Algebraic Elliptic Curve and Analytic Theory of Elliptic Functions

Sachin Kumar
Faculty of Mathematics, Univeristy of Waterloo

April 2024

Abstract

The theory of elliptic curve's has been a integral part in pushing modern mathematics, particularly in the field of arithmetic geometry (using algebraic geometry techniques to solve problems in algebraic number theory) and cryptography (mainly elliptic curve and isogeny-based cryptography). There are many important conjectures based on elliptic curves (such as the Birch-Swinnerton Dyer Conjecture), and has helped to solve important problems (such as The Fermat's Last Theorem), whose implication led to the modern statement of the BSD conjecture. In this essay, I will give an overview on the important topics relating to the theory of elliptic curves and elliptic functions.

Contents

1 Algebraic curves

Let K denote a perfect field, i.e., every algebraic extension of K is separable, $\overline{K}$ denotes a fixed algebraic closure of K, $G_{\overline{K}/K}$ denote the Galois group of $\overline{K}/K$, P^σ denotes the action of $\sigma \in G_{\overline{K}/K}$ on the point P, C/K denotes a curve C defined over K, $\overline{K}(C)$ denotes the function field of C over $\overline{K}$, $K(C)$ denotes the function field of C over K. $\overline{K}[C]_P$ denotes the local ring of C at P (DVR when P smooth), and M_P denotes the maximal ideal of $\overline{K}[C]_P$.

Projective n-space. A projective n-space over $\overline{K}$, denoted as $\mathbb{P}^n$ or $\mathbb{P}^n(\overline{K})$, is the set of all $(n+1)$-tuples, $(x_0, \dots, x_n) \in \mathbb{A}^{n+1} = \{(y_1, \dots, y_{n+1}) : y_i \in \overline{K}\}$ such that at least one x_i is nonzero, modulo the equivalence relation $(x_0, \dots, x_n) \sim (y_0, \dots, y_n)$ if there exists a

$\lambda \in \overline{K}$ such that $x_i = \lambda y_i$ for all i. An equivalence class, $\{(\lambda x_0, \dots, \lambda x_n) : \lambda \in \overline{K}^*\}$ is denoted by $[x_0, \dots, x_n]$, and the individuals $x_0, \dots, x_n$ are called homogeneous coordinates for the corresponding point in $\mathbb{P}^n$.

Ideal $I \subset \overline{K}[X]$ is homogeneous if it is generated by homogeneous polynomials. A (projective) algebraic set : $V_I = \{P \in \mathbb{P}^n : f(P) = 0 \text{ for all homogeneous } f \in I\}$. (Homogeneous) ideal of V: $I(V)$ is the ideal of $\overline{K}[X]$ generated by $\{f \in \overline{K}[X] \text{ is homogeneous and } f(P) = 0 \text{ for all } P \in V\}$.

Projective algebraic set. A projective algebraic set is called a (projective) variety if its homogeneous ideal $I(V)$ is a prime ideal in $\overline{K}[X]$.

Dimension. Let V be a projective variety. The dimension of V, denoted as $\dim(V)$, is the transcendence degree of $\overline{K}(V \cap \mathbb{A}^n)$ over $\overline{K}$, where $V \cap \mathbb{A}^n \neq \emptyset$ is affine.

Nonsingular. Let V be a projective variety, let $P \in V$, and choose $\mathbb{A}^n \subset \mathbb{P}^n$ with $P \in \mathbb{A}^n$. Then, V is nonsingular (or smooth) at P if $V \cap \mathbb{A}^n$ is nonsingular at P. The local ring V at P, denoted by $\overline{K}[V]_P$, is the local ring of $V \cap \mathbb{A}^n$ at P.

$$\overline{K}[V]_P = \{F \in \overline{K}[V] \mid F = f/g,\ f, g \in \overline{K}[V] = \frac{\overline{K}[X]}{I(V)}, g(P) \neq 0\}$$

A function $F \in \overline{K}[V]$ is regular (or defined) at P if it is in $\overline{K}[V]_P$, in which case it makes sense to evaluate F at P. Curve means a projective variety of dimension one.

a. *Valuation*

Uniformizer. Let C be a curve and $P \in C$ be a smooth point. The normalized valuation on $\overline{K}[C]_P$ is given by,

$$\begin{aligned} \text{ord}_P &: \overline{K}[C]_P \to \{0, 1, 2, \dots\} \cup \{\infty\} \\ \text{ord}_P(f) &: \sup\{d \in \mathbb{Z} : f \in M_P^d\} \end{aligned}$$

Using $\text{ord}_P(f/g) = \text{ord}_P(f) - \text{ord}_P(g)$, we extend ord_P to $\overline{K}(C)$,

$$\text{ord}_P : \overline{K}(C) \to \mathbb{Z} \cup \infty$$

A uniformizer for C at P is any function $t \in \overline{K}(C)$ with $\text{ord}_P(t) = 1$, ie., a generator for the ideal M_P.

Let C and P be as above, and let $t \in \overline{K}(C)$. The order of f at P is $\text{ord}_P(f)$.

- if $\text{ord}_P(f) > 0$, then f has a zero at P.
- if $\text{ord}_P(f) < 0$, then f has a pole at P.
- if $\text{ord}_P(f) \geq 0$, then f is regular (or defined) at P and we can evaluate $f(P)$. Otherwise f has a pole at P and we write $f(P) = \infty$.

Let's take an example. Consider the curve $C : Y^2 = X^3 + X = X(X^2 + 1)$. Let $P = (0, 0)$. The maximal ideal M_P is generated by Y. Notice that $X = Y^2/(X^2 + 1) \in \langle Y \rangle$ as $1/(X^2 + 1)$ does not vanish at P. We see that the valuation on $\overline{K}[C]_P$ is $\mathrm{ord}_P(Y) = 1$, $\mathrm{ord}_P(X) = 2$ and $\mathrm{ord}_P(2Y^2 - X) = 2$.

Rational maps. Let $V_1, V_2 \subset \mathbb{P}^n$ be two projective varieties. A rational map from V_1 and V_2 is a map of the form,

$$\phi : V_1 \to V_2, \qquad \phi = [f_0, \dots, f_n]$$

where the functions $f_0, \dots, f_n \in \overline{K}(V_1)$ have the property that for every point $P \in V_1$ at which $f_0, \dots, f_n$ are all defined,

$$\phi(P) = [f_0(P), \dots, f_n(P)] \in V_2$$

A rational map $\phi : V_1 \to V_2$ is not necessarily a well-defined functions at every point $P \in V_1$. However, it may be possible to evaluate $\phi(P)$ at points at P of V_1 where some f_i is not regular by replacing each f_i by gf_i for an appropriate $g \in \overline{K}(V_1)$.

Morphism. A rational map $\phi = [f_1, \dots, f_n] : V_1 \to V_2$ is regular (or defined) at $P \in V_1$ if there is a function $g \in \overline{K}(V_1)$ such that each gf_i is regular at P; there is some i for which $(gf_i)(P) \neq 0$. If such a g exists, then we set $\phi(P) = [(gf_0)(P), \dots, (gf_n)(P)]$. It may be necessary to take different g's for different points. A rational map that is regular at every point is called a morphism.

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

Let's think about an example. Let C be smooth. $f, g \in \overline{K}(C)$. Then f and g define a morphism $\phi : C \to \mathbb{P}^2$, $\phi(P) = [f(P), g(P), 1]$.

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

Composition of ϕ. Let C_1/K and C_2/K be curves and let $\phi : C_1 \to C_2$ be a non constant rational map defined over K. Then composition with ϕ induces an injection of function fields fixing K, $\phi^* : K(C_2) \to K(C_1)$, $\phi^* f = f \circ \phi$.

Degree of ϕ. Let $\phi : C_1 \to C_2$ be a map of curves defined over K. If ϕ is constant, we define the degree of ϕ to be zero. Otherwise we say that ϕ is a finite map and we define its degree to be $\deg \phi = [K(C_1) : \phi^* K(C_2)]$.

Divisor Group. The divisor group of a curve C, denoted by $\mathrm{Div}(C)$, is the free abelian group generated by the points of C. Thus a divisor $D \in \mathrm{Div}(C)$ is a formal sum,

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

where $n_P \in \mathbb{Z}$ and $n_P = 0$ for all but finitely many $P \in C$. The degree of D is defined by,

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

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

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

Divisor of f. Let $f \in \overline{K}(C)^*$. Then we define the divisor of f by,

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

Picard Group. A divisor $D \in \mathrm{Div}(C)$ is principal if it has the form $D = \mathrm{div}(f)$ for some $f \in \overline{K}(C)^*$. Two divisors are linearly equivalent, written $D_1 \sim D_2$, if $D_1 - D_2$ is principal. The divisor class group (or Picard group) of C, denoted by $\mathrm{Pic}(C)$, is the quotient of $\mathrm{Div}(C)$ by its subgroup of principal divisors.

Proposition. Let C be a smooth curve and let $f \in \overline{K}(C)^*$. Then $\mathrm{div}(f) = 0$ if and only if $f \in \overline{K}^*$ and $\deg(\mathrm{div}(f)) = 0$.

Let's think about an example. Assume that $\mathrm{char}(K) \neq 2$. Let $e_1, e_2, e_3 \in \overline{K}$ be distinct, and consider the curve, $C : y^2 = (x - e_1)(x - e_2)(x - e_3)$. One can check that C is smooth and that it has a single point at infinity, which we denote by P_∞. For $i = \{1, 2, 3\}$, let $P_i = (e_i, 0) \in C$. Then $\mathrm{div}(x - e_i) = 2(P_i) - 2(P_\infty)$ and $\mathrm{div}(y) = (P_1) + (P_2) + (P_3) - 3(P_\infty)$. The above definitions and proposition may be summarized by saying that there exists an exact sequence,

$$1 \to \overline{K}^* \to \overline{K}(C)^* \xrightarrow{\mathrm{div}} \mathrm{Div}^0(C) \to \mathrm{Pic}^0(C) \to 0$$

2 Elliptic Curves

Definition. An elliptic curve is a pair $(E, \mathcal{O})$ consisting of a smooth curve E of genus one, with a distinguished point $\mathcal{O} \in E$.

The interest in elliptic curves arises from their fundamental value to many areas of mathematics. From the point of view of number theory, elliptic curves turn to have many remarkable properties. The set of rational points of an elliptic curve defined over $\mathbb{Q}$ has the structure of a finitely generated abelian group, which may be of infinite cardinality. The situation with regard to rational points is vastly different from that of higher genus curves by virtue of the following theorem.

Theorem (Faltings). Let C be a smooth curve of genud, $g > 1$ defined over $\mathbb{Q}$. Then $C(\mathbb{Q}) < \infty$, ie., finite.

Further, elliptic curves defined over number fields have remarkable connections to the class

groups of number fields and the problem of studying abelian extensions of number fields. From the point of view of complex analysis, elliptic curves defined over $\mathbb{C}$ are precisely Riemann surfaces of genus one and are complex tori. The moduli space of elliptic curves also has deep connections with quotients of the upper half plane, which we will discuss in the later sections. From the point of algebraic geometry, elliptic curves form a useful class of curves on which a lot of geometric phenomena can be exhibited. A main tool that we will use in what follows is the Riemann-Roch Theorem which we state for genus one curves.

Theorem (Riemann-Roch). Let C be a smooth curve of genus one and let K_C be a canonical divisor on C. Then for any $D \in DG(\mathbb{C})$ we have,

$$\ell(D) - \ell(K - D) = \deg(D) - g + 1$$

Typically, the number $\ell(D)$ is the one of interest, while $\ell(K - D)$ is thought of as a correction term, called index of speciality. Because it is the dimension of a vector space, the correction term $\ell(K - D)$ is always non-negative, so that $\ell(D) \geq \deg(D) - g + 1$. This is called Riemann's inequality. Recall, that the spaces $\mathcal{L}(D)$ keep track of functions of C which prescribed zeroes and poles data. In particular, $\mathcal{L}(nP)$ contains all functions f such that f is regular everywhere possibly at P, where it has no worse that a pole of order n.

Corollary. Let $\mathbb{C}$ be a smooth curve with genus, $g = 1$, K_C be a canonical divisor and $D \in \mathrm{Div}(C)$. Then,

(a) $\ell(K_C) = 0$.

(b) $\deg K_C = 0$.

(c) If $\deg D > 0$, then $\ell(D) = \deg D$.

Often times while working with a curve C defined over K, we are interested in studying divisors D that defined over K. This is to say that,

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

where the sum is taken over K-rational points of the curve C. In conjunction, we are also interested in the K-vector space, $\mathcal{L}_K(D)$ which is defined as, $\mathcal{L}_K(D) = \{f \in K(C)^* : \mathrm{div}(f) + D \geq 0\} \cup \{0\}$. Note that $\mathcal{L}_K(D)$ is a finite dimensional K-vector space due to the existence of a natural embedding,

$$\iota : \mathcal{L}_K(D) \otimes_K \overline{K} \hookrightarrow \mathcal{L}(D)$$

of $\overline{K}$-vector space.

Corollary. Let C be a curve defined over K and D be a divisor defined over K. Then the map ι is an isomorphism of $\overline{K}$-vector spaces. In particular, $\dim_K \mathcal{L}_K(D) = \ell(D)$

The corollary amounts to saying that we may find a basis of the $\overline{K}$-vector space $\mathcal{L}(D)$ consisting of functions, in $K(C)^*$.

a. *The Weierstrass Form of E/K*

Proposition. Let $\mathrm{char} K \geq 5$ and E/K be an elliptic curve. Then there exists functions $x, y \in K(E)$ such that the mapping, $\phi : E \to \mathbb{P}^2$, $P \longmapsto \phi(P) := [x(P) : y(P) : 1]$,

gives an isomorphism of E to a curve in $\mathbb{P}^2$, which in homogenous coordinates is given by $Y^2Z = X^3 + aXZ^2 + bZ^3$ where $a, b \in K$.

In the proof of the above proposition, we wouldn't mention why the image curve C is smooth. This is because if C was non-smooth then it would admit a birational map to $\mathbb{P}^1$ which would imply that E is birational to $\mathbb{P}^1$. This cannot hold since E has genus one while $\mathbb{P}^1$ has genus zero. The proof of this fact relies on the study of singular Weierstrass equations. Concept's get complicated when the char$K = 2, 3$, In these lower characteristics, elliptic curves will continue to have similar properties but the computational proofs of these facts will be harder. We will discuss theories in char$K \geq 5$ to get simpler computations and formulae. The proposition, shows us that any elliptic curve, $E/K \cong E$, where $E \subset \mathbb{P}^2$ is a smooth curve, defined by a Weierstrass equation, $E : Y^2Z = X^3 + aXZ^2 + bZ^3$, where $a, b \in K$. In practice, we prefer to de-homogenize with respect to Z and look at the affine curve, $E : y^2 = ax^3 + bx + c$, which we refer to as the Weierstrass equation associated to E/K while always remembering that we have a point at infinity given by $\mathcal{O} = [0 : 1 : 0]$.

b. *Properties of the Weierstrass Form and the j-invariant*

Assume that char$K \geq 5$.

Smoothness. Since E is smooth, then the Weierstrass equation must describe a smooth curve. This is equivalent to requiring that the polynomial $x^3 + ax + b$ has no repeated roots. This can be seen for instance by using the Jacobian criterion of smoothness. By computing the cubic discriminant, d we see that, $x^3 + ax + b$ has has no repeated roots $\iff 4a^3 + 27b^2 \neq 0$. To prove that the Weierstrass equation is smooth, we must prove that the equation describes a genus one curve. We compute the canonical class by studying the differential given by

$$\omega = \frac{dx}{y}$$

In fact the differential ω is both holomorphic and non-vanishing. This implies that the divisor $\text{div}(\omega) = 0$ and in particular the canonical class is trivial. A corollary of the Riemann-Roch tells us that the degree of any canonical divisor is given by $2g - 2$. Since 0 is canonical in our case, clearly $g = 1$. Hence any smooth Weierstrass equation describes a genus one curve, which along with the point at infinity $\mathcal{O}$ forms an elliptic curve. Thus, elliptic curves are curves described by a smooth Weierstrass equation,

$$E : y^2 = x^3 + ax + b, \qquad 4a^3 + 27b^2 \neq 0$$

with a point at infinity $\mathcal{O} = [0 : 1 : 0]$. The differential $\omega = dx/y$ associated to an elliptic curve will be useful and is known as the invariant differential of an elliptic curve.

Uniqueness of the Weierstrass Form. Let E be an elliptic curve which is isomorphic to the two following Weierstrass equations, $E : y^2 = x^3 + ax + b$ and $E' : y'^2 = x'^3 + a'x' + b'$. Then these two equations are related by a very simple change of coordinates.

Proposition. Let E be an elliptic curve given by the two Weierstrass equations as above.

Then the two equations are related by the change of coordinates, $x = u^2x' + r$ and $y = u^3y' + su^2x' + t$, where $u \in \overline{K}^*$ and $r, s, t \in \overline{K}$.

It is also possible to compute when two Weierstrass equations will yield isomorphic elliptic curves.

j-invariant. Let E be an elliptic curve. Then we define the j-invariant of the curve E,

$$j(E) = 1728\frac{4a^3}{d}$$

where, d is the discriminant of E.

The above quantity j is conceptually elegent, such that it describs the isomorphism type of an elliptic curve.

Proposition. Let E and E' be elliptic curves. Then $E \cong E'$ if and only if $j(E) = j(E')$.

c. *Group Law*

Group $\mathrm{Pic}^0(E)$. The points of an elliptic curve naturally admit a group structure, where the point $\mathcal{O}$ will serve as the identity element. To show this we first recall that on any curve there is a map, $\mathrm{div} : \overline{K}(C)^* \to \mathrm{Div}^0(C)$, $f \longmapsto \mathrm{div}(f)$, where $\mathrm{Div}^0(C)$ denotes the subgroup of divisors of degree zero on C. We denote by $\mathrm{Pic}^0(C)$, the co-kernel of the above map div. In particular

$$\mathrm{Pic}^0(C) = \frac{\{\text{divisors of degree 0}\}}{\text{principal divisors}}$$

We compute $\mathrm{Pic}^0(E)$ for an elliptic curve E. We define the following map, $\sigma : E \to \mathrm{Pic}^0(E)$, $P \longmapsto \{\text{divisor class of } P - \mathcal{O}\}$.

Proposition. The map $\sigma : E \to \mathrm{Pic}^0(E)$ is an isomorphism.

PROOF. Showing σ is an injective map is trivial, so we will restrict ourselves in showing that σ is surjective. Let $D \in \mathrm{Div}^0(E)$ be any divisor of degree zero. Consider the space $\mathcal{L}(D + \mathcal{O})$ which has dimension 1 by the Riemann-Roch theorem. Let us assume $f \in \overline{K}(E)^*$ generates $\mathcal{L}(D + \mathcal{O})$. Then, $\mathrm{div}(f) \geq -\mathcal{O} - D$ by definition. Further since f has degree zero, it must be that $\mathrm{div}(f) = P - \mathcal{O} - D$, for some point $P \in E$. This proves that $D \sim P - \mathcal{O}$ and hence the map is surjective. □

The abstract group law. We use the bijection σ between the points of an elliptic curve and the abelian group $\mathrm{Pic}^0(E)$ to transfer the group structure of $\mathrm{Pic}^0(E)$ to the set of points of E. Explicitly, the addition in this group law is given as follows: Let $P, Q \in E$, we define $P + Q$ as the unique point on E such that, $P - \mathcal{O} + Q - \mathcal{O} \sim (P + Q) - \mathcal{O}$, where $\sim$ denotes linear equivalence of divisors. The inverse of a point P is defined as the unique point $-P$ such that $\mathcal{O} - P \sim (-P) + \mathcal{O}$. One also checks that the point $\mathcal{O}$ becomes the identity element for

the group law. Since $\mathrm{Pic}^0(E)$ is abelian, we see that the above group law on the points of E is abelian too.

The explicit group law. We study the group law in a more explicit fashion. Let $E : y^2 = x^3 + ax + b$ be an elliptic curve.

Inversion. Let $P \in E$, and let $L(X, Y, Z) = \alpha X + \beta Y + \gamma Z = 0$ be the line in $\mathbb{P}^2$ joining P and $\mathcal{O}$, the point at infinity. If $P = (x_0, y_0)$ then the line L is given by $L : X - x_0(Z) = 0$, or in the affine plane it is the vertical line $x = x_0$. Since E is a degree three curve, the line L intersects E at three points (after counting multiplicities). This is a special case of Bezout's theorem.

Let Q denote the third point of intersection of L and E. Notice that the line $Z = 0$ intersects E at $\mathcal{O}$ with multiplicity three. We define the function, $f \in \overline{K}(E)^*$ as, $f = \frac{L}{Z}$ and notice that $\mathrm{div}(f) = P+Q+\mathcal{O}-3\mathcal{O} = P+Q-2\mathcal{O}$. This proves that, $\mathcal{O}-P \sim Q-\mathcal{O}$. Hence $Q = -P$.

Addition. Let $P, Q \in E$ and let $L(X, Y, Z)$ denote the equation of the line joining P and Q. Let R denote the third intersection point of L and E. We again consider $f = L/Z$ and see that,

$$\mathrm{div}(f) = P + Q + R - 3\mathcal{O} \implies P - \mathcal{O} + Q - \mathcal{O} \sim \mathcal{O} - R$$

This shows that the sum $P + Q$ is given by the inverse of the point R.

d. *Explicit formulae*

We have defined an abstract group law on the set of points of E but it is not clear that the induced addition map, $+ : E \times E \to E$ and inversion map $- : E \to E$ are morphisms of algebraic varieties. We tackle this problem by using the explicit descriptions using rational functions for addition and multiplication, which shows that the group law we have found is indeed algebraic.

Proposition. The inversion map for the curve $y^2 = x^3 + ax + b$ is given by, $- : E \to E$, $(x_0, y_0) \longmapsto (x_0, -y_0)$, with $-\mathcal{O} = \mathcal{O}$ in addition.

The above explicit description shows us that the inversion map is indeed a morphism of algebraic varieties. The addition map is slightly more computational to describe. Let (x_1, y_1) and (x_2, y_2) be two points on $E : y^2 = x^3 + ax + b$. The case is trivial, when one (or both) of the points is $\mathcal{O}$. Let λ denote the slope of the line joining these points. We define λ to be the slope of the tangent to curve E at this point if the two points are the same. Clearly λ is a rational function, of x_1, y_1, x_2 and y_2.

Proposition. Let $P, Q \in E$ and λ be as above. Then, $P + Q$ is the point,

$$P + Q = (\lambda^2 - x_1 - x_2, -\lambda x_3 - \nu)$$

The description of the addition map in terms of rational functions shows that it is a morphism of algebraic varieties. In particular, E has the structure of an abelian variety. That is,

a variety equipped with an abelian group law that is algebraic i.e. the addition and inversion maps are morphisms of varieties as above.

e. *Isogeny*

An isogeny is the notion of morphism in the category of elliptic curves.

Isogeny. Let E_1 and E_2 be elliptic curves with distinguished points $\mathcal{O}_1$ and $\mathcal{O}_2$. An isogeny from E_1 to E_2 is a morphism of varieties $\phi : E_1 \to E_2$ such that $\phi(\mathcal{O}_1) = \mathcal{O}_2$.

Analogous, to the definition of elliptic curve, we have defined an isogeny without making any reference to the group structure. It turns out all isogenies are group homomorphisms. If $\phi : E_1 \to E_2$ is a non-constant isogeny, we have an induced group homomorphism,

$$\begin{aligned} \phi^* = \mathrm{Pic}^0(E_2) &\to \mathrm{Pic}^0(E_1) \\ Q &\longmapsto \sum_{\phi(P)=Q} e_\phi(P)P \end{aligned}$$

We have a group isomorphism,

$$\begin{aligned} \sigma_1 : E_1 &\to \mathrm{Pic}^0(E_1) \\ P &\longmapsto P - \mathcal{O}_1 \end{aligned}$$

and similarly for E_2. By the above, we have a group homomorphism,

$$E_2 \xrightarrow{\sigma_2} \mathrm{Pic}^0(E_2) \xrightarrow{\phi^*} \mathrm{Pic}^0(E_1) \xrightarrow{\sigma_1^{-1}} E_1$$

Let $\hat{\phi} = \sigma_1^{-1} \circ \phi^* \circ \sigma_2$. Then $\hat{\phi} \circ \phi = [\deg \phi]$, and $\hat{\phi}$ is the unique isogeny with this property. Let's formalize our intuition.

Proposition. Let $\phi : E_1 \to E_2$ be an isogeny. Then, given points $P, Q \in E_1$, we have, $\phi(P + Q) = \phi(P) + \phi(Q)$. In particular, any isogeny is a group homomorphism.

PROOF. Consider the following commutative diagram,

$$\begin{array}{ccc} E_1 & \xrightarrow[\sigma_1]{} & \mathrm{Pic}^0(E_1) \\ \downarrow{\scriptstyle \phi} & & \downarrow{\scriptstyle \phi_*} \\ E_2 & \xrightarrow[\sigma_2]{} & \mathrm{Pic}^0(E_2) \end{array}$$

where $\phi_* : \mathrm{Pic}^0(E_1) \to \mathrm{Pic}^0(E_2)$ is the induced by the natural push-forward map of divisors given by,

$$\phi_* \left(\sum_{P \in E_1} n_P P \right) = \sum_{P \in E_2} n_P \phi(P)$$

since, ϕ_* is a group morphism and σ_1 and σ_2 are group isomorphisms by definition, it follows that ϕ is also a group morphism. □

Definition. If ϕ is a non-constant isogeny, we define the degree of an isogeny to be the degree of the ϕ as a map of curves. If ϕ is a constant isogeny, then we define $\deg \phi = 0$.

The constant map, $\phi : E_1 \to E_2$ given by $\phi(P) = \mathcal{O}_2$ for all $P \in E_1$ and the identity map $\mathrm{id}_E : E \to E$ are isogenies of degree 0 and 1 respectively. The multiplication-by-n maps given by $[n] : E \to E$,

$$P \longmapsto \underbrace{P + \cdots + P}_{n \text{ times}}$$

is an isogeny. We will say more about $\deg[n]$ later.

Frobenius morphism. Let an elliptic curve E over a finite field, denoted as $E/\mathbb{F}_p$ be an elliptic curve given by, $y^2 = x^3 + ax + b$, where $a, b \in \mathbb{F}_p$. We define a map $\phi : E \to E$ given on homogenous coordinates by $[X : Y : Z] \longmapsto [X^p : Y^p : Z^p]$. Since, $\phi(\mathcal{O}) = \mathcal{O}$, it is clearly an isogeny. Further the degree of this isogeny is p. The map ϕ is known as the Frobenius morphism.

f. *Dual Isogenies*

Dual Isogeny. Let $\phi : E_1 \to E_2$ be a non-constant isogeny. The isogeny $\hat{\phi}$ defined above is called the dual isogeny of ϕ. We define $[\hat{0}] = [0]$.

PROOF. We will first prove the uniqueness, let $m = \deg \phi$ and suppose $\hat{\phi}$ and $\hat{\phi}'$ are isogenies such that $\hat{\phi} \circ \phi = \hat{\phi}' \circ \phi = [m]$. Then,

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

so $\hat{\phi} - \hat{\phi}'$ is constant. Then Reduce to the case where ϕ is either separable or a Frobenius morphism. Separable case follows from results about isogenies in III.4. If K has characteristic p, assume ϕ is the p^{th} -power morphism, i.e. $\deg \phi = p$. $[p]$ is not separable, so can be decomposed as $[p] = \psi \circ \phi^e$. □

Properties of Dual Isogenies. Let $\phi, \psi : E_1 \to E_2$ and $\lambda : E_2 \to E_3$ be isogenies. Let $m = \deg \phi$.

(a) $\hat{\phi} \circ \phi = [m]$ on E_1 and $\phi \circ \hat{\phi} = [m]$ on E_2
(b) $\widehat{\lambda \circ \phi} = \hat{\lambda} \circ \hat{\phi}$
(c) $\widehat{\phi \hat{+} \psi} = \hat{\phi} + \hat{\psi}$
(d) For all $n \in \mathbb{Z}$, $[\hat{n}] = [n]$, and $\deg[n] = n^2$
(e) $\deg \hat{\phi} = \deg \phi$
(f) $\hat{\hat{\phi}} = \phi$

PROOF. We will prove that $[\hat{n}] = [n]$ and $\deg[n] = n^2$. Clearly holds for $n = 0$ and $n = 1$. Applying part 3 with $\phi = [n]$ and $\psi = [1]$ gives,

$$[n \hat{+} 1] = [\hat{n}] + [\hat{1}]$$

and by ascending and descending induction we see that $[\hat{n}] = [n]$ for all $n \in \mathbb{Z}$. Now let $d = \deg[n]$. Then,

$$[d] = [\hat{n}] \circ [n] = [n]^2$$

since the endomorphism ring of an elliptic curve is torsion-free as a $\mathbb{Z}$-module, this shows that $d = n^2$. □

Quadratic Forms. A positive definite quadratic form is a function $d : A \to \mathbb{R}$, where A is an Abelian group, such that

(a) $d(\alpha) = d(-\alpha)$, for all $\alpha \in A$.

(b) The pairing, $A \times A \to \mathbb{R}$,

$$(\alpha, \beta) \longmapsto d(\alpha + \beta) - d(\alpha) - d(\beta)$$

is bilinear.

(c) $d(\alpha) \geq 0$ for all $\alpha \in A$, with equality precisely when $\alpha = 0$.

Corollary (Degree Map). Let E_1 and E_2 be elliptic curves. The degree map,

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

is a positive definite quadratic form.

Torsion Subgroup Structure. Let E be an elliptic curve and $m \in \mathbb{Z} \setminus \{0\}$.

(a) If $m \neq 0$ in K, ie., if $\mathrm{char}(K) = 0$ or p and $p \nmid m$, then $E[m] = \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$.

(b) If $\mathrm{char}(K) = p$, then one of the following holds:

$$E[p^e] = \{\mathcal{O}\} \text{ for all } e \in \mathbb{Z}_+$$
$$E[p^e] = \mathbb{Z}/p^e\mathbb{Z} \text{ for all } e \in \mathbb{Z}_+$$

PROOF. Since, $m \neq 0$ and $\deg[m] = m^2$, $[m]$ is separable and $\#E[m] = m^2$. Further, for every $d \mid m$, we have $\#E[d] = d^2$. Analyzing the structure theorem of finitely generated Abelian groups gives the result. Let ϕ be the p^{th}-power Frobenius morphism. Using various results from Chapters 2 and 3, we have $\#E[p^e] = \deg_s[p^e] = (\deg_s \hat{\phi})^e$. If $\hat{\phi}$ is inseparable then $\deg_s \hat{\phi} = 1$, so $\#E[p^e] = 1$ for all e. Otherwise, $\deg_s \hat{\phi} = p$, so $\#E[p^e] = p^e$, and the structure theorem again gives the result. □

3 The Weil Pairing

Throughout, let $m \geq 2$ be coprime to $\mathrm{char}(K)$. We saw that $E[m]$ is a free $\mathbb{Z}/m\mathbb{Z}$-module of rank 2. We wish to define a non-degenerate, alternating, bilinear pairing on $E[m]$ which is basis-free and Galois invariant:

Galois Invariance. Let $P, Q \in E[m]$ and $\sigma \in G_{\overline{K}/K}$. A Galois-invariant pairing on $E[m]$ is a map $e_m : E[m] \times E[m] \to R$ such that,

$$e_m(P^\sigma, Q^\sigma) = e_m(P, Q)^\sigma$$

We will know construct the Weil pairing. Recall that a divisor $\sum n_i P_i$ on a curve is the divisor of a function if and only if both $\sum n_i = 0$ and $\sum [n_i]P_i = \mathcal{O}$. Let $T \in E[m]$. By the above, there is an $f \in \overline{K}(E)$ such that, $\mathrm{div}(f) = mT - m\mathcal{O}$. Since, $[m]$ is non-constant, hence surjective, let $T' \in E$ satisfy $[m]T' = T$. There is similarly a function $g \in \overline{K}(E)$ such that,

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

$f \circ [m]$ and g^m have the same divisor, so up to a constant multiple, we have $f \circ [m] = g^m$. Now, let $S \in E[m]$. For any $P \in E$, we have

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

Thus, as a function of P, $\frac{g(P+S)}{g(P)}$ is the m^{th} root of unity in K, of which there are finitely many. In particular, the morphism

$$\begin{aligned} E &\to \mathbb{P}^1 \\ P &\longmapsto \frac{g(P+S)}{g(P)} \end{aligned}$$

is not surjective, so it is constant.

The Weil e_m-Pairing. The Weil e_m-Pairing is defined as,

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

We have now constructed the Weil-pairing, but what properties does it have? The Weil-pairing is bilinear, alternating, where $e_m(T,T) = 1$ so in particular, $e_m(S,T) = e_m(T,S)^{-1}$. It is non-degenerate pairing, ie., if $e_m(S,T) = 1$ for all $S \in E[m]$, $T = \mathcal{O}$. It is closed under the galois invariance, ie., $e_m(S,T)^\sigma = e_m(S^\sigma, T^\sigma)$, for all $\sigma \in G_{\overline{K}/K}$. Finally, it is compatibile, ie., $e_{mm'}(S,T) = e_m([m']S, T)$, for all $S \in E[mm']$ and $T \in E[m]$.

Dual Isogenies are Adjoints. Let $\phi : E_1 \to E_2$ be an isogeny. Then for all $S \in E_1[m]$ and $T \in E_2[m]$,

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

a. *Tate Module of E*

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

$$T_\ell(E) = \varprojlim E[\ell^n]$$

where the inverse limit is taken with respect to the maps $E[\ell^{n+1} \to E[\ell^n]$, $T \longmapsto [\ell]T$. Since each $E[\ell^n]$ is $\mathbb{Z}/\ell^n\mathbb{Z}$-module, $T_\ell(E)$ is a $\mathbb{Z}_\ell$-module.

Analogously, if μ_{ℓ^n} is the multiplicative group of $(\ell^n)^{\text{th}}$ roots of unity in $\overline{K}^*$, then we have maps $\mu_{\ell^{n+1}} \to \mu_{\ell^n}, \zeta \mapsto \zeta^n$. The Tate module of K is then defined as,

$$T_\ell(\mu) = \varprojlim \mu_{\ell^n}$$

Structure of the Tate Module. $T_\ell(E) \cong \mathbb{Z}_\ell \times \mathbb{Z}_\ell$ as a $\mathbb{Z}_\ell$-module if $\ell \neq \text{char}(K)$. $T_p(E) \cong \{0\}$ or $\mathbb{Z}_p$ as a $\mathbb{Z}_p$-module if $p = \text{char}(K) > 0$.

Corollary. Let E_1 and E_2 be elliptic curves. Then the $\text{Hom}(E_1, E_2)$ is a free $\mathbb{Z}$-module of a rank at most 4.

ℓ-adic Weil Pairing. There exists a pairing,

$$e : T_\ell(E) \times T_\ell(E) \to T_\ell(\mu)$$

which is bilinear, alternating, non-degenerate, Galois-invariant, and for which taking dual isogenies is an adjoint operation.

b. *Endomorphism Rings*

Let's discuss the structure of endomorphism rings of elliptic curves. Let E be an elliptic curve, and $\text{End}(E)$ denote its endomorphism ring. We have amassed the following facts: $\text{End}(E)$ has characteristic 0, no zero divisors, and rank at most 4 as a $\mathbb{Z}$-module. $\text{End}(E)$ has an anti-involution $\phi \mapsto \hat{\phi}$. For all $\phi \in \text{End}(E)$, $\phi \circ \hat{\phi} \in \mathbb{Z}_{\geq 0}$, with $\phi \circ \hat{\phi} = 0$ if and only if $\phi = 0$. These properties greatly restrict the structure of $\text{End}(E)$ and allow us to characterize endomorphism rings of elliptic curves.

Order of $\mathbb{Q}$-algebras. Let A be a (not necessarily commutative) $\mathbb{Q}$-algebra which is finitely generated over $\mathbb{Q}$. An order of A is a subring R of A that is finitely generated as a $\mathbb{Z}$-module such that $R \otimes \mathbb{Q} = A$.

Let's analyse an example. Let K be be an imaginary quadratic field with ring of integers Ok. Then for each integer $n \geq 1$,the ring $\mathbb{Z} + n\mathcal{O}_K$ is an order of K. In fact, one can show that these are the only orders of K.

Quaternion Algebras. A $\mathbb{Q}$-algebra A is called a quaternion algebra if,

$$A = \mathbb{Q} + \mathbb{Q}\alpha + \mathbb{Q}\beta + \mathbb{Q}\alpha\beta$$

where $\alpha^2, \beta^2 \in \mathbb{Q}_-$ and $\beta\alpha = -\alpha\beta$.

Structure of Endomorphism Rings of Elliptic Curves. Let E be an elliptic curve over the field K. Then $\text{End}(E)$ is either $\mathbb{Z}$, an order in an imaginary quadratic field, or an order in a quaternion algebra. If $\text{char}(K) = 0$, then only the first two are possible.

Complex Multiplication (CM). If $\text{char}(K) = 0$, we say that E has complex multiplication, or is CM, if $\text{End}(E) \supsetneq \mathbb{Z}$, ie., $|\text{End}(E)| > |\mathbb{Z}|$.

Supersingular. If $\text{char}(K) > 0$, we say that E is supersingular if $\text{End}(E)$ is an order in a quaternion algebra, and otherwise we call E ordinary.

If $K = \mathbb{F}_q$, a finite field of order $q = p^e$ for a prime p, then Chapter 5 shows that $\text{End}(E)$ is always larger than $\mathbb{Z}$, and that there are always elliptic curves with $\text{End}(E) \otimes \mathbb{Q}$ a quaternion algebra. A comprehensive description of $\text{End}(E)$ in all cases is given in [Deuring].

c. *Inverse Galois Theory*

Inverse Galois Problem. Let G be a finite group. Find a finite Galois extension $K/\mathbb{Q}$ such that $\text{Gal}(K/\mathbb{Q}) \cong G$.

A systematic study began in 1892 with Hilbert. A group for which the inverse Galois property holds is called ***realizable***. This is equivalent to the inverse Galois problem over $\mathbb{Q}(t)$. The conjecture is resolved over $\mathbb{C}(t)$, $\overline{\mathbb{Q}}(t)$, and $\overline{\mathbb{Q}}$. Examples of realizable groups are finite solvable groups, sporadic simple groups (except possibly M_{23}), permutation groups of degree up to 16 and rigid groups.

Absolute Galois Group. Let F be a field and F^{sep} a separable closure of F. The absolute Galois group of F, denoted by G_F, is the Galois group $\text{Gal}(F^{\text{sep}}/F)$. When F is perfect field (finite or characteristic 0), $F^{\text{sep}} = \overline{F}$. Now, the inverse Galois problem can be rephrased as follows:

Inverse Galois Problem. Let G be a finite group. Find a normal subgroup H of $G_{\mathbb{Q}}$ such that $G_{\mathbb{Q}}/H \cong G$.

What about the structure of the Galois Group, $G_{\mathbb{Q}}$? $G_{\mathbb{Q}}$ is a profinite group with the profinite topology. We can view,

$$G_{\mathbb{Q}} \subseteq \prod_i \text{Gal}(K_i/\mathbb{Q}) \tag{1}$$

$G_{\mathbb{Q}}$ is a compact, Hausdorff, totally disconnected topological group. The Langlands program, study the representations of $G_{\mathbb{Q}}$, known as Galois representations. Class field theory is the 1-dimensional case. What is our Goal? It is to realize Galois groups as matrix groups via representations arising from elliptic curves.

d. *Representations of Galois Groups*

We will know discuss representations, when $K = \mathbb{Q}(E[n])$. Let $n \geq 1$ and $E/\mathbb{Q}$ be an elliptic curve. We know $E[n]$ has n^2 points; let $E[n] = \{\mathcal{O}, (x_1, y_1), \ldots, (x_m, y_m)\}$, where $[x_i : y_1 : 1] \in E[n]$ and $m = n^2 - 1$. Let $K = \mathbb{Q}(E[n]) := \mathbb{Q}(x_1, y_1, \ldots, x_m, y_m)$. $K/\mathbb{Q}$ is algebraic, so $nP : P \oplus \cdots \oplus P = \mathcal{O}$, and addition on E is algebraic. $K/\mathbb{Q}$ is also Galois (extend field automorphisms component-wise). Since $E[n] \cong \mathbb{Z}/n\mathbb{Z} \oplus \mathbb{Z}/n\mathbb{Z}$, we can write $E[n] = \{a_1P_1 + a_2P_2 \mid a_1, a_2 \in \mathbb{Z}/n\mathbb{Z}\}$ for some generators P_1 and P_2. Let $\sigma \in \text{Gal}(K/\mathbb{Q})$.

Then,

$$\sigma(P_1) = \alpha_\sigma P_1 + \gamma_\sigma P_2$$
$$\sigma(P_2) = \beta_\sigma P_1 + \delta_\sigma P_2$$

for some $\alpha_\sigma, \dots, \delta_\sigma \in \mathbb{Z}/n\mathbb{Z}$. Define the map

$$\rho_n = \mathrm{Gal}(K/\mathbb{Q}) \to GL_2(\mathbb{Z}/n\mathbb{Z})$$

by,

$$\rho \longmapsto \begin{bmatrix} \alpha_\sigma & \beta_\sigma \\ \gamma_\sigma & \delta_\sigma \end{bmatrix}$$

Example. Let $E : y^2 = x^3 + x$ be defined over $\mathbb{Q}$. Then,

$$E[2] = \{\mathcal{O}, (0,0), (i,0), (-i,0)\}$$

so $K := \mathbb{Q}(E[2]) = \mathbb{Q}(i)$ and $\mathrm{Gal}(K/\mathbb{Q}) = \{\mathrm{id}_K, \sigma\}$, where σ is a complex conjugation. Can take generators of $E[2]$ to be $(0,0)$ and $(i,0)$, so

$$\rho_2(\mathrm{id}_K) = 1$$
$$\rho_2(\sigma) = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$$

In particular, ρ_2 is injective. Note that $GL_2(\mathbb{F}_2) \cong S_3$.

e. *Serre's Open Image Theorem*

We will continue with representations, when $K = \mathbb{Q}(E[n])$. Let $n \geq 1$, ρ_n is always injective. If ρ_n is also surjective, then $GL_2(\mathbb{Z}/n\mathbb{Z})$ is realizable. This leads to a celebrated theorem of Serre:

Open Image Theorem. Let $E/\mathbb{Q}$ be an elliptic curve which is not CM. Then,

(a) There is an $M_E \in \mathbb{Z}_+$, which depends on E, such that for all $n \geq 1$,

$$[GL_2(\mathbb{Z}/n\mathbb{Z}) : \rho_n(\mathrm{Gal}(K/\mathbb{Q}))] < M_E$$

(b) There is an $N_E \in \mathbb{Z}_+$, depending on E, such that for all $n \geq 1$ with $\gcd(n, N_E) = 1$, ρ_n is an isomorphism.

Open Image Theorem (V2). Let $E/\mathbb{Q}$ be an non-CM elliptic curve and

$$\rho_E : G_\mathbb{Q} \to GL_2(\hat{\mathbb{Z}})$$

be the representation of $G_\mathbb{Q}$ induced by the ρ_n, called adelic representation of E. Then $\rho_E(G_\mathbb{Q})$ is open in $GL_2(\hat{\mathbb{Z}})$.

In a profinite group, open subgroups are precisely the closed subgroups of finite index. We will know discuss, the Effective Open Image Theorem,

(Jones, 2010). The adelic representations of almost all $E/\mathbb{Q}$ have index 2 (called a Serre curve).

(Lombardo, 2014). Let E/K be a non-CM elliptic curve. Then,

$$[GL_2(\hat{\mathbb{Z}}) : \rho_E(G_K)] < C_1 \cdot [K : \mathbb{Q}]^{C_2} \cdot \max\{1, h(E), \log, [K : \mathbb{Q}]\}^{2C_2}$$

where $C_1 = \exp(6.4 \times 10^{13})$, $C_2 = 24480$, and $h(E)$ is the stable Faltings height of E.

Uniformity Conjecture (Serre). There is some $M \in \mathbb{Z}_+$, such that

$$[GL_2(\mathbb{Z}/n\mathbb{Z}) : \rho_n(\mathrm{Gal}(K/\mathbb{Q}))] < M$$

for all $n \geq 1$ and all non-CM elliptic curves defined over $\mathbb{Q}$.

Uniformity Conjecture (V2). There is some prime $p_{\mathbb{Q}}$ such that, for any non-CM elliptic curve $E/\mathbb{Q}$, the representation

$$\overline{\rho}_{E,P} : G_{\mathbb{Q}} \to GL_2(\mathbb{F}_p)$$

is surjective for all primes $p > p_{\mathbb{Q}}$.

What has been done toward the Uniformity Conjecture? Due to results like the following, it is strongly believed that $p_{\mathbb{Q}} = 37$,

Bilu, Mazur, Parent, Rebolledo, Serre (1972-2013). Let $E/\mathbb{Q}$ be a non-CM elliptic curve. If $p > 37$ is a prime, then $\overline{\rho}_{E,P}$ is either surjective, or its image is contained in the normalizer of a non-split Cartan subgroup.

Lemos (2017). Let $E/\mathbb{Q}$ be a non-CM elliptic curve. Suppose that E admits a non-cyclic $\mathbb{Q}$-isogeny. Then for $p > 37$ prime, $\overline{\rho}_{E,P}$ is surjective.

4 Elliptic curves over $\mathbb{C}$

We have viewed elliptic curves from an algebraist perspective **(which is method I prefer and do!)**. Now let's look at the function, the derives an elliptic curves from an analyst perspective using techniques from complex analysis.

Evaluation of the integral giving are length on a circle, namely,

$$\int \frac{1}{\sqrt{1-x^2}}\, dx$$

leads to an inverse trigonometric function. The analogous problem for the arc length of an ellipse yields an integral that is not computable in terms of so-called elementary functions. The indeterminacy of the sign of the square root means that such integrals are not well-defined on $\mathbb{C}$; instead, they are more naturally studied on an associated Riemann surface.

For the arc length integral of an ellipse, this Riemann surface turns out to be the set of complex points on an elliptic curve E. We thus begin our study of elliptic curves over $\mathbb{C}$ by studying certain elliptic integrals, which are line integrals on $E(\mathbb{C})$. Indeed, the reason that elliptic curves are so named is because they are the Riemann surfaces associated to are length integrals of ellipses.

a. *Elliptic integrals*

Let E be an elliptic curve defined over $\mathbb{C}$. Since $\mathrm{char}(\mathbb{C}) = 0$ and $\mathbb{C}$ is algebraically closed, there is a Weierstrass equation for E in Legendre form (III.1.7),

$$E : y^2 = x(x-1)(x-\lambda)$$

The natural map,

$$\begin{aligned} E(\mathbb{C}) &\to \mathbb{P}^1(\mathbb{C}) \\ (x,y) &\longmapsto x \end{aligned}$$

is a double cover ramified over precisely the four points $0, 1, \lambda, \infty \in \mathbb{P}^1(\mathbb{C})$. We know from (III.1.5) that $\omega = dx/y$ is a holomorphic differential form on E. Suppose that we try to define a map by the rule,

$$\begin{aligned} E(\mathbb{C})^* &\stackrel{?}{\to} \mathbb{C} \\ P &\longmapsto \int_O^P \omega \end{aligned}$$

where the integral is along some path connecting O to P. Unfortunately, this map is not well-defined, since it depends on the choice of path. We let $P = (x,y) \in E(\mathbb{C})$ and look more closely at what is happening in $\mathbb{P}^1(\mathbb{C})$. We are attempting to compute the complex line integral,

$$\int_\infty^x \frac{1}{\sqrt{t(t-1)(t-\lambda)}}\,dx$$

This line integral is not path-independent, because the square root is not singlevalued. Thus in the below figure, the three integral,

$$\int_\alpha \omega, \quad \int_\beta \omega, \quad \int_\gamma \omega$$

need not be equal. In order to make the integral well-defined, it is necessary to make branch cuts. For example, the integral will be path-independent on the complement of the branch cuts illustrated in the figure, because in this region it is possible to define a single-valued branch of $\sqrt{t(t-1)(t-\lambda)}$. More generally, since the square root is double-valued, we should take two copies of $\mathbb{P}^1(\mathbb{C})$, make branch cuts as indicated in the figure, and glue them together along the branch cuts to form the Riemann surface illustrated in the figure.

(Note that $\mathbb{P}^1(\mathbb{C}) = \mathbb{C} \cup \infty$ is topologically a 2-sphere.) It is readily seen that the resulting Riemann surface is a torus, and it is on this surface that we should study the integral,

$$\int \frac{1}{\sqrt{t(t-1)(t-\lambda)}}\, dt$$

Returning now to our hypothetical map,

$$\begin{aligned} E(\mathbb{C}) &\to \mathbb{C} \\ P &\longmapsto \int_O^P \omega \end{aligned}$$

we see that the indeterminacy comes from integrating across branch cuts in $\mathbb{P}^1(\mathbb{C})$, or equivalently around non-contractible loops on the torus. The figure illustrates two closed paths α and β for which the integrals $\int_\alpha \omega$ and $\int_\beta \omega$ may be nonzero. We thus obtain two complex numbers, which are called periods of E, $\omega_1 = \int_\alpha \omega$ and $\omega_2 = \int_\beta \omega$. Notice that the paths α and β generate the first homology group of the torus. Thus any two paths from O to P differ by a path that is homologous to $n_1\alpha + n_2\beta$ for some $n_1, n_2 \in \mathbb{Z}$. Thus the integral $\int_O^P \omega$ is well-defined up to addition of a number of the form $n_1\omega_1 + n_2\omega_2$, which suggests that we should look at the set $\Lambda = \{n_1\omega_1 + n_2\omega_2 \,:\, n_1, n_2 \in \mathbb{Z}\}$. The preceding discussion shows that there is a well-defined map,

$$\begin{aligned} F \,:\, E(\mathbb{C}) &\to \mathbb{C}/\Lambda \\ P &\longmapsto \int_O^P \omega \pmod{\Lambda} \end{aligned}$$

The set Λ is clearly a subgroup of $\mathbb{C}$, so the quotient $\mathbb{C}/\Lambda$ is a group. Using the translation invariance of ω that we proved in (III.5.1), we easily verify that F is a homomorphism:

$$\int_O^{P+Q} \omega \equiv \int_O^P \omega + \int_P^{P+Q} \omega \equiv \int_O^P \omega + \int_O^Q \tau_P^*\omega \equiv \int_O^P \omega + \int_O^Q \omega \pmod{\Lambda}$$

The quotient space $\mathbb{C}/\Lambda$ will be a compact Riemann surface, i.e., a compact one-dimensional complex manifold, if and only if Λ is a lattice, or equivalently, if and only if the periods ω_1 and ω_2 that generate Λ are linearly independent over $\mathbb{R}$. This turns out to be the case, and further, the map F is a complex analytic isomorphism from $E(\mathbb{C})$ to $\mathbb{C}/\Lambda$. However, rather than proving these statements here, we instead turn to the study of the space $\mathbb{C}/\Lambda$ for a given lattice Λ. we construct the inverse to the map F and prove that $\mathbb{C}/\Lambda$ is analytically isomorphic to $E_\Lambda(\mathbb{C})$ for a certain elliptic curve $E_\Lambda/\mathbb{C}$. We then apply the uniformization theorem (VI.5.1), which says that every elliptic curve $E/\mathbb{C}$ is isomorphic to some E_Λ, to deduce (VI.5.2) that the periods of $E/\mathbb{C}$ are $\mathbb{R}$-linearly independent and that F is a complex analytic isomorphism. (For a direct proof of the $\mathbb{R}$-linear independence of ω_1 and ω_2 using only Stokes's theorem in $\mathbb{R}^2$).

Let $\Lambda \subset \mathbb{C}$ be a lattice, ie., Λ is a discrete subgroup of $\mathbb{C}$ that contains an $\mathbb{R}$-basis for $\mathbb{C}$. In this section we study meromorphic functions on the quotient space $\mathbb{C}/\Lambda$, or equivalently, meromorphic functions on $\mathbb{C}$ that are periodic with respect to the lattice Λ.

Elliptic Function. An elliptic function (relative to the lattice Λ) is a meromorphic function $f(z)$ on $\mathbb{C}$ that satisfies, $f(z+\omega) = f(z)$, for all $z \in \mathbb{C}$ and all $\omega \in \Lambda$.

The set of all such functions is denoted by $\mathbb{C}(\Lambda)$. It is clear that $\mathbb{C}(\Lambda)$ is a field.

Fundamental Parallelogram. A fundamental parallelogram for Λ is a set of the form $D = \{a + t_1\omega_1 + t_2\omega_2 \,:\, 0 \le t_1, t_2 < 1\}$, where $a \in \mathbb{C}$ and $\{\omega_1, \omega_2\}$ is a basis for Λ.

b. *Elliptic Functions*

Proposition. A holomorphic elliptic function, i.e., an elliptic function with no poles, is constant. Similarly, an elliptic function with no zeros is constant.

PROOF. Suppose that $f(z) \in \mathbb{C}(\Lambda)$ is holomorphic. Let D be a fundamental parallelogram for Λ. The periodicity of f implies that,

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

The function f is continuous and the set $\overline{D}$ is compact, so $|f(z)|$ is bounded on $\overline{D}$. Hence f is bounded on all of $\mathbb{C}$, so Liouville's theorem tells us that f is constant. This proves the first statement. Finally, if f has no zeros, then $1/f$ is holomorphic, hence constant. □

Let f be an elliptic function and let $w \in \mathbb{C}$. Then, just as for any meromorphic function, we can look at its order of vanishing and its residue, which we denote by

$$\begin{aligned} \operatorname{ord}_w(f) &= \text{ order of vanishing of } f \text{ at } w \\ \operatorname{res}_w(f) &= \text{ residue of } f \text{ at } w \end{aligned}$$

The fact that f is elliptic implies that the order and the residue of f do not change if we replace w by $w+\omega$ for any $\omega \in \Lambda$. This prompts the following convention,

$$\sum_{w\in\mathbb{C}/\Lambda}$$

denotes a sum over $w \in D$, where D is a fundamental parallelogram for Λ. By implication, the value of the sum is independent of the choice of D and only finitely many terms of the sum are nonzero. Notice that (VI.2.1) is the complex analogue of (II.1.2), which says that an algebraic function that has no poles is constant. The next theorem and corollary continue this theme by proving for $\mathbb{C}/\Lambda$ results that are analogous to (II.3.1) and (III.3.5).

Theorem. Let $f \in \mathbb{C}(\Lambda)$ be an elliptic function relative to Λ.

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

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

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

PROOF. Let D be a fundamental parallelogram for Λ such that $f(z)$ has no zeros or poles on the boundary ∂D of D.

(a) The residue theorem tells us that,

$$\sum_{w\in\mathbb{C}/\Lambda} \operatorname{res}_w(f) = \frac{1}{2\pi i}\int_{\partial D} f(z)\,dz$$

The periodicity of f implies that the integrals along the opposite sides of the parallelogram cancel, so the total integral around the boundary of D is zero.

(b) The periodicity of $f(z)$ implies that $f'(z)$ is also periodic, so applying (1) to the elliptic function $f'(z)/f(z)$ gives,

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

since $\operatorname{res}_w(f'/f) = \operatorname{ord}_w(f)$, this is the desired result.

(c) We apply the residue theorem to the function, $zf'(z)/f(z)$ to obtain,

$$\begin{aligned}\sum_{w\in\mathbb{C}/\Lambda} \operatorname{ord}_w(f)w &= \frac{1}{2\pi i}\int_{\partial D}\frac{zf'(z)}{f(z)}\,dz \\ &= \frac{1}{2\pi i}\left(\int_a^{a+\omega_1} + \int_{a+\omega_1}^{a+\omega_1+\omega_2} + \int_{a+\omega_1+\omega_2}^{a+\omega_2} + \int_{a+\omega_2}^{a}\right)\frac{zf'(z)}{f(z)}\,dz\end{aligned}$$

In the second (respectively third) integral we make the change of variable $z \longmapsto z+\omega_1$ (respectively $z \longmapsto z+\omega_2$). Then the periodicity of $f'(z)/f(z)$ yields,

$$\sum_{w\in\mathbb{C}/\Lambda} \operatorname{ord}_w(f)w = -\frac{\omega_2}{2\pi i}\int_a^{a+\omega_1}\frac{f'(z)}{f(z)}\,dz + \frac{\omega_1}{2\pi i}\int_a^{a+\omega_2}\frac{f'(z)}{f(z)}\,dz$$

If $g(z)$ is any meromorphic function, then the integral,

$$\frac{1}{2\pi i}\int_a^b \frac{g'(z)}{g(z)}\,dz$$

is the winding number around 0 of the path.

$$\begin{aligned}[0,1] &\to \mathbb{C} \\ t &\longmapsto g((1-t)a+tb)\end{aligned}$$

In particular, if $g(a) = g(b)$, then the integral is an integer. Thus the periodicity of $f'(z)/f(z)$ implies that $\sum \operatorname{ord}_w(f)w$ has the form, $-\omega_2 n_2 + \omega_1 n_1$ for $n_1, n_2 \in \mathbb{Z}$, so it is in Λ.

Hence, we have proved the theorem. □

Order. The order of an elliptic function is its number of poles (counted with multiplicity) in a fundamental parallelogram. Equivalently, (VI.2.2b) says that the order is the number of zeros.

Corollary. A non-constant elliptic function has order at least 2.

If $f(z)$ has a single simple pole, then (VI.2.2a) tells us that the residue at that pole is 0, so $f(z)$ is actually holomorphic. We now define the divisor group of $\mathbb{C}/\Lambda$, denoted by $\mathrm{Div}(\mathbb{C}/\Lambda)$, to be the group of formal linear combinations,

$$\sum_{w\in\mathbb{C}/\Lambda} n_w(w)$$

with $n_w \in \mathbb{Z}$ and $n_w = 0$ for all but finitely many w. Then for $D = \sum n_w(w) \in \mathrm{Div}(\mathbb{C}/\Lambda)$, we define and $\deg D = \sum n_w$, $\mathrm{Div}^0(\mathbb{C}/\Lambda) = \{D \in \mathrm{Div}(\mathbb{C}/\Lambda) : \deg D = 0\}$. Further, for any $f \in \mathbb{C}(\Lambda)^*$ we define the divisor of f to be,

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

We see from (VI.2.2b) that $\mathrm{div}(f) \in \mathrm{Div}^0(\mathbb{C}/\Lambda)$. The map, $\mathrm{div} : \mathbb{C}(\Lambda)^* \to \mathrm{Div}^0(\mathbb{C}/\Lambda)$ is clearly a homomorphism, since each ord_w is a valuation. Finally, we define a summation map, $\mathrm{sum} : \mathrm{Div}^0(\mathbb{C}/\Lambda) \to \mathbb{C}/\Lambda$, $\mathrm{sum}(\sum n_w(w)) = \sum n_w w \pmod{\Lambda}$. The next result gives an exact sequence that encompasses our main results so far for $\mathbb{C}/\Lambda$, plus one fact (VI.3.4) that will be proven in the next section.

Theorem. The following is an exact sequence:

$$1 \to \mathbb{C}^* \to \mathbb{C}(\Lambda)^* \xrightarrow{\mathrm{div}} \mathrm{Div}^0(\mathbb{C}/\Lambda) \xrightarrow{\mathrm{sum}} \mathbb{C}/\Lambda \to 0$$

c. *Construction of Elliptic Functions*

We saw the theory behind elliptic functions, but how do we construct there special complex functions? In order to show that the results, we saw are not vacuous, we must construct some non-constant elliptic functions. We know from (VI.2.3) that any such function has order at least 2. Following Weierstrass, we look for a function with a pole of order 2 at $z = 0$.

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

$$\wp(z,\Lambda) = \frac{1}{z^2} + \sum_{\omega\in\Lambda,\ \omega\neq 0} \left(\frac{1}{(z-\omega)^2} - \frac{1}{\omega^2}\right)$$

The Eisenstein series of weight $2k$ (for Λ) is the series,

$$G_{2k}(\Lambda) = \sum_{\omega\in\Lambda,\ \omega\neq 0} \omega^{-2k}$$

For notational convenience, we write $\wp(z)$ and G_{2k} if the lattice Λ has been fixed.

Theorem. Let $\Lambda \subset \mathbb{C}$ be a lattice.

(a) The Eisenstein series $G_{2k}(\Lambda)$ is absolutely convergent for all $k > 1$.

(b) The series defining the Weierstrass $\wp$-function converges absolutely and uniformly on every compact subset of $\mathbb{C}/\Lambda$. The series defines a meromorphic function on $\mathbb{C}$ having a double pole with residue 0 at each lattice point and no other poles.

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

PROOF. (a) Since Λ is discrete in $\mathbb{C}$, it is not hard to see that there is a constant $c = c(\Lambda)$ such that for all $N \geq 1$, the number of points in an annulus satisfies,

$$\#\{\omega \in \Lambda : N \leq |\omega| < N+1\} < cN$$

This allows us to estimate,

$$\sum_{\omega\in\Lambda,\ |\omega|\geq 1} \frac{1}{|\omega|^{2k}} \leq \sum_{N=1}^{\infty} \frac{\#\{\omega \in \Lambda : N \leq |\omega| < N+1\}}{N^{2k}} < \sum_{N=1}^{\infty} \frac{c}{N^{2k-1}} < \infty$$

(b) If $|\omega| > 2|z|$, then

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

It follows from (1) that the series for $\wp(z)$ is absolutely convergent for all $z \in \mathbb{C}/\Lambda$, and that it is uniformly convergent on every compact subset of $\mathbb{C}/\Lambda$. Therefore the series defines a holomorphic function on $\mathbb{C}/\Lambda$, and it is clear from the series expansion that $\wp(z)$ has a double pole with residue 0 at each point in Λ.

(c) Replacing ω by $-\omega$ in the series for $\wp$ it is clear that $\wp(z) = \wp(-z)$, so $\wp$ is an even function. We know from (2) that the series for $\wp$ is uniformly convergent, so we can compute its derivative by differentiating term by term,

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

It is clear from this expression that $\wp'$ is an elliptic function, so $\wp'(z+\omega) = \wp'(z)$ for all $\omega \in \Lambda$. Integrating this equality with respect to z, yields $\wp(z+\omega) = \wp(z) + c(\omega)$ for all $z \in \mathbb{C}$ and $c(\omega) \in \mathbb{C}$ is independent of z. Setting, $z = -\frac{1}{2}\omega$ and using the evenness of $\wp(z)$ proves that $c(\omega) = 0$, so $\wp$ is an elliptic function.

Hence proved. □

Next we show that every elliptic function is a rational function of the Weierstrsss $\wp$-function and its derivative. This result is the analytic analogue of (III.3.1.1).

Theorem. Let $\Lambda \subset \mathbb{C}$ be a lattice. Then

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

ie., every elliptic function is a rational combination of $\wp$ and $\wp'$.

PROOF. Let $f(z) = \mathbb{C}(\Lambda)$. Writing,

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

we see that it suffices to prove the theorem for functions that are either odd or even. Further, if $f(z)$ is odd, then $f(z)\wp'(z)$ is even, so we are reduced to the case that f is an even elliptic function. The assumption that f is even implies that,

$$\operatorname{ord}_w f = \operatorname{ord}_{-w} f$$

for every $w \in \mathbb{C}$. Further, we claim that if $2w \in \Lambda$, then $\operatorname{ord}_w f$ is even. To see this, we differentiate $f(z) = f(-z)$ epeatedly to obtain,

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

If $2w \in \Lambda$, then $f^{(i)}(z)$ has the same value at w and $-w$, so

$$f^{(i)}(w) = f^{(i)}(-w) = (-1)^i f^{(i)}(w)$$

Thus, $f^{(i)}(w) = 0$ for odd values of i, so $\operatorname{ord}_w f$ is even. □

Let D be a fundamental parallelogram for Λ, and let H be $\frac{1}{2}D$. In other words, H is a fundamental domain for $(\mathbb{C}/\Lambda) \setminus \{\pm 1\}$, or equivalently, $\mathbb{C}$ is a disjoint union,

$$\mathbb{C} = (H + \Lambda) \cup (-H + \Lambda)$$

as illustrated in the figure. The above discussion implies that the divisor of f has the form,

$$\sum_{w \in H} n_w((w) + (-w))$$

for certain $n_w \in \mathbb{Z}$. Note that for $2w \in \Lambda$, we are using the fact that $\operatorname{ord}_w f$ is even. Consider the function,

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

The divisor of $\wp(z) - \wp(w)$ is $(w) + (-w) - 2(0)$, so we see that f and g have exactly the same zeros and poles except possibly at $w = 0$. But then (VI.2.2b) implies that they have the same order at 0, too. Thus, $f(z)/g(z)$ is a holomorphic elliptic function, hence it is constant from (VI.2.1).

The Weierstrass σ-function. The Weierstrass σ-function relative to Λ is the function defined by the product,

$$\sigma(z) = \sigma(z, \Lambda) = \prod_{\omega \in \Lambda,\ \omega \neq 0} \left(1 + \frac{z}{\omega}\right) e^{(z/\omega) + \frac{1}{2}(z/\omega)^2}$$

The next lemma describes the basic facts about $\sigma(z)$ that are needed for our applications.

Lemma. $\sigma(z)$ follows these basic facts:

(a) 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 no other zeros.

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

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

(c) For every $\omega \in \Lambda$, there exists $a, b \in \mathbb{C}$, depending on ω, such that

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

for all $z \in \mathbb{C}$.

PROOF. (a) The absolute and uniform convergence of the infinite product on $\mathbb{C}$ follows from (VI.3.1a) and standard facts about convergence of infinite products. The location and order of the zeros is clear by inspection.

(b) The logarithm of $\sigma(z)$ is,

$$\log \sigma(z) = \log z + \sum_{\omega \in \Lambda,\ \omega \neq 0} \left\{ \log\left(1 + \frac{z}{\omega}\right) + \frac{z}{\omega} + \frac{1}{2}\left(\frac{z}{\omega}\right)^2 \right\}$$

and (1) tells us that we may differentiate term by term. The second derivative, up to sign, is exactly the series defining $\wp(z)$.

(c) The Weierstrass $\wp$-function is elliptic (VI.3.1c), so $\wp(z + \omega) = \wp(z)$. Integrating twice with respect to z and using (2) yields,

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

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

Proposition. Let $n_1, \ldots, n_r \in \mathbb{Z}$ and $z_1, \ldots, z_r \in \mathbb{C}$ satsify,

$$\sum n_i = 0, \qquad \sum n_i z_i \in \Lambda$$

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

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

More precisely, if we choose the n_i and z_i to satisfy $\sum n_i z_i = 0$, then we may take

$$f(z) = \prod \sigma(z - z_i)^{n_i}$$

PROOF. Let $\lambda = \sum n_i z_i \in \Lambda$. Replacing,

$$n_1(z_1) + \cdots + n_r(z_r) \to n_1(z_1) + \cdots + n_r(z_r) + (0) - (\lambda)$$

we may assume that $\sum n_i z_i = 0$. Then (VI.3.3a) implies that,

$$f(z) = \prod \sigma(z - z_i)^{n_i}$$

□

We next derive the Laurent series expansions for $\wp(z)$ around $z = 0$, from which we will deduce the fundamental algebraic relation satisfied by $\wp(z)$ and $\wp'(z)$.

Theorem.

(a) The Laurent series for $\wp(z)$ around $z = 0$ is given by,

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

(b) For all $z \in \mathbb{C} \setminus \Lambda$, the Weierstrass $\wp$-function and its derivative satisfy the relation,

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

PROOF. (a) For all z with $|z| < |\omega|$ we have,

$$\frac{1}{(z-\omega)^2} - \frac{1}{\omega^2} = \frac{1}{\omega^2}\left(\frac{1}{(1-z/\omega)^2} - 1\right) = \sum_{n=1}^{\infty} (n+1)\frac{z^n}{\omega^{n+2}}$$

(b) We write out the first few terms of various Laurent expansions:

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

Comparing these expansions, we see that the function,

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

is holomorphic at $z = 0$ and satisfies $f(0) = 0$. But $f(z)$ is an elliptic function relative to Λ, and from (VI.3.1b) it is holomorphic away from Λ, so $f(z)$ is a holomorphic elliptic function. Then (VI.2.1) says that $f(z)$ is constant, and the fact that $f(0) = 0$ implies that f is identically zero. □

Remark 3.5.1. It is standard notation to set,

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

Then the algebraic relation satisfied by $\wp(z)$ and $\wp'(z)$ reads,

$$\wp'(z)^2 = 4\wp(z)^3 - g_{2\wp}\wp(z) - g_3$$

Let $E/\mathbb{C}$ be an elliptic curve. The group law $E \times E \to E$ is given by everywhere locally defined rational functions (III.3.6), so we see in particular that $E = E(\mathbb{C})$ is a complex Lie group, i.e., it is a complex manifold with a group law given locally by complex analytic functions. Similarly, if $\Lambda \subset \mathbb{C}$ is a lattice, then $\mathbb{C}/\Lambda$ with its natural addition is a complex Lie group. The next result says that $\mathbb{C}/\Lambda$ is always complex analytically isomorphic to an elliptic curve.

Proposition. Let $g_2 = g_2(\Lambda)$ and $g_3 = g_3(\Lambda)$ be the quantities associated to a lattice $\Lambda \subset \mathbb{C}$.

(a) The polynomial $f(x) = 4x^3 - g_2x - g_3$ has distinct roots, so its discriminant $\Delta(\Lambda) = g_2^3 - 27g_3^2$ is nonzero.

(b) Let $E/\mathbb{C}$ be the curve, where $E : y^2 = 4x^3 - g_2x - g_3$, which from (1) is an elliptic curve. Then the map, $\phi : \mathbb{C}/\Lambda \to E(\mathbb{C}) \subset \mathbb{P}^2(\mathbb{C})$, $z \longmapsto [\wp(z), \wp'(z), 1]$, is a complex analytic isomorphism of complex Lie groups, i.e., it is an isomorphism of Riemann surfaces that is also a group homomorphism.

PROOF. (a) Let ω_1, ω_2 be a basis for Λ and $\omega_3 = \omega_1 + \omega_2$. Then, since $\wp'(z)$ is an odd elliptic function, we see that

$$\wp'(z)\left(\frac{\omega_i}{2}\right) = -\wp'(z)\left(\frac{-\omega_i}{2}\right) = -\wp'(z)\left(\frac{\omega_i}{2}\right)$$

so $\wp'(z)(\omega_i/2) = 0$. It follows from (VI.3.5b) that $f(x)$ vanishes at each of the values $x = \wp(\omega_i/2)$, so it suffices to show that these three values are distinct. The function $\wp(z) - \wp(\omega_i/2)$ is even, so it has at least a double zero at $z = \omega_i/2$. However, it is an elliptic function of order 2 , so it has only these zeros in an appropriate fundamental parallelogram. Hence $\wp(\omega_j/2) \neq \wp(\omega_i/2)$ for $j \neq i$.

(b) The image of ϕ is contained in $E(\mathbb{C})$ from (VI.3.5b). To see that ϕ is surjective, let $(x, y) \in E(\mathbb{C})$. Then $\wp(z) - x$ is a nonconstant elliptic function, so from(VI.2.1) it has a zero, say $z = a$. It follows that $\wp'(a)^2 = y^2$, so replacing a by $-a$ if necessary, we obtain $\wp'(a) = y$. Then $\phi(a) = (x, y)$. Next suppose that $\phi(z_1) = \phi(z_2)$. Assume first that $2z_1 \in\notin \Lambda$. Then the function, $\wp(z) - \wp(z_1)$ is an elliptic function of order 2 that vanishes at z_1, $-z_1$ and z_2. It follows that two of these values are congruent modulo Λ, so the assumption that $2z_1 \notin \Lambda$ tells us that, $z_2 \equiv \pm z_1 \pmod{\Lambda}$ for some choice of sign. Then, $\wp'(z_1) = \wp'(z_2) = \wp'(\pm z_1) = \pm\wp'(z)$ implies that $z_2 \equiv z_1 \pmod{\Lambda}$ (Note that $\wp'(z_2) \neq 0$ from the proof of (1)). Similarly if $2z_1 \in \Lambda$, then $\wp(z) - \wp(z_1)$ has a double zero at z_1 and vanishes at z_2, so we again conclude that $z_2 \equiv z_1 \pmod{\Lambda}$. This proves that ϕ is injective. Next we show that ϕ is an analytic isomorphism by computing its effect on the cotangent spaces of $\mathbb{C}/\Lambda$ and $E(\mathbb{C})$. At every point of $E(\mathbb{C})$, the differential form dx/y is holomorphic and nonvanishing. Finally, we must check that ϕ is a homomorphism. Let $z_1, z_2 \in \mathbb{C}$. Using (VI.3.4), we can find a function $f(z) \in \mathbb{C}(\Lambda)$ with divisor, $\operatorname{div}(f) = (z_1 + z_2) - (z_1) - (z_2) + (0)$. Then (VI.3.2) allows us to write $f(z) = F(\wp(z), \wp'(z))$ for a rational function $F(X, Y) \in \mathbb{C}(X, Y)$. Treating, $F(x, y)$ as an element of $\mathbb{C}(x, y) = \mathbb{C}(E)$, we have $\operatorname{div}(F) = (\phi(z_1 + z_2)) - (\phi(z_1)) - (\phi(z_2)) + (\phi(0))$. It follows from (III.3.5) that, $\phi(z_1 + z_2) = \phi(z_1) + \phi(z_2)$. Hence a homorphism.

Hence completing the proof of the proposition. □

5 References

[1] Christina Birkenhake and Herbert Lange. Complex tori, volume 177. Springer Science and Business Media, 1999.

[2] Craig Costello, Patrick Longa, and Michael Naehrig. Efficient algorithms for supersingular isogeny diffie-hellman. In Advances in Cryptology-CRYPTO 2016: 36th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 14-18, 2016, Proceedings, Part I 36, pages 572-601. Springer, 2016.

[3] Gerd Faltings. Finiteness theorems for abelian varieties over number fields. Arithmetic geometry, pages 9-26, 1986.

[4] Robin Hartshorne. Algebraic geometry, volume 52. Springer Science and Business Media, 2013.

[5] Joseph H Silverman. Advanced topics in the arithmetic of elliptic curves, volume 151. Springer Science and Business Media, 1994.

[6] Deuring, M. (1941). Die Typen der Multiplikatorenringe elliptischer Funktionenkorper. Abh. Math. Sem. Hansischen, 14:197-272.

[7] Silverman, J. H. (1986). The Arithmetic of Elliptic Curves. Springer, New York, NY.

[8] Bull, A. J. (2018). Galois representations and elliptic curves. Personal collection of Gilbert Moss, University of Utah, Salt Lake City, UT.

[9] Fourn, S. and Lemos, P. (2021). Residual Galois representations of elliptic curves with image contained in the normaliser of a non-split Cartan. Algebra Number Theory, 15(3):747-771. DOI: 10.2140/ant.2021.15.747

[10] Jones, N. (2010). Almost all elliptic curves are Serre curves. Trans. Amer. Math. Soc., 362(3):1547-1570. DOI: 10.1090/s0002-9947-09-04804-1

[11] Lemos, P. (2017). Serre's Uniformity Conjecture for Elliptic Curves with Rational Cyclic Isogenies [preprint]. Retrieved March 26, 2023 from arXiv:1702.01985v2 [math.NT]

[12] Lombardo, D. (2014). Bounds for Serre's open image theorem for elliptic curves over number fields. Algebra Number Theory, 9(10):2347-2395. DOI: 10.2140/ant.2015.9.2347

[13] Ranjbar, F. and Ranjbar, S. (2015). Inverse Galois problem and significant methods [preprint]. Retrieved July 18, 2022 from arXiv:1512.08708v1 [math.HO]

[14] Serre, J.-P. (1972). Propriétés galoisiennes des points d'ordre fini des courbes elliptiques. Inventiones Mathematicae, 15:259-331.