g/h \,|\, g, h \in \Gamma(V), h(P) \neq 0 \text{ and } g(P) = 0\}\,. \tag{A.7}$$

$\mathcal{O}_P(V)$ is called the *local ring* of V at P. For $f = g/h \in \mathcal{O}_P(V)$ with $h(P) \neq 0$, the *value* of f at P is defined to be $f(P) = g(P)/h(P)$.

B.2. Projective Varieties. On the set $\mathbf{A}^{n+1}\backslash\{(0, \dots, 0)\}$, an equivalence relation $\sim$ is given by

$$\begin{aligned}&(a_0, a_1, \dots, a_n) \sim (b_0, b_1, \dots, b_n) \Longleftrightarrow \\ &\text{there is an element } 0 \neq \lambda \in K \text{ such that } b_i = \lambda a_i \text{ for } 0 \leq i \leq n.\end{aligned} \tag{A.8}$$

The equivalence class of $(a_0, a_1, \dots, a_n)$ with respect to $\sim$ is denoted by $(a_0 : a_1 : \dots : a_n)$. The n-dimensional *projective space* $\mathbf{P}^n = \mathbf{P}^n(K)$ is the set of all equivalence classes

$$\mathbf{P}^n = \{(a_0 : \dots : a_n) \,|\, a_i \in K,\ \text{not all } a_i = 0\}. \tag{A.9}$$

An element $P = (a_0 : \dots : a_n) \in \mathbf{P}^n$ is a *point*, and $a_0, \dots, a_n$ are called *homogenous coordinates* of P.

A *monom* of degree d is a polynomial $G \in K[X_0, \dots, X_n]$ of the form

$$G = a \cdot \prod_{i=0}^{n} X_i^{d_i} \text{ with } 0 \neq a \in K \text{ and } \sum_{i=0}^{n} d_i = d \tag{A.10}$$

A polynomial F is a *homogeneous polynomial* if F is the sum of monomials of the same degree. An ideal $I \subseteq K[X_0, \dots, X_n]$ which is generated by homogeneous polynomials is called a *homogeneous ideal.*

Let $P = (a_0 : \dots : a_n) \in \mathbf{P}^n$ and $F \in K[X_0, \dots, X_n]$ be a homogeneous polynomial. We say that $F(P) = 0$ if $F(a_0, \dots, a_n) = 0$. This makes sense: since

$F(\lambda a_0, \dots, \lambda a_n) = \lambda^d \cdot F(a_0, \dots, a_n)$ (with $d = deg\ F$), one has $F(a_0, \dots, a_n) = 0 \Longleftrightarrow F(\lambda a_0, \dots, \lambda a_n) = 0$.

A subset $V \subseteq \mathbf{P}^n$ is a *projective algebraic set* if there exists a set of homogeneous polynomials $M \subseteq K[X_0, \dots, X_n]$ such that

$$V = \{P \in \mathbf{P}^n \mid F(P) = 0 \text{ for all } F \in M\}\,. \tag{A.11}$$

The ideal $I(V) \subseteq K[X_0, \dots, X_n]$, which is generated by all homogeneous polynomials F with $F(P) = 0$ for all $P \in V$, is called the *ideal* of V. It is a homogeneous ideal. *Irreducibility* of projective algebraic sets is defined as in the affine case. Again, $V \subseteq P^n$ is irreducible iff $I(V)$ is a homogeneous prime ideal in $K[X_0, \dots, X_n]$. A *projective variety* is an irreducible projective algebraic set.

Given a non-empty variety $V \subseteq P^n$, we define its *homogeneous coordinate*

$$\Gamma_h(V) = K[X_0, \dots, X_n]/I(V); \tag{A.12}$$

this is an integral domain containing K. An element $f \in \Gamma_h(V)$ is said to be a *form* a degree d if $f = F + I(V)$ for some homogeneous polynomial $F \in K[X_0, \dots, X_n]$ with $deg\ F = d$. The *function field* of V is defined by

$$K(V) = \left\{ \frac{g}{h} \,\middle|\, g, h \in \Gamma_h(V) \text{ are forms of the same degree and } \ h \neq 0 \right\}\,, \tag{A.13}$$

which is a subfield of $Quot\,(\Gamma_h(V))$, the quotient field of $\Gamma_h(V)$.

The *dimension* of V is the transcendence degree of $K(V)$ over K.

Let $P = (a_0 : \ldots : a_n) \in V$ and $f \in K(V)$. Write $f = g/h$ where $g = G + I(V)$, $h = H + I(V) \in \Gamma_h(V)$ and G, H are homogeneous polynomials of degree d. Since

$$\frac{G(\lambda a_0, \dots, \lambda a_n)}{H(\lambda a_0, \dots, \lambda a_n)} = \frac{\lambda^d \cdot G(a_0, \dots, a_n)}{\lambda^d \cdot H(a_0, \dots, a_n)} = \frac{G(a_0, \dots, a_n)}{H(a_0, \dots, a_n)}\,, \tag{A.14}$$

we can set $f(P) = G(a_0, \dots, a_n)/H(a_0, \dots, a_n) \in K$, if $H(P) \neq 0$. Then we say that f is *defined* at P and call $f(P)$ the *value* of f at P. The ring

$$\mathcal{O}_P(V) = \{f \in K(V) \mid f \text{ is defined at } P\} \subseteq K(V) \tag{A.15}$$

is a local ring with maximal ideal

$$M_P(V) = \{f \in \mathcal{O}_P(V) \mid f(P) = 0\}\,. \tag{A.16}$$

B.3. Covering Projective Varieties by Affine Varieties. For $0 \leq i \leq n$, we consider the mapping $\varphi_i : \mathbf{A}^n \to \mathbf{P}^n$ given by

$$\varphi_i(a_0, \dots, a_{n-1}) = (a_0 : \ldots : a_{i-1} : 1 : a_i : \ldots : a_{n-1})\,. \tag{A.17}$$

φ_i is a bijection from $\mathbf{A}^n$ onto the set

$$U_i = \{(c_0 : \ldots : c_n) \in \mathbf{P}^n \mid c_i \neq 0\}, \tag{A.18}$$

and $\mathbf{P}^n = \bigcup_{i=0}^n U_i$. So $\mathbf{P}^n$ is covered by $n+1$ copies of the affine space $\mathbf{A}^n$ (this is not a disjoint union).

Let $V \subseteq \mathbf{P}^n$ be a projective variety, then $V = \bigcup_{i=0}^n (V \cap U_i)$. Suppose that $V \cap U_i \neq 0$. Then

$$V_i := \varphi_i^{-1}(V \cap U_i) \subseteq \mathbf{A}^n \tag{A.19}$$

is an affine variety, and the ideal $I(V_i)$ (in the sense of B.1) is given by

$$I(V_i) = \{F(X_0, \ldots, X_{i-1}, 1, X_{i+1}, \ldots, X_n) \mid F \in I(V)\}. \tag{A.20}$$

For convenience, we restrict ourselves in the following to the case $i = n$ (and $V \cap U_n \neq 0$). The complement $H_n = \mathbf{P}^n \setminus U_n = \{(a_0 : \ldots : a_n) \in \mathbf{P}^n \mid a_n = 0\}$ is called the *hyperplane at infinity*, and the points $P \in V \cap H_n$ are the *points at infinity*.

There is a natural K-isomorphism α from $K(V)$ (the function field of the projective variety V) onto $K(V_n)$ (the function field of the affine variety $V_n = \varphi_n^{-1}(V \cap U_n)$). This isomorphism is defined as follows: Let $f = g/h \in K(V)$ where $g, h \in \Gamma_h(V)$ are forms of the same degree and $h \neq 0$. Choose homogeneous polynomials $G, H \in K[X_0 \ldots, X_n]$ which represent g resp. h. Let $G_* = G(X_0, \ldots, X_{n-1}, 1)$ and $H_* = H(X_0, \ldots, X_{n-1}, 1) \in K[X_0, \ldots, X_{n-1}]$. Their residue classes in $\Gamma(V_n) = K[X_0, \ldots, X_{n-1}]/I(V_n)$ are g_* resp. h_*. Then $\alpha(f) = g_*/h_*$. Under this isomorphism, the local ring of a point $P \in V \cap U_n$ is mapped onto the local ring of $\varphi_n^{-1}(P) \in V_n$, hence these local rings are isomorphic.

B.4. The Projective Closure of an Affine Variety. For a polynomial $F = F(X_0, \ldots, X_{n-1}) \in K[X_0, \ldots, X_{n-1}]$ of degree d, set

$$F^* = X_n^d \cdot F(X_0/X_n, \ldots, X_{n-1}/X_n) \in K[X_0, \ldots, X_n]. \tag{A.21}$$

F^* is a homogeneous polynomial of degree d in $n+1$ variables.

Consider now an affine variety $V \in \mathbf{A}^n$ and the corresponding ideal $I(V) \subseteq K[X_0, \ldots, X_{n-1}]$. Define the projective variety $\bar{V} \subseteq \mathbf{P}^n$ as follows:

$$\bar{V} = \{P \in \mathbf{P}^n \mid F^*(P) = 0 \text{ for all } F \in I(V)\}. \tag{A.22}$$

This variety $\bar{V}$ is called the *projective closure* of V. One can recover V from $\bar{V}$ by the process described in B.3, namely

$$V = \varphi_n^{-1}(\bar{V} \cap U_n) = \left(\bar{V}\right)_n. \tag{A.23}$$

Consequently, the function fields of V and $\bar{V}$ are naturally isomorphic, and V and $\bar{V}$ have the same dimension.

B.5. Rational Maps and Morphisms. Let $V \subseteq \mathbf{P}^m$ and $W \subseteq \mathbf{P}^n$ be projective varieties. Suppose that $F_0, \ldots, F_n \in K[X_0, \ldots, X_m]$ are homogeneous polynomials with the following properties:

(a) $F_0, \ldots, F_n$ have the same degree;

(b) not all F_i are in $I(V)$;

(c) for all $H \in I(V)$ holds $H(F_0, \ldots, F_n) \in I(V)$.

Let $Q \in V$ and assume that $F_i(Q) \neq 0$ for at least one $i \in \{0, \ldots, n\}$ (by (b), such a point exists). Then the point $(F_0(Q) : \ldots : F_n(Q)) \in \mathbf{P}^n$ lies in W, by (c). Let $(G_0, \ldots, G_n)$ be another n-tuple of homogeneous polynomials satisfying (a), (b) and (c). We say that $(F_0, \ldots, F_n)$ and $(G_0, \ldots, G_n)$ are equivalent if

(d) $F_i G_j \equiv F_j G_i \ \mathit{mod}\, I(V)$ for $0 \leq i, j \leq n$.

The equivalence class of $(F_0, \ldots, F_n)$ with respect to this equivalence relation is denoted by

$$\phi = (F_0 : \ldots : F_n)\,, \tag{A.24}$$

A rational map $\phi = (F_0 : \ldots : F_n)$ is *regular* (or *defined*) at the point $P \in V$ if there exist homogeneous polynomials $G_0, \ldots, G_n \in K[X_0, \ldots, X_m]$ such that $\phi = (G_0 : \ldots : G_n)$ and $G_i(P) \neq 0$ for at least one i. Then we set

$$\phi(P) = (G_0(P) : \ldots : G_n(P)) \in W\,, \tag{A.25}$$

which is well-defined by (a) and (d).

Two varieties V_1, V_2 are *birationally equivalent* if there are rational maps $\phi_1 : V_1 \to V_2$ and $\phi_2 : V_2 \to V_1$ such that $\phi_1 \circ \phi_2$ and $\phi_2 \circ \phi_1$ are identity maps on V_2 and V_1 respectively. V_1 and V_2 are birationally equivalent if and only if their function fields $K(V_1)$ and $K(V_2)$ are K-isomorphic.

A rational map $\phi : V \to W$ which is regular at all points $P \in V$ is called a *morphism*. It is called an *isomorphism* if there is a morphism $\psi : W \to V$ such that $\phi \circ \psi$ and $\psi \circ \phi$ are the identity maps on W and V respectively. In this case, V and W are said to be *isomorphic*. Clearly, isomorphy implies birational equivalence, but the converse is not true in general.

B.6. Algebraic Curves. A *projective (affine) curve* V is a projective (affine) variety od dimension one. This means that the field $K(V)$ of rational functions on V is an algebraic function field of one variable.

A point $P \in V$ is *non-singular* (or *simple*) if the local ring $\mathcal{O}_P(V)$ is a discrete valuation ring (i.e. $\mathcal{O}_P(V)$ is a principal ideal domain with exactly one maximal ideal $\neq \{0\}$). There exist only finitely many singular points on a curve. The curve V is called *non-singular* (or *smooth*) if all points $P \in V$ are non-singular.

A *plane affine curve* is an affine curve $V \subseteq \mathbf{A}^2$. Its ideal $I(V) \subseteq K[X_0, X_1]$ is generated by an irreducible polynomial $G \in K[X_0, X_1]$ (which is unique up to a constant factor). Conversely, given an irreducible polynomial $G \in K[X_0, X_1]$, the set $V = \{P \in \mathbf{A}^2 \,|\, G(P) = 0\}$ is a plane affine curve, and G generates the corresponding ideal $I(V)$. A point $P \in V$ is non-singular if and only if

$$G_{X_0}(P) \neq 0 \quad \text{or} \quad G_{X_1}(P) \neq 0 \quad \text{(or both)}\,, \tag{A.26}$$

where $G_{Xi} \in K[X_0, X_1]$ is the partial derivative of G with respect to X_i (*Jacobi-Criterion*).

Accordingly, the ideal of a *plane projective curve* $V \subseteq \mathbf{P}^2$ is generated by an irreducible homogeneous polynomial $H \in K[X_0, X_1, X_2]$. A point $P \in V$ is non-singular iff $H_{X_i}(P) \neq 0$ for at least one $i \in \{0, 1, 2\}$.

If $V = \{P \in \mathbf{A}^2 \,|\, G(P) = 0\}$ is a plane affine curve (with an irreducible polynomial $G \in K[X_0, X_1]$ of degree d), the projective closure $\bar{V} \subseteq \mathbf{P}^2$ is the set of zeros of the homogeneous polynomial $G^* = X_2^d \cdot G(X_0/X_2, X_1/X_2)$.

B.7. Maps Between Curves. We consider now rational maps $\phi : V \to W$ where V and W are projective curves. The following holds:

(a) ϕ is defined at all non-singular points $P \in V$. Hence, if V is a non-singular curve, then ϕ is a morphism.

(b) If V is non-singular and ϕ is non-constant then ϕ is surjective.

B.8. The Non-singular Model of a Curve. Let V be a projective curve. Then there exists a non-singular projective curve V' and a birational morphism $\phi' : V' \to V$. The pair (V', ϕ') is unique in the following sense: given another non-singular curve V'' and a birational morphism $\phi'' : V'' \to V$, there exists a unique isomorphism $\phi : V' \to V''$ such that $\phi' = \phi'' \circ \phi$. Hence V' (more precisely: the pair (V', ϕ')) is called the *non-singular model* of V.

If $\phi' : V' \to V$ is the non-singular model of V and $P \in V$ is non-singular, there exists a unique $P' \in V'$ with $\phi'(P') = P$; for a singular point $P \in V$ the number of $P' \in V'$ with $\phi'(P') = P$ is finite (it may be one).

B.9. The Curve Associated with an Algebraic Function Field. Starting from an algebraic function field of one variable F/K, there exists a non-singular projective curve V (unique up to isomorphism) whose function field $K(V)$ is (K-isomorphic to) F. One can construct V as follows: choose $x, y \in F$ such that $F = K(x, y)$. Let $G(X, Y) \in K[X, Y]$ be the irreducible polynomial with

$G(x, y) = 0$. Let $W = \{P \in \mathbf{A}^2 \mid G(P) = 0\}$ and $\bar{W} \subseteq \mathbf{P}^2$ be the projective closure of W. Let V be the non-singular model of $\bar{W}$; then $K(V) \simeq F$.

B.10. Non-singular Curves and Algebraic Function Fields. Let V be a non-singular projective curve and $F = K(V)$ be its function field. There is a 1-1 correspondence between the points $P \in V$ and the places of F/K, given by

$$P \longmapsto M_P(V)\,, \tag{A.27}$$

the maximal ideal of the local ring $\mathcal{O}_P(V)$. This correspondence makes it possible to translate definitions and results from algebraic function fields to algebraic curves (and vice versa). We give some examples:

– The *genus* of the curve V is the genus of the function field $K(V)$.

– A *divisor* of V is a formal sum $D = \sum_{P \in V} n_P P$ where $n_P \in \mathbb{Z}$ and almost all $n_P = 0$. The *degree* of D is $deg\, D = \sum_{P \in V} n_P$. The divisors of V form an additive group $\mathcal{D}(V)$, the *divisor group* of V.

– The *order of a rational function* at a point $P \in V$ is defined to be $v_P(f)$ (where v_P is the discrete valuation of $K(V)$ corresponding to the valuation ring $\mathcal{O}_P(V)$).

– The *principal divisor* (f) of a rational function $0 \neq f \in K(V)$ is $(f) = \sum_{P \in V} v_P(f)P$. The degree of a principal divisor is 0.

– The principal divisors form a subgroup $\mathcal{P}(V)$ of the divisor group $\mathcal{D}(V)$. The factor group $Jac(V) = \mathcal{D}^0(V)/\mathcal{P}(V)$, where $\mathcal{D}^0(V)$ is the group of divisors of degree 0, is called the *Jacobian* of V.

– For $D \in \mathcal{D}(V)$, the space $\mathcal{L}(D)$ is defined as in the function field case. It is a finite-dimensional vector space over K, its dimension is given by the Riemann-Roch Theorem.

B.11. Varieties over a Non-algebraically Closed Field. Thus far, it was assumed that K is an algebraically closed field. Now we drop this assumption and suppose only that K is a *perfect* field. Let $\bar{K} \supseteq K$ be the algebraic closure of K.

An affine variety $V \subseteq \mathbf{A}^n\left(\bar{K}\right)$ is said to be *defined over* K if its ideal $I(V) \subseteq \bar{K}[X_1, \ldots, X_n]$ can be generated by polynomials $F_1, \ldots, F_r \in K[X_1, \ldots, X_n]$. If V is defined over K, the set

$$V(K) = V \cap \mathbf{A}^n(K) = \{P = (a_1, \ldots, a_n) \in V \mid \text{all } a_i \in K\} \tag{A.28}$$

is called the set of *K-rational points* of V.

Similarly, a projective variety $V \subseteq \mathbf{P}^n\left(\bar{K}\right)$ is *defined over* K if $I(V)$ is generated by homogeneous polynomials $F_1, \ldots, F_r \in K[X_0, \ldots, X_n]$. A point $P \in V$ is called K-*rational* if there exist homogeneous coordinates $a_0, \dots, a_n$ of P which are in K, and we set

$$V(K) = \{P \in V \mid \text{is } K\text{-rational}\}\,. \tag{A.29}$$

Let $V \subseteq \mathbf{A}^n\left(\bar{K}\right)$ be an affine variety defined over K. Define the ideal

$$I(V/K) = I(V) \cap K[X_1, \dots, X_n] \tag{A.30}$$

and the residue class ring

$$\Gamma(V/K) = K[X_1, \dots, X_n]/I(V/K)\,. \tag{A.31}$$

The quotient field

$$K(V) = Quot(\,\Gamma(V/K)) \subseteq \bar{K}(V) \tag{A.32}$$

is the field of K-*rational functions* of V. The field extension $K(V)/K$ is finitely generated, its transcendence degree is the dimension of V. In the same manner, the field of K-rational functions of a projective variety can be defined.

Consider two varieties $V \subseteq \mathbf{P}^m\left(\bar{K}\right)$ and $W \subseteq \mathbf{P}^n\left(\bar{K}\right)$. A rational map $\phi : V \to W$ is *defined over* K if there exist homogeneous polynomials $F_0, \dots, F_n \in K[X_0 \dots, X_m]$ satisfying the conditions (a), (b) and (c) of B.5, such that $\phi = (F_0 : \dots : F_n)$.

Another way to describe K-rational points, K-rational functions etc. on a variety which is defined over K is the following: Let $\mathcal{G}_{\bar{K}/K}$ be the Galois group of $\bar{K}/K$. The action of $\mathcal{G}_{\bar{K}/K}$ on $\bar{K}$ extends naturally to an action on the set of $\bar{K}$-rational points of the projective variety $V \subseteq P^n\left(\bar{K}\right)$ (defined over K), a point $P = (a_0 : \dots : a_n) \in V$ and an automorphism $\sigma \in \mathcal{G}_{\bar{K}/K}$; then $P^\sigma = (a_0^\sigma : \dots : a_n^\sigma)$. It is easily seen that

$$\begin{aligned} V(K) &= \{P \in V \mid P^\sigma = P \text{ for all } \sigma \in \mathcal{G}_{\bar{K}/K}\}\,, \\ K(V) &= \{f \in \bar{K}(V) \mid f^\sigma = f \text{ for all } \sigma \in \mathcal{G}_{\bar{K}/K}\}\,, \end{aligned} \tag{A.33}$$

and so on.

B.12. Curves over a Non-algebraically Closed Field. Consider a projective curve $V \subseteq \mathbf{P}^n\left(\bar{K}\right)$ which is defined over K (where K is perfect and $\bar{K}$ is the algebraic closure of K, as in B.11). Then the field $K(V)$ of K-rational functions on V is an algebraic function field of one variable over K, and $\bar{K}(V)$ is the constant field extension of $K(V)$ with $\bar{K}$.

A divisor $D = \sum_{P \in V} n_P P \in \mathcal{D}(V)$ is *defined over* K if $D^\sigma = D$ for all $\sigma \in \mathcal{G}_{\bar{K}/K}$ (this means that $n_{P^\sigma} = n_P$ for all $P \in V$). The divisors of V defined over K form a subgroup $\mathcal{D}(V/K) \subseteq \mathcal{D}(V)$. For $D \in \mathcal{D}(V/K)$, the space $\mathcal{L}_K(D)$ is given by

$$\mathcal{L}_K(D) = K(V) \cap \mathcal{L}(D)\,. \tag{A.34}$$

It is a finite-dimensional K-vector space, and its dimension (over K) equals the dimension of $\mathcal{L}(D)$ (over $\bar{K}$).

A divisor $Q \in \mathcal{D}(V/K)$ with $Q > 0$ is called a *prime divisor* of V/K if Q cannot be written as $Q = Q_1 + Q_2$ with effective divisors $Q_1, Q_2 \in \mathcal{D}(V/K)$. It is easily seen that the divisor group $\mathcal{D}(V/K)$ is the free abelian group generated by the prime divisors. Prime divisors of V/K correspond to the places of the function field $K(V)/K$; under this correspondence, prime divisors of degree one (i.e. K-rational points) of V correspond to the places of $K(V)/K$ of degree one.

Bibliography

[1] Rudin, Walter. Analýza v reálném a komplexním oboru. Praha: Academia, 1977. Chapter 15, p. 326.

[2] Silverman, Joseph H. The arithmetic of Elliptic Curves. New York: Springer Verlag, 1986.

[3] Husemöller,D.: Elliptic curves. Graduate texts in Mathematics, Springer Verlag, 2004

[4] Cox,D.A.: Primes of the Form $x^2 + ny^2$. Volume in Pure and Aplied Mathematics, A Wiley–interscience serves of texts, monographs and tracts, 1989

[5] Silvermann,J.H.: The Arithmethic of Elliptic Curves. Graduate texts in Mathematics 106, Springer Verlag, 1986

[6] Farhas,H., Kra,I.: Theta Constants, Riemann Surfaces and the Modular Group. Graduate Studies in Mathematics, Volume 37, AMS 2001