Elliptic Curves and Elliptic Functions

ARASH ISLAMI
Professor: Dr. Chung Pang Mok
McMaster University - Math 790
June 27, 2012

Abstract
Elliptic curves are algebraic curves of genus 1 which can be embedded into projective plane \( \mathbb{P}^2 \) as a cubic with a point identified on the line at infinity. This is achieved by using explicit polynomial equations namely, Weierstrass equations. The set of points of an elliptic curve form an abelian group. The study of arithmetic properties of elliptic curves with their points defined over algebraically closed field of complex numbers is of our interest in this paper. Historically, computing the integral of an arc-length of an ellipse lead to the idea of elliptic curves and their Riemann surface. This Riemann surface for an ellipse turns out to be the set of complex points on an elliptic curve. The theory of Elliptic Functions and Weierstrass \( \wp \) - function and the connection to the original study of elliptic integrals with various results about elliptic curves over \( \mathbb{C} \) will be presented.

1 Elliptic Curves

We begin our study of elliptic curves by introducing the basic objects and definitions which will be used in the following sections of this paper. To start, we will set the following notations:

- \( K \): a perfect field ( i.e. every algebraic extension of \( K \) is separable )
- \( \bar{K} \): a fixed algebraic closure of \( K \)
- \( C/K : C \) is defined over \( K \)
- \( K(C) \): function field of \( C \)

The material in this paper is mainly based on “The Arithmetic of Elliptic Curves” by: Joseph H. Silverman and other references written in the bibliography. After briefly going over the basic concepts, the algebraic view and the idea of Riemann surfaces we continue on to discuss the elliptic curves over \( \mathbb{C} \) which contains elliptic integrals, functions and their construction. In the end, the Abel-Jacobi theorem will be presented.

Affine Spaces
The Cartesian (or Affine) n-space is defined as the following:

**Definition.** Affine \( n \)-space over \( K \) is the set of \( n \)-tuples:

\[ A^n = A^n(K) = \{ P = (x_1, ..., x_n) : x_i \in \bar{K} \} \]

Similarly the set of \( K \)-rational points in \( A^n \) is the set:

\[ A^n = A^n(K) = \{ P = (x_1, ..., x_n) : x_i \in K \} \]
Projective Varieties

The idea of projective space came through the process of adding points at infinity to affine space. We define projective space as the collection of lines through the origin in affine space of one dimension higher.

Definition. Projective $n$-space over $K$ denoted by $\mathbb{P}^n$ or $\mathbb{P}^n(K)$ is the set of all $(n + 1)$-tuples:

$$ (x_0, ..., x_n) \in \mathbb{A}^{n+1} $$

Such that at least one $x_i$ is nonzero, modulo the equivalence relation

$$ (x_0, ..., x_n) \sim (y_0, ..., y_n) $$

if there exists a $\lambda \in \tilde{K}^*$ with $x_i = \lambda y_i$ for all $i$.

Homogeneous Coordinates

An equivalence class $\{\lambda x_0, ..., \lambda x_n : \lambda \in \tilde{K}^*\}$ is denoted by $[x_0, ..., x_n]$ and the individual $x_0, ..., x_n$ are called homogeneous coordinates for the corresponding point in $\mathbb{P}^n$.

K-rational points

The set of $K$- rational points in $\mathbb{P}^n$ is the set

$$ \mathbb{P}^n(K) = \{[x_0, ..., x_n] \in \mathbb{P}^n : \text{all } x_i \in K\} $$

Note: If $\mathbb{P} = [x_0, ..., x_n] \in \mathbb{P}^n(K)$ it does not follow that each $x_i \in K$. However, choosing some $i$ with $x_i \neq 0$, it does follow that $x_i/x_j \in K$ for every $j$.

Elliptic Curves

An Elliptic Curves over field $K$ is a non-singular projective algebraic curve $E$ of genus one with a specified chosen base-point. Here is a definition:

Definition. An elliptic curve is a pair $(E, \mathcal{O})$, where $E$ is a curve of genus 1 and $\mathcal{O} \in E$.

The elliptic curve $E$ is defined over the field $K$, written $E/K$, if $E$ is defined over $K$ as a curve and $\mathcal{O} \in E(K)$. This base point is a distinguished identity element in order to make the set $E$ into a group.

The main focus in this paper is the study of elliptic curves over the algebraically closed field of complex numbers, $\mathbb{C}$. To show that every elliptic curve can be written as a plane cubic we present the following:

Weierstrass Equation

Every curve of genus 1 can be written as a locus in $\mathbb{P}^2$ of cubic equation with only one point on the line at $\infty$. We will express elliptic curves by explicit polynomial equation called Weierstrass equations. Note that, using this explicit equations, it is shown that the set of points of an elliptic curve forms an abelian group and the group law is given by rational functions.

Definition. A generalized Weierstrass Equation over $K$ is an equation of the form:

$$ E : Y^2Z + a_1XYZ + a_3YZ^2 = X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3 $$

where the coefficients $a_i \in \tilde{K}$ and $\mathcal{O} = [0, 1, 0]$ is the base point.
Important notes:

- This equation defines a curve with a single point at infinity: $O = [0, 1, 0]$ as the base point.
- The curve $E$ is non-singular at $O$; but it may be singular elsewhere.
- Conversely, any cubic satisfying these conditions must be in Weierstrass form.

To express with non-homogeneous coordinates: $x = X/Z$, $y = Y/Z$, the Weierstrass equation for our elliptic curves is written as:

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

If $\text{Char}(K) \neq 2$, changing variable: $y \rightarrow \frac{1}{2}(y - a_1x - a_3)$ gives an equation of the form:

$$E : y^2 = 4x^3 + b_2x^2 + 2b_4x + b_6$$

Where

$$b_2 = a_1^2 + 4a_2, \quad b_4 = 2a_4 + a_1a_3, \quad b_6 = a_3^2 + 4a_6$$

And define the following:

$$b_8 = a_1^2a_6 + 4a_2a_6 - a_1a_3a_4 + a_2a_3^2 - a_1^2$$

$$\triangle = -b_2^2b_8 - 8b_4^3 - 27b_6^2 + 9b_2b_4b_6$$

**Definition.** For a generalized Weierstrass equation over $K$, with quantities of $b_2, b_4, b_6, b_8$ and $\triangle$ as above, then $\triangle$ is the discriminant of the generalized Weierstrass equation.

**Proposition 1.1:** The Weierstrass equation defines a non-singular curve if and only if $\triangle \neq 0$.

The following proposition connects the material we have presented so far. It is the idea that every elliptic curve can be written as a plane cubic, and conversely, every smooth Weierstrass plane cubic curve is an elliptic curve.

**Proposition 1.2:** Let $E$ be an elliptic curve defined over $K$.

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

$$\phi : E \rightarrow \mathbb{P}^2$$

$$\phi = [x, y, 1]$$

gives an isomorphism of $E/K$ onto a curve given by a Weierstrass equation

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

with coefficients in $K$ and such that $\phi(O) = [0, 1, 0]$.

**Note:** The functions $x$ and $y$ are called Weierstrass coordinates for the elliptic curve $E$.

(b) Conversely, every smooth cubic curve $E$ given by a Weierstrass equation as in (a) is an elliptic curve defined over $K$ with origin $\phi(O) = [0, 1, 0]$. 

3
Legendre form

A Legendre form is another form of Weierstrass equation that is sometimes convenient to use:

**Definition.** A Weierstrass equation is in Legendre form if it can be written as:

\[ y^2 = x(x - 1)(x - \lambda) \]

**Proposition 1.3** Assume that \( \text{Char}(K) \neq 2 \). Every elliptic curve is isomorphic (over \( \bar{K} \)) to an elliptic curve in Legendre form

\[ E_\lambda : y^2 = x(x - 1)(x - \lambda) \]

for some \( \lambda \notin \bar{K} \) with \( \lambda \neq 0, 1 \).

2 Riemann Surfaces

Before we proceed to the next topics, it is necessary to briefly define the idea of Riemann surfaces:

**Definition.** A Riemann surface is a paracompact Hausdorff topological space \( C \) with an open covering \( C = \bigcup \lambda U_\lambda \) such that for each open set \( U_\lambda \) there is an open domain \( V_\lambda \) of complex plane \( \mathbb{C} \) and a homeomorphism

\[ \phi_\lambda : V_\lambda \rightarrow U_\lambda \]

that satisfies that if \( U_\lambda \cap U_\mu \neq \emptyset \), then the “gluing map” : \( \phi_\mu^{-1} \circ \phi_\lambda \)

\[ V_\lambda \supset \phi_\lambda^{-1}(U_\lambda \cap U_\mu) \xrightarrow{\phi_\lambda} U_\lambda \cap U_\mu \xrightarrow{\phi_\mu^{-1}} \phi_\mu^{-1}(U_\lambda \cap U_\mu) \subset V_\mu \]

is a bioholomorphic function.

\[ \begin{array}{c}
\begin{array}{c}
\text{Figure 2.1: Gluing two coordinates charts}
\end{array}
\end{array} \]
Remarks:

- A topological space $X$ is paracompact if for every open covering $X = \bigcup_{\lambda} U_{\lambda}$, there is a locally finite open cover $X = \bigcup_{i} V_{i}$ such that $V_{i} \subset U_{\lambda}$ for some $\lambda$. Locally finite means that for every $x \in X$, there are only finitely many $V_{i}$'s that contain $x$.

- A continuous map $f : V \to \mathbb{C}$ from an open subset $V$ of $\mathbb{C}$ into the complex plane is said to be holomorphic if it admits a convergent Taylor series expansion at each point of $V \subset \mathbb{C}$. If a holomorphic function $f : V \to V'$ is one-to-one and onto, and its inverse is also holomorphic, then we call it biholomorphic.

- Each open set $V_{\lambda}$ gives a local chart of the Riemann surface $C$. We often identify $V_{\lambda}$ and $U_{\lambda}$ by the homeomorphism $\phi_{\lambda}$, and say “$U_{\lambda}$ and $U_{\mu}$ are glued by a biholomorphic function”. The collection $\{ \phi_{\lambda} : V_{\lambda} \to U_{\lambda} \}$ is called a local coordinate system.

- A Riemann surface is a complex manifold of complex dimension 1. We call the Riemann surface structure on a topological surface a complex structure. The definition of complex manifolds of an arbitrary dimension can be given in a similar manner.

Example: Let $\omega_{1}, \omega_{2} \in \mathbb{C}$ be two complex numbers which are linearly independent over the reals, and define an equivalence relation on $\mathbb{C}$ by $z_{1} \sim z_{2}$ if there are integers $m, n$ such that $z_{1} - z_{2} = m\omega_{1} + n\omega_{2}$. Let $X$ be the set of equivalence classes (with the quotient topology). A small enough disc $V$ around $z \in \mathbb{C}$ has at most one representative in each equivalence class, so this gives a local homeomorphism to its projection $U$ in $X$. If $U$ and $U'$ intersect, then the two coordinates are related by a map

$$z \mapsto z + m\omega_{1} + n\omega_{2}$$

which is holomorphic.

This surface is topologically described by noting that every $z$ is equivalent to one inside the closed parallelogram whose vertices are $0, \omega_{1}, \omega_{2}, \omega_{1} + \omega_{2}$, but that points on the boundary are identified.

![Figure 2.2: A Riemann Surface (Torus).](image)

We thus get a torus this way. Another way of describing the points of the torus is as orbits of the action of the group $\mathbb{Z} \times \mathbb{Z}$ on $\mathbb{C}$ by $(m, n) \cdot z = z + m\omega_{1} + n\omega_{2}$.

We will use this space in the coming section.
Elliptic Curves over $\mathbb{C}$

In the following sections, the focus is on elliptic curves over algebraically closed field of complex numbers $\mathbb{C}$.

3 Elliptic Integrals

Motivation: Consider the following 2 examples:

**Example 1.** Arc-length on a circle: Evaluating the integral of arc length of a circle namely, $\int \frac{1}{\sqrt{1-x^2}} \, dx$, leads us to the inverse trigonometric functions, therefore, in this case it is easily computable.

**Example 2.** Arc-length on an ellipse: The arc-length of an ellipse, $\frac{x^2}{a^2} + \frac{y^2}{b^2} = 1$ with $a \geq b > 0$ is: $4aE(\sqrt{1 - \left(\frac{b}{a}\right)^2})$, where $E(k) = \int_0^1 ((1-x^2)(1-k^2x^2))^{1/2} \, dx$. As we see, this integral is not computable in terms of ordinary functions.

Computing the arc-length of an ellipse and integrals of such form was the origin of the “name” of elliptic curves. Due to the indeterminacy in the sign of square root, the study of such integrals over $\mathbb{C}$ leads us to look at the Riemann surface on which they are naturally defined.

An elliptic curve over $\mathbb{C}$ is a Riemann surface

In case of the ellipse, this Riemann surface turns out to be set of complex points on an elliptic curve $E$. Therefore we begin studying certain integrals that are line integrals on $E(\mathbb{C})$. To study the elliptic integrals let $E$ be an elliptic curve defined over $\mathbb{C}$. Since $\text{char}(\mathbb{C}) = 0 \neq 2$ and $\mathbb{C}$ is algebraically closed, therefore there exists a Weierstrass equation in Legendre form:

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

The following natural map is a double cover ramified over precisely 4 points: 0, 1, $\lambda$, $\infty \in \mathbb{P}^1(\mathbb{C})$.

$$E(\mathbb{C}) \to \mathbb{P}^1(\mathbb{C})$$

$$(x,y) 
\mapsto x$$

On the other hand, by the following proposition, $\omega = dx/y$ is a holomorphic differential 1-form on $E$:

**Proposition 3.1 :** Let $E$ be an elliptic curve. Then the invariant differential $\omega$ associated to a Weierstrass equation for $E$ is holomorphic and non-vanishing. (i.e., $\text{div}(\omega) = 0$)

Now, consider the integral of differential form related to the line integral as the following:

$$\text{line integral : } \int \omega = \oint dx/y = \int \frac{dx}{\sqrt{x(x-1)(x-\lambda)}}$$

Define a map where the integral of the differential 1-form is along some path connecting $O$ to $P$:

$$E(\mathbb{C}) \to \mathbb{C}$$

$$(x,y) \mapsto \int_O^P \omega$$

As we will see, this map, unfortunately is not well-defined since it depends on the choice of path.
The following steps guides us to reach our goal of finding a solution to make the map well-defined. Also, the ideas of periods and lattice will be introduced. Let $P = (x, y) \in E(\mathbb{C})$ and examine what is happening in $\mathbb{P}^1(\mathbb{C})$:

**Step 1: Line Integral**

From the equation of $E$, we need to compute the complex integral:

$$
\int_{\infty}^{z} \frac{dt}{\sqrt{t(t-1)(t-\lambda)}}
$$

The square root in the above integral means that the line integral is not path independent. Therefore considering the figure below, the 3 integrals $\int_{\alpha} \omega$, $\int_{\beta} \omega$, $\int_{\gamma} \omega$ are not equal.

![Figure 3.1: Three path line integrals](image)

**Step 2: Branch Cuts**

In order to make the integral well-defined, it is necessary to consider the branch cuts. For example, the integral will be path-independent on the "complement" of the branch cuts illustrated in Figure below. This is because, in this region it is possible to define a single-valued branch of $\sqrt{t(t-1)(t-\lambda)}$.

The figure below shows branch cuts that makes the integral single-valued:

![Figure 3.2: Branch Cuts that make the integral single-valued](image)

Since the square root is double-valued, we should take two copies of Riemann Sphere of $\mathbb{P}^1(\mathbb{C})$, make branch cuts as indicated in Figure 3.3, and glue them together along the branch cuts to form a Riemann Surface illustrated in Figure 3.4.
**Riemann Sphere**: \( \mathbb{P}^1(\mathbb{C}) = \mathbb{C} \cup \{ \infty \} \) is topologically a 2- sphere and is called Riemann Sphere.

Two copies of Riemann Sphere of \( \mathbb{P}^1(\mathbb{C}) \), with branch cuts on the spheres is shown in below diagram:

![Diagram of Riemann Sphere](image)

Figure 3.3: Branch cuts on the sphere

**Gluing**: Matching the positive and negative signs on the cut and opened branch cuts from the two spheres and gluing them will give us the Riemann surface. It is readily seen that the resulting Riemann surface is a torus, and it is on this surface that we should study the integral.

\[ \therefore \text{ The Riemann Surface is a torus.} \]

![Diagram of Glued branch cuts](image)

Figure 3.4: Glued branch cuts (Torus)

**Step 3: Periods and Lattices**

We return to our map: \( E(\mathbb{C}) \to \mathbb{C} \), with \( P \mapsto \int_\alpha^P \omega \). As it is shown in figure 3.5, we can see that the indeterminacy comes from integrating across branch cuts in \( \mathbb{P}^1 \) or around non-contractible loops on the torus.

![Diagram of Paths](image)

Figure 3.5: Paths in \( \mathbb{P}^1(\mathbb{C}) \) and on Torus

Consider two closed paths \( \alpha \) and \( \beta \) for which the integrals \( \int_\alpha \omega, \int_\beta \omega \) maybe non-zero and define:
Periods of \( E \):

We have obtained two complex numbers, called periods of \( E \):

\[
\omega_1 = \int_{\alpha} \omega, \quad \omega_2 = \int_{\beta} \omega
\]

Lattice \( \Lambda \):

The paths \( \alpha \) and \( \beta \) generate the first homology group of the torus therefore any two paths from \( O \) to \( P \) differ by a path that is homologous to \( n_1 \alpha + n_2 \beta \) for \( n_1, n_2 \in \mathbb{Z} \). Therefore the integral is well-defined up to addition of a number of the form \( n_1 \alpha + n_2 \beta \), which leads us to introduce the set:

\[
\Lambda = \{ n_1 \alpha + n_2 \beta : n_1, n_2 \in \mathbb{Z} \}
\]

Step 4: Well-defined

At this step we will show that there is a well-defined map:

\[
F : E(\mathbb{C}) \rightarrow \mathbb{C}/\Lambda
\]

\[
P \mapsto \int_{\mathcal{O}}^P \omega \pmod{\Lambda}
\]

We will verify that \( F \) is a homomorphism by using the translation invariance of \( \omega \):

**Proposition 3.2**: Let \( E/K \) be an elliptic curve given by Weierstrass equation

\[
E : y^2 + a_1 xy + a_3 y = x^3 + a_2 x^2 + a_4 x + a_6
\]

and \( \omega \) be a differential 1-form:

\[
\omega = \frac{dx}{2y + a_1 x + a_3} \in \Omega_E
\]

Let \( Q \in E \) and let \( \tau_Q : E \rightarrow E \) be the translation-by- \( Q \) map. Then \( \tau_Q^* \omega = \omega \).

**\( F \) is a homomorphism**

To continue, we must show \( F \) is a homomorphism:

\[
\int_{\mathcal{O}}^{P+Q} \omega \equiv \int_{\mathcal{O}}^P \omega + \int_{P}^{P+Q} \omega \equiv \int_{\mathcal{O}}^P \omega + \int_{\mathcal{O}}^Q \tau_Q^* \omega \equiv \int_{\mathcal{O}}^P \omega + \int_{\mathcal{O}}^Q \omega \pmod{\Lambda}
\]

\( \mathbb{C}/\Lambda \) will be a Riemann surface

The quotient space \( \mathbb{C}/\Lambda \) will be a Riemann surface, i.e. a 1-dimensional complex manifold, if and only if \( \Lambda \) is a lattice, i.e. if and only if the periods \( \omega_1 \) and \( \omega_2 \) that generate \( \Lambda \) are linearly independent over \( \mathbb{R} \). Furthermore, it is proven that the map \( F \) is a complex analytic isomorphism. We will present this proof in later section (The Abel Jacobi Theorem), but at this stage will continue the study of the space \( \mathbb{C}/\Lambda \) for a given lattice \( \Lambda \).
4 Elliptic Functions

Let $\Lambda \subset \mathbb{C}$ be a lattice, i.e. $\Lambda$ is a discrete subgroup of $\mathbb{C}$ which contains an $\mathbb{R}$-basis for $\mathbb{C}$. The following material is the study of meromorphic functions on the quotient space $\mathbb{C}/\Lambda$; i.e. the meromorphic functions on $\mathbb{C}$ that are periodic with respect to lattice $\Lambda$.

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

$$f(z + \omega) = f(z) \quad \text{for } \forall \omega \in \Lambda, \ z \in \mathbb{C}$$

The set of all such functions is denoted by $\mathbb{C}(\Lambda)$.

**Note:** $\mathbb{C}(\Lambda)$ is a field.

**Definition.** A fundamental parallelogram for $\Lambda$ is the set of the form

$$D = \{a + t_1 \omega_1 + t_2 \omega_2 : 0 \leq t_1, t_2 < 1\}$$

where $a \in \mathbb{C}$ and $\{\omega_1, \omega_2\}$ is a basis for $\Lambda$.

A lattice and 3 different fundamental parallelogram are illustrated below:

![Figure 4.1: Fundamental Parallelograms](image)

**Note:** The definition of $D$ implies that the natural map $D \rightarrow \mathbb{C}/\Lambda$ is bijective.

![Figure 4.2: Riemann Surface = A Complex Torus](image)
Before proceeding to the following proposition, we present Liouville’s theorem:

**Liouville’s Theorem**: Every bounded entire function must be constant.

(Corollary of Liouville’s theorem: A non-constant elliptic functions cannot be defined on $\mathbb{C}$)

**Proposition 4.1**: A holomorphic elliptic function, i.e. an elliptic function with no poles is constant. Similarly, an elliptic function with no zeros is constant.

**Proof**.
Let $f$ be an elliptic function relative to lattice $\Lambda$, i.e. $f(z) \in \mathbb{C}(\Lambda)$. Suppose $f(z)$ is holomorphic. Let $D$ be a fundamental parallelogram for $\Lambda$. We know $f$ is an elliptic function therefore it is periodic, i.e. $f(z + \omega) = f(z)$ for $\forall \omega \in \Lambda$, $z \in \mathbb{C}$, hence we have:

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

Since the map $D \rightarrow \mathbb{C}/\Lambda$ is bijective, it is enough to analyze $\sup_{z \in D} |f(z)|$ in $\bar{D}$ instead of $\mathbb{C}$.

By assumption our function $f$ has no poles hence it is continuous and also, we know that $\bar{D}$ is compact so $|f(z)|$ is bounded on $\bar{D}$ hence it is bounded on all $\mathbb{C}$. Now we use Liouville’s Theorem as $f$ is holomorphic on $\mathbb{C}$, or entire, therefore $f$ is constant.

To prove for an elliptic function with no zero (or no root), by fundamental theorem of algebra the degree of this function cannot be greater or equal to one therefore it is constant. Another way is to say if $f$ has no zeros, then $1/f$ is holomorphic and bounded, hence constant. □

**Order and Residue**
Let $w \in \mathbb{C}$ and $f$ be an elliptic function. By definition of elliptic functions, $f$ is meromorphic, and we define its order of vanishing and its residue at point $w \in \mathbb{C}$ denoted by:

$$\text{ord}_w(f) = \text{order of vanishing of } f \text{ at } w$$

$$\text{res}_w(f) = \text{residue of } f \text{ at } w$$

**Note**: Multiplicity of zero at $f$ at is the positive integer $n \in \mathbb{Z}^+$ where $f(z) = (z - w)^n g(z)$, is known as *order of vanishing of $f$ at $w$.*

By definition $f$ is an elliptic function, therefore is periodic and $f(w + \omega) = f(w)$ for $\forall \omega \in \Lambda$, $w \in \mathbb{C}$, hence $w$ can be replaced by $w + \omega$ for any $\omega \in \Lambda$.

**Notation**
The notation $\sum_{w \in \mathbb{C}/\Lambda}$ denotes a sum over $w \in D$, where $D$ is a fundamental parallelogram for $\Lambda$.

**Note**: The value of the sum is independent of the choice of $D$ and only finitely many terms of the sum are nonzero. ($D$ is compact)
Theorem 4.2: Let \( f(z) \in \mathbb{C}(\Lambda) \) be an elliptic function relative to \( \Lambda \).

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

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

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

Proof.

Let \( D \) be a fundamental parallelogram for \( \Lambda \) such that \( f(z) \) has no zeros or poles on the boundary \( \partial D \) of \( D \). All three parts of the theorem are simple applications of the residue theorem applied to appropriately chosen functions on \( D \).

(a): By residue theorem we have:

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

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 as we can write:

Let be the set \( \{\omega_1, \omega_2\} \) be the periods of \( \Lambda \) and the boundary is consist of 4 \( \gamma \)'s. Write:

\( \partial D = \gamma_1 + \gamma_2 + \gamma_3 + \gamma_4 \)

we have:

\[
\int_{\partial D} f = \int_{\gamma_1} f + \int_{\gamma_2} f + \int_{\gamma_3} f + \int_{\gamma_4} f
\]

\[
= \int_A^B f + \int_B^C f + \int_C^D f + \int_A^D f
\]

As in the diagram:

Figure 4.3: Directions on the boundary of \( D \)

Assume \( \omega_1, \omega_2 \) are the periods of \( \Lambda \). The periodicity of \( f \) and change of variable : \( z \mapsto z + \omega_2 \) gives:

\[
\int_A^B f(z)dz = \int_{A+\omega_2}^{B+\omega_2} f(z)dz = \int_C^D f(z)dz = -\int_C^D f(z)dz
\]
Similarly:
\[ \int_B^C f(z) \, dz = - \int_A^D f(z) \, dz \]

And the proof of part (a) is complete.

(b) The periodicity of \( f(z) \) implies that \( f'(z) \) is also periodic, therefore the function \( f'(z)/f(z) \) is an elliptic function and applying (a) on this function gives:
\[ \sum_{w \in \mathbb{C}/\Lambda} \text{res}_w (f'/f) = 0 \]
But since: \( \text{ord}_w(f) = \frac{1}{2\pi i} \oint_{\partial D} (f'/f) = \text{res}_w(f'/f) \), therefore the proof is complete.

(c) For this part we apply the residue theorem to the function: \( z f'(z)/f(z) \) and write:
\[ \sum_{w \in \mathbb{C}/\Lambda} \text{ord}_w(f) \cdot w = \frac{1}{2\pi i} \oint_{\partial D} z \frac{f'(z)}{f(z)} \, dz \]
therefore:
\[ \sum_{w \in \mathbb{C}/\Lambda} \text{ord}_w(f) \cdot w = \frac{1}{2\pi i} \left( \int_a^{a+\omega_1} + \int_{a+\omega_1}^{a+\omega_1+\omega_2} + \int_{a+\omega_1+\omega_2}^{a+\omega_2} \right) z \frac{f'(z)}{f(z)} \, dz \]
In the second (respectively third) integral a change of variable: \( z \mapsto z + \omega_1 \) (respectively \( z \mapsto z + \omega_2 \)), the periodicity of \( f'(z)/f(z) \) yields:
\[ \sum_{w \in \mathbb{C}/\Lambda} \text{ord}_w(f) \cdot w = \frac{-\omega_2}{2\pi i} \int_a^{a+\omega_1} \frac{f'(z)}{f(z)} \, dz + \frac{\omega_1}{2\pi i} \int_a^{a+\omega_2} \frac{f'(z)}{f(z)} \, dz \]
Recall that 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 \textbf{winding number} around 0 of the path:
\[ [0, 1] \to \mathbb{C}, \ t \mapsto g((1-t)a + tb) \]
In particular, if \( g(a) = g(b) \), then the integral is an integer.

Therefore, with \( f(a) = f(a+\omega_1) = f(a+\omega_2) \), and the periodicity of \( f'/f \) implies that \( \sum_{w \in \mathbb{C}/\Lambda} \text{ord}_w(f) \cdot w \) has the form: \( -\omega_2 n_2 + \omega_1 n_1 \) for integers \( n_1 \) and \( n_1 \) and this is clearly an element of \( \Lambda \). \( \square \)
Order of an elliptic function

**Definition.** The order of an elliptic function is its number of poles (counted with multiplicity) in a fundamental parallelogram. (By Theorem 4.2 part (b) the order is also equal to the number of zeros.)

**Corollary 4.3:** A non-constant elliptic function has order at least 2.

**Proof.**

If \( f(z) \) has a single simple pole, then by Theorem 4.2 (a) the residue at that pole is 0, so \( f(z) \) is actually holomorphic. Now applying Proposition 4.1 the function can only be constant, which is not the case by the assumption hence, the elliptic function of order of at least 2 is required and the proof is complete. □

\( \mathbb{C}/\Lambda \) is a group

The set \( \Lambda \) is an additive subgroup of \( \mathbb{C} \), hence the quotient \( \mathbb{C}/\Lambda \) is a group. The group law on \( \mathbb{C}/\Lambda \) being induced by addition on \( \mathbb{C} \). The group operations are given by holomorphic functions and therefore \( \mathbb{C}/\Lambda \) is a 1-dimensional complex Lie group. (Related material to be presented in Theorem 5.7)

**Divisor group of \( \mathbb{C}/\Lambda \)**

We now define the divisor group of \( \mathbb{C}/\Lambda \), denoted by \( \text{Div}(\mathbb{C}/\Lambda) \), to be the group of formal linear combinations: 
\[
\sum_{w \in \mathbb{C}/\Lambda} n_w(w) \text{ with } n_w \in \mathbb{Z} \text{ and } n_w = 0 \text{ for all but finitely many } w.
\]

Then for \( D = \sum_{w \in \mathbb{C}/\Lambda} n_w(w) \in \text{Div}(\mathbb{C}/\Lambda) \) we define:

\[
\deg D = \text{degree of } D = \sum_{w \in \mathbb{C}/\Lambda} n_w
\]

and

\[
\text{Div}^0(\mathbb{C}/\Lambda) = \{ D \in \text{Div}(\mathbb{C}/\Lambda) : \deg D = 0 \}
\]

**Divisor of \( f \):** For any \( f \in \mathbb{C}(\Lambda)^* \) we define the divisor of \( f \) to be

\[
\text{div}(f) = \sum_{w \in \mathbb{C}/\Lambda} \text{ord}_w(f)(w)
\]

Also \( \text{div}(f) \in \text{Div}^0(\mathbb{C}/\Lambda) \). Each \( \text{ord}_w \) is a valuation hence the following map is a homomorphism:

\[
\text{div} : \mathbb{C}(\Lambda)^* \longrightarrow \text{Div}^0(\mathbb{C}/\Lambda)
\]

**Summation map:** Define the summation map:

\[
\text{sum} : \text{Div}^0(\mathbb{C}/\Lambda) \longrightarrow \mathbb{C}(\Lambda)
\]

with

\[
\text{sum}(\sum_{w \in \mathbb{C}/\Lambda} n_w(w)) = \sum_{w \in \mathbb{C}/\Lambda} n_w(w) \pmod{\Lambda}
\]

**Theorem 4.4:** The following is an exact sequence:

\[
1 \longrightarrow \mathbb{C}^* \longrightarrow \mathbb{C}(\Lambda)^* \xrightarrow{\text{div}} \text{Div}^0(\mathbb{C}/\Lambda) \xrightarrow{\text{sum}} \mathbb{C}/\Lambda \longrightarrow 0
\]
5 Construction of Elliptic Functions

To show the previous ideas are relative, we must construct some elliptic functions. By corollary 4.3: A non-constant elliptic function has order at least 2; hence any such function at least must be of order 2. Following Weierstrass idea, we look for a function with pole of order 2 at \( z = 0 \).

**Weierstrass \( \wp \) - function**

**Definition.** Let \( \Lambda \in \mathbb{C} \) be a lattice. The Weierstrass \( \wp \) - function, relative to \( \Lambda \), is defined by the series:

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

**Eisenstein series of weight 2k**

**Definition.** The Eisenstein series of weight 2k, for \( \Lambda \) is the series:

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

**Theorem 5.1:** Let \( \Lambda \in \mathbb{C} \) be a lattice.

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

(b) The series defining the Weierstrass \( \wp \) - function converges absolutely and uniformly on every compact subset of \( \mathbb{C} \setminus \Lambda \). It 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): Suppose \( D \) be the fundamental parallelogram of lattice \( \Lambda \). Let \( A \) be the area of \( D \). Inside a circle of radius \( R \) in lattice, there will be discrete number of points of the lattice, therefore, roughly speaking, the area of circle is: \( \pi \cdot R^2 = (\text{number of } D) \cdot A \)

The number of lattice points inside this circle is approximately: \( \frac{\pi R^2}{A} + O(R) \), so there exists a constant value \( c = c(\Lambda) \) such that for all \( N \geq 1 \), the number of lattice points in an annulus satisfies:

\[
\# \{ \omega \in \Lambda : N \leq |\omega| < N + 1 \} < cN,
\]

hence: \( G_{2k}(\Lambda) = \sum_{\omega \in \Lambda, \omega \neq 0} \omega^{-2k} \leq \sum_{N=1}^{\infty} \frac{cN}{N^{2k}} = c \sum_{N=1}^{\infty} \frac{1}{N^{2k-1}} < \infty \)

Note: The first inequality above is because: \( N \leq |\omega| \) so \( \frac{1}{|\omega|^2} \leq \frac{1}{N^2} \).

Therefore proof is complete if \( 2k - 1 > 1 \) or, for \( k > 1 \) and \( G_{2k}(\Lambda) \) is absolutely convergent.

(b) To prove the absolute convergent of the Weierstrass \( \wp \) - function it suffices to find a bound for:

\[
\left| \frac{1}{(z - \omega)^2} - \frac{1}{\omega^2} \right|
\]
If $|\omega| > 2|z|$, write:
\[
\left| \frac{1}{(z - \omega)^2} - \frac{1}{\omega^2} \right| = \left| \frac{2\omega - z}{\omega^2 (z - \omega)^2} \right| \leq \frac{|z|(2|\omega| + |z|)}{|\omega|^2(|\omega| - |z|)^2} \leq \frac{10|z|}{|\omega|^2}
\]

(Since $\frac{|\omega|}{2} > |z|$, so $2|\omega| + |z| < \frac{5}{2}|\omega|$ and $\frac{|\omega|}{2} \leq |\omega| - |z| \leq |\omega| - |z|$)

To complete the proof, observe that for any given $|z|$, the summation: \[
\sum_{\omega \in \mathbb{C} \setminus \Lambda, \omega \neq 0} 10\frac{|z|}{|\omega|^2}
\]
converges absolutely by part (a). Thus $\wp(z)$ is absolutely convergent for $z \in \mathbb{C} \setminus \Lambda$ and uniformly convergent on every compact subset of $\mathbb{C} \setminus \Lambda$. Consequently, $\wp(z)$ defines a holomorphic function on $\mathbb{C} \setminus \Lambda$ and in addition by observing the series expansion, it is clear that $\wp(z)$ has a double pole with residue 0 at each point of $\Lambda$.

(c) To show $\wp(z)$ is an even function consider:
\[
\wp(z; \Lambda) = \frac{1}{z^2} + \sum_{\omega \in \Lambda, \omega \neq 0} \left( \frac{1}{(z - \omega)^2} - \frac{1}{\omega^2} \right)
\]

Let $\omega = m\omega_1 + n\omega_2$ where $m, n \in \mathbb{Z}$. By definition of lattices, $-\omega \in \Lambda$, and: $-\omega = (-m)\omega_1 + (-n)\omega_2$ therefore:
\[
\wp(-z; \Lambda) = \frac{1}{(-z)^2} + \sum_{-\omega \in \Lambda, \omega \neq 0} \left( \frac{1}{(-z - \omega)^2} - \frac{1}{\omega^2} \right) = \wp(z; \Lambda)
\]

Hence $\wp(z)$ is an even function. To see that is an elliptic function, we must show: $\wp(z + \omega) = \wp(z)$ for all $z, \omega \in \mathbb{C}$. By part (b) we know that $\wp(z)$ is uniformly convergent series and we may differentiate term by term:
\[
\wp'(z) = \frac{-2}{z^2} + \sum_{\omega \in \Lambda, \omega \neq 0} \frac{-2}{(z - \omega)^3} = \sum_{\omega \in \Lambda} \frac{-2}{(z - \omega)^3}
\]

Now, let $\lambda \in \Lambda$ and by definition $\lambda - \omega \in \Lambda$, hence:
\[
\wp'(z + \lambda) = \sum_{\omega \in \Lambda} \frac{-2}{(z + \lambda - \omega)^3} = \sum_{\omega \in \Lambda} \frac{-2}{(z - (\lambda - \omega))^3} = \wp'(z)
\]

This shows $\wp'(z)$ is periodic and since it is meromorphic, it is also an elliptic function. Integrating yields:
\[
\wp(z + \lambda) = \wp(z) + c(\lambda) \quad for\ all\ z \in \mathbb{C} \setminus \Lambda
\]

The function $c(\lambda)$ does not depend on $z$. Now set $z = -\frac{\lambda}{2}$ then:
\[
\wp(\frac{\lambda}{2}) = \wp(-\frac{\lambda}{2}) + c(\lambda)
\]

But $\wp(z)$ is an even function, therefore:
\[
\wp(\frac{\lambda}{2}) = \wp(\frac{\lambda}{2}) + c(\lambda)
\]

Hence: $c(\lambda) = 0$ and proof is complete.

16
The following theorem shows that every elliptic curve can be expressed as a rational function of the Weierstrass $\wp$ - function and it’s derivative. we will not present the proof in here.

**Theorem 5.2** : Let $\Lambda \in \mathbb{C}$ be a lattice. Then $\mathbb{C}(\Lambda) = \mathbb{C}(\wp(z), \wp'(z))$.

**Theorem 5.3** :
(a) The Laurent series for $\wp(z)$ about $z = 0$ 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 it’s derivative satisfy the relation:

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

*Proof.*

(a) Provided $|z| < |\omega|$, we have:

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

To see this, write:

$$\sum_{n=1}^{\infty} (n + 1) \frac{z^n}{\omega^{n+2}} = \sum_{n=0}^{\infty} (n + 1) \frac{z^n}{\omega^{n+2}} - \frac{1}{\omega^2}$$

and:

$$\sum_{n=0}^{\infty} (n + 1) \frac{z^n}{\omega^{n+2}} = \frac{1}{\omega^2} \sum_{n=0}^{\infty} \frac{z^n}{\omega^n} = \frac{1}{\omega^2} \sum_{n=0}^{\infty} \frac{d}{dz} \left( \frac{z^{n+1}}{\omega^n} \right) = \frac{1}{\omega^2} \frac{d}{dz} \left( \sum_{n=0}^{\infty} \frac{z^{n+1}}{\omega^n} \right)$$

and by geometric series:

$$\frac{1}{\omega^2} \frac{d}{dz} \left( \sum_{n=0}^{\infty} \frac{z^{n+1}}{\omega^n} \right) = \frac{1}{\omega^2} \frac{d}{dz} \left( \frac{z}{1 - \frac{z}{\omega}} \right) = \frac{1}{(1 - \frac{z}{\omega})^2}$$

Substituting this into the series of $\wp(z)$ and reversing the order of summation:

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

Let: $n = 2k$

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

Therefore:

$$\wp(z) = \frac{1}{z^2} + \sum_{k=1}^{\infty} (2k + 1)G_{2k+2}z^{2k}.$$
(b) By part (a), writing the first few terms in the Laurent expansions, with simple computations we have:

\[ \varphi(z) = z^{-2} + \sum_{k=1}^{\infty} (2k+1)G_{2k+2}z^{2k}, \]

\[ \varphi'(z) = -2z^{-3} + \sum_{k=1}^{\infty} 2k(2k+1)G_{2k+2}z^{2k-1}, \]

\[ \varphi'(z)^2 = 4z^{-6} - 24G_4z^{-2} - 80G_6 + \ldots, \]

\[ \varphi(z)^3 = z^{-6} + 9G_4z^{-2} + 15G_6 + \ldots, \]

\[ \varphi(z) = z^{-2} + 3G_4z^{2} + \ldots. \]

Comparing these, we write the function \( f \) as:

\[ f(z) = \varphi'(z)^2 - 4\varphi(z)^3 + 60G_4\varphi(z) + 140G_6 \]

This function, is not just meromorphic, but it is holomorphic and it’s value at point \( z = 0 \) is 0, \( f(z) = 0 \). In addition, \( \varphi(z) \) and \( \varphi'(z) \) are both elliptic functions therefore \( f \) is an elliptic function relative to \( \Lambda \).

On the other hand, by proposition 4.1: An elliptic function with no poles (or no zeros) is constant. We conclude that \( f(z) \) is identically zero and proof is complete. 

**Remark 5.4 :** It is standard notation to set

\[ g_2 = g_2(\Lambda) = 60G_4, \quad g_3 = g_3(\Lambda) = 140G_6 \]

Therefore the algebraic relation between \( \varphi(z) \) and \( \varphi'(z) \) will be as following:

\[ \varphi'(z)^2 = 4\varphi(z)^3 - g_2\varphi(z) - g_3 \]

**Remark 5.5 :** In summary, the following is the result of the preceding material:

- \( f(z) \) is a globally defined doubly periodic meromorphic function with possible poles at the lattice \( \Lambda \).
- \( f(z) \) is holomorphic at the origin, and hence, holomorphic at every lattice points.
- \( f(z) \) has a double zero at the origin.
Remark 5.6: We have derived the Weierstrass differential equation:
\[ \varphi'(z)^2 = 4\varphi(z)^3 - g_2\varphi(z) - g_3 \]
This implies the elliptic integral:
\[ z = \int dz = \int \frac{dz}{d\varphi} = \int \frac{1}{d\varphi/dz} = \int \frac{1}{\varphi'} = \int \frac{1}{\sqrt{4\varphi(z)^3 - g_2\varphi(z) - g_3}} \]
Hence the Weierstrass \( \varphi \)-function is the inverse function of an elliptic integral.

\[ \mathbb{C}/\Lambda \text{ is complex analytically isomorphic to an elliptic curve } E \]
Let \( E/\mathbb{C} \) be an elliptic curve. Since the group law \( E \times E \to E \) is given by everywhere locally defined rational functions, we see in particular \( E = E(\mathbb{C}) \) is a complex Lie group. If \( \Lambda \subset \mathbb{C} \) is a lattice, then \( \mathbb{C}/\Lambda \) with its natural addition is complex Lie group.

Proposition 5.7: Let \( g_2 \) and \( g_3 \) 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. Its discriminant:
\[ \Delta(\Lambda) = g_2^3 - 27g_3^2 \]
is not zero.
(b) Let \( E/\mathbb{C} \) be the curve:
\[ E: y^2 = 4x^3 - g_2x - g_3 \]
which is an elliptic curve from (a). Then the map:
\[ \phi: \mathbb{C}/\Lambda \to E \subset \mathbb{P}^2(\mathbb{C}) \]
\[ z \mapsto [\varphi(z), \varphi'(z), 1] \]
is a complex analytic isomorphism of complex Lie groups, i.e., it is an isomorphism of Riemann surfaces which is a group homomorphism.

Proof.
(a) Let \( \{\omega_1, \omega_2\} \) be a basis for \( \Lambda \), and let \( \omega_3 = \omega_1 + \omega_2 \). Then since \( \varphi(z) \) is an even function and consequently \( \varphi'(z) \) is an odd elliptic function, write:
\[ \varphi'(\frac{\omega_i}{2}) = -\varphi'(-\frac{\omega_i}{2}) = -\varphi'(\omega_1 - \frac{\omega_i}{2}) = -\varphi'(\frac{\omega_i}{2}) \]
Hence: \( \varphi'(\frac{\omega_i}{2}) = 0 \). By proposition 5.3 (b) for \( z = \frac{\omega_i}{2} \not\in \Lambda \) and \( x = \varphi(\frac{\omega_i}{2}) \) the function \( f \) vanishes, \( f(x) = 0 \), therefore it suffices to show these three values are distinct.
To prove this part we must compute its \( e^\phi \). Considering the assumption, we obtain

\[ \text{And: } x = \phi \left( \frac{\omega_1}{2} \right), \quad f(x) = 4x^3 - g_2x - g_3 \implies f(x) = 4\phi \left( \frac{\omega_1}{2} \right)^3 - g_2\phi \left( \frac{\omega_1}{2} \right) - g_3 = \phi' \left( \frac{\omega_1}{2} \right)^2 = 0. \]

The function \( \phi(z) - \phi \left( \frac{\omega_1}{2} \right) \) is even, hence it will have at least double zero at points \( z = \frac{\omega_1}{2} \). On the other hand, it is also an elliptic function of order 2 therefore it has only these zeros in an appropriate fundamental parallelogram. Hence \( \phi \left( \frac{\omega_i}{2} \right) \neq \phi \left( \frac{\omega_j}{2} \right) \) for \( i \neq j \) and the roots are distinct values and the proof is complete.

**Note:** Let \( e_1, e_2 \) and \( e_3 \) be the roots of the polynomial equation \( 4X^3 - g_2X - g_3 = 0 \), then except the four points \( e_1, e_2, e_3, \infty \) of \( \mathbb{P}^1 \), the map \( \phi \) is two-to-one. This is because only at pre-image of \( e_1, e_2 \) and \( e_3 \) the derivative \( \phi' \) vanishes, and we know \( \phi \) has a double pole at 0. The map \( \phi \) is called a branched double covering of \( \mathbb{P}^1 \) ramified at \( e_1, e_2, e_3 \) and \( \infty \). It is customary to choose the three roots \( e_1, e_2 \) and \( e_3 \) so that we have:

\[ \phi \left( \frac{\omega_1}{2} \right) = e_1, \quad \phi \left( \frac{\omega_2}{2} \right) = e_2, \quad \phi \left( \frac{\omega_1 + \omega_2}{2} \right) = e_3. \]

The quantities \( \frac{\omega_1}{2}, \frac{\omega_2}{2} \) and \( \frac{\omega_1 + \omega_2}{2} \) are called the half periods of the Weierstrass \( \phi \)-function.

(b) By Proposition 5.3 (b), the image of \( \phi \) is contained in \( E \). The following proves \( \phi \) is a complex analytic isomorphism:

**\( \phi \) is surjective**

To show \( \phi \) is surjective, let \( (x, y) \in E \). Then with \( x = \phi \left( \frac{\omega_1}{2} \right) \), the function \( \phi(z) - x \) is a non-constant elliptic function, so by proposition 4.1 it has a zero, say \( z = a \). It follows that \( \phi' (a)^2 = y^2 \), replacing \( a \mapsto -a \) if necessary, we obtain \( \phi' (a) = y \). Then \( \phi(a) = (x, y) \) and \( \phi \) is surjective.

**\( \phi \) is injective**

Next, we suppose that \( \phi(z_1) = \phi(z_2) \). Assume first \( 2z_1 \notin \Lambda \). Then function \( \phi(z) - \phi(z_1) \) is elliptic of order 2 and it vanishes at \( z_1, -z_1, z_2 \). Only possibility will be that two of these values are congruent modulo \( \Lambda \) and considering the assumption, \( 2z_1 \notin \Lambda \), we must have: \( z_2 \equiv \pm z_1 (\text{mod } \Lambda) \). Then

\[ \phi' (z_1) = \phi' (z_2) = \phi' (\pm z_1) = \pm \phi' (z_1) \]

implies: \( z_2 \equiv z_1 (\text{mod } \Lambda) \)

On the other hand, if \( 2z_1 \in \Lambda \) then \( \phi(z) - \phi(z_1) \) has a double zero at \( z_1 \) and vanishes at \( z_2 \), and again we conclude \( z_2 \equiv z_1 (\text{mod } \Lambda) \). This completes the proof \( \phi \) is injective.

**\( \phi \) is analytic isomorphism**

To prove this part we must compute its effect on cotangent space. At every point of \( E \), the differential 1-form \( \omega = dx/y \) is a non-vanishing holomorphic function. since:

\[ \phi^*(dx/y) = \frac{d\phi(z)}{\phi'(z)} = dz \]

is also non-vanishing and holomorphic at every point of \( \mathbb{C}/\Lambda \) we can see \( \phi \) is a local analytic isomorphism. But \( \phi \) is bijective by above proof, therefore this implies that it is a global isomorphism.
\( \phi \) is group homomorphism

Let \( z_1, z_2 \in \mathbb{C} \). Then there is a function \( f(z) \in \mathbb{C}(\Lambda) \) with the divisor:

\[
\text{div}(f) = (z_1 + z_2) - (z_1) - (z_2) + (0)
\]

By theorem 5.2, we can write \( f(z) = F(\wp(z), \wp'(z)) \) for some rational function \( F(X, Y) \in \mathbb{C}(X, Y) \) and considering \( F(x, y) \in \mathbb{C}(x, y) = \mathbb{C}(E) \), We have:

\[
\text{div}(F) = (\wp(z_1 + z_2)) - (\wp(z_1)) - (\wp(z_2)) + (\wp(0))
\]

Therefore:

\[
\wp(z_1 + z_2) = \wp(z_1) + \wp(z_2)
\]

and the proof is complete. \( \blacksquare \)

The Abel-Jacobi map

The Abel-Jacobi map for \( E(\mathbb{C}) \) is defined by formula: ( \( \alpha \equiv \wp^{-1} \) )

\[
\alpha : E(\mathbb{C}) \rightarrow \mathbb{C}/\Lambda, \quad \alpha(P) = \int_{\mathcal{O}}^P \omega \pmod{\Lambda}
\]

This is a holomorphic map satisfying \( \alpha^*(dz) = \omega \) and the induced map on homology groups:

\[
\alpha_* : H_1(E(\mathbb{C}), \mathbb{Z}) \rightarrow H_1(\mathbb{C}/\Lambda, \mathbb{Z}) = \Lambda
\]

is an isomorphism, as:

\[
\{ \int_{\gamma} dz \mid \gamma : \text{a closed path on } \mathbb{C}/\Lambda \} = \Lambda
\]

The canonical identification of \( \Lambda \) and the first homology group of \( \mathbb{C}/\Lambda \) is defined as follows: one associates to each \( u \in \Lambda \) the homology class of the projection to \( \mathbb{C}/\Lambda \) of any path in \( \mathbb{C} \) from 0 to \( u \). (Note: this is well-defined, as \( \mathbb{C} \) is contractible).

**Theorem 5.8**: The map \( \alpha : E(\mathbb{C}) \rightarrow \mathbb{C}/\Lambda \) is an isomorphism of compact Riemann surfaces.

**Proof**.

Before we begin the proof, we will present the following proposition:

**Proposition 5.9**: If \( X \) and \( Y \) are Riemann surfaces and the map \( f : X \rightarrow Y \) is bijective, then the ramification index, \( e_x = 1 \) for every \( x \in X \) and \( f^{-1} : Y \rightarrow X \) is holomorphic.

Hence, it suffices to show that \( \alpha \) is bijective. For each \( P \in E(\mathbb{C}) \), we have:

\[
\text{ord}_P(\alpha^*(dz - \alpha(P))) = \text{ord}_P(\alpha^*(dz)) = \text{ord}_P(\omega) = 0
\]

Hence the ramification index \( e_P = 1 \), i.e., for \( f = \alpha \) and \( \omega = dz \) in formula: \( \text{ord}_x(f^*(d(z))) = e_x - 1 \)

This implies that \( \alpha \) is an unramified covering. As the induced map on fundamental groups

\[
\pi_1(E(\mathbb{C}), \mathcal{O}) = H_1(E(\mathbb{C}), \mathbb{Z}) \xrightarrow{\alpha_*} H_1(\mathbb{C}/\Lambda, \mathbb{Z}) = \pi_1(\mathbb{C}/\Lambda, 0)
\]

is an isomorphism, and theory of covering spaces implies that \( \alpha \) is a bijection, as required, hence the proof is complete. \( \blacksquare \)
Weierstrass φ-function and Complex Projective Space

A meromorphic function is a holomorphic map into the Riemann sphere \( \mathbb{P}^1 \). Thus the Weierstrass φ-function defines a holomorphic map from an elliptic curve onto the Riemann sphere:

\[
\phi : E \equiv \mathbb{C}/\Lambda \rightarrow \mathbb{P}^1 = \mathbb{C} \cup \{\infty\}
\]

It is proven that this map is surjective. This is done by proving that the Weierstrass \( \wp \) function is surjective \( \mathbb{C} \setminus \Lambda \rightarrow \mathbb{C} \) is surjective.

The complex projective space \( \mathbb{P}^n \) of dimension \( n \) is the set of equivalence classes of nonzero vectors \( (x_0, x_1, ..., x_n) \in \mathbb{C}^{n+1} \). Where \( (x_0, x_1, ..., x_n) \) and \( (y_0, y_1, ..., y_n) \) are equivalent if there is a nonzero complex number \( c \) exists such that \( y_j = cx_j \) for all \( j \). The equivalence class of vector \( (x_0, x_1, ..., x_n) \) is denoted by \( (x_0 : x_1 : ... : x_n) \).

We define the map from an elliptic curve into \( \mathbb{P}^1 \) by:

\[
\phi = (\wp, \wp') : E \equiv \mathbb{C}/\Lambda \rightarrow \mathbb{P}^2
\]

As the following: For \( 0 \neq z \in E \), we map it to \((\wp(z) : \wp'(z) : 1) \in \mathbb{P}^2 \). The origin of the elliptic curve is mapped to \((0 : 1 : 0) \in \mathbb{P}^2 \). In terms of the global coordinate \((X : Y : Z) \in \mathbb{P}^2 \), the image of the map satisfies a homogeneous cubic equation

\[
Y^2Z - 4X^3 + g_2XZ^2 + g_3Z^3 = 0
\]

The zero locus \( C \) of this cubic equation is a cubic curve, and this is the reason that the Riemann surface \( E \) is called a curve. The affine part of the curve \( C \) is the locus of the equation

\[
Y^2 = 4X^3 - g_2X - g_3
\]

In \((X, Y)\)-plane and its real locus looks like figure below:

![Figure 5.1: An example of nonsingular cubic curve \( Y^2 = 4X^3 - g_2X - g_3 \)]

We denote the association:

\[
X = \wp(z), \quad Y = \wp'(z), \quad Z = 1
\]

is holomorphic for \( z \in \mathbb{C} \setminus \Lambda \) and gives a local holomorphic parameter of cubic curve \( C \). Therefore \( C \) is non-singular at these points. Around the point \((0 : 1 : 0) \in C \subset \mathbb{P}^2 \), since \( Y \neq 0 \), we have an affine equation

\[
\frac{Z}{Y} - 4\left(\frac{X}{Y}\right)^3 + g_2\frac{XZ}{Y^2} + g_3\left(\frac{Z}{Y}\right)^3 = 0
\]
The association
\[ \frac{X}{Y} = \frac{\wp(z)}{\wp'(z)} = -z^2 + \mathcal{O}(z^5), \quad \frac{Z}{Y} = \frac{1}{\wp'(z)} = -z^3 + \mathcal{O}(z^7) \]

shows that the curve \( C \) near \( (0:1:0) \) has a holomorphic parameter \( z \in \mathbb{C} \) defined near the origin. Thus the cubic curve \( C \) is non-singular everywhere.

As we proved in 5.7, the map \( \phi \) with \( z \mapsto (\wp(z) : \wp'(z) : 1) \) determines a bijection from \( E \) onto \( C \). To see this in another way, take a point \( (X:Y:Z) \) on \( C \):

- If this point is the point at infinity, then the above association shows that the map is bijective near \( z = 0 \) because the relation can still be solved for \( z = z(\frac{X}{Y}) \) which gives a holomorphic function in \( \frac{X}{Y} \).
- If the point \( (X:Y:Z) \) is not the point at infinity, then there are two points \( z \) and \( z' \) on \( E \) such that \( \wp(z) = \wp(z') = X/Z \).

In later case, since \( \wp \) is an even function, in fact we have \( z' = -z \). For \( z = -z \) as a point on \( E \) means \( 2z = 0 \). This happens when \( z \) is equal to one of the three half periods. Therefore for a given value of \( X/Z \) there are two points on \( C \), namely \( (X:Y:Z) \) and \( (X:-Y:Z) \), that have the same value of \( X/Z \). Hence, if
\[ (\wp(z) : \wp'(z) : 1) = (X:Y:Z) \]
then:
\[ (\wp(-z) : \wp'(-z) : 1) = (X:-Y:Z) \]

Therefore we have:
\[
\begin{array}{ccc}
E_{\omega_1,\omega_2} & \xrightarrow{\wp;\wp':1} & C \\
\text{bijection} & \subset & \mathbb{P}^2 \\
\| & \downarrow & \\
\mathbb{P}^1 & \xrightarrow{\wp} & \mathbb{P}^1
\end{array}
\]

Figure 5.2: The vertical arrows are 2:1 ramified coverings

Since the inverse image of the 2:1 holomorphic mapping \( \wp : E \to \mathbb{P}^1 \) is \( \pm z \), the map \( \wp \) induces a bijective map
\[ E/\{\pm 1\} \xrightarrow{\text{bijection}} \mathbb{P}^1 \]

The group \( \mathbb{Z}/2\mathbb{Z} \cong \{\pm 1\} \) acts on the elliptic curve \( E \) with exactly 4 points:
\[ 0, \frac{\omega_1}{2}, \frac{\omega_2}{2} \text{ and } \frac{\omega_1 + \omega_2}{2} \]

The quotient space \( E/\{\pm 1\} \) is not naturally Riemann surface. It is \( \mathbb{P}^1 \) with orbifold singularities at \( e_1, e_2, e_3 \) and \( \infty \).
Degeneration of Weierstrass Elliptic Function: The relation between the coefficients and the roots of the cubic polynomial:

\[ 4X^3 - g_2X - g_3 = 4(X - e_1)(X - e_2)(X - e_3) \]

with:

\[
\begin{align*}
0 &= e_1 + e_2 + e_3 \\
g_2 &= -4(e_1e_2 + e_2e_3 + e_3e_1), \\
g_3 &= 4e_1e_2e_3
\end{align*}
\]

The discriminant of this polynomial is defined by

\[ \Delta = (e_1 - e_2)^2(e_2 - e_3)^2(e_3 - e_1)^2 = \frac{1}{16}(g_2^2 - 27g_3^3) \]

We have seen that \( e_1, e_2, e_3 \) and \( \infty \) are the branched points of the double covering \( \wp : E \rightarrow \mathbb{P}^1 \).

When discriminant vanishes, these branched points are no longer separated, and the cubic curve:

\[ Y^2Z - 4X^3 + g_2XZ^2 + g_3Z^3 = 0 \]

becomes singular. \( \Delta \)

References


24