Elliptic Curves over $\mathbb{C}$

Hongxiang Zhao

Abstract

In this survey we discuss elliptic curves over $\mathbb{C}$. We first introduce the elliptic curve from the calculation of the arc length of ellipse, which is the history origin of elliptic curve. Then we introduce some general basics of elliptic curves. Finally, we prove equivalences of categories between elliptic curves over $\mathbb{C}$ and lattices. We admit some basic concepts in algebraic geometry covered in the first two chapters of [3].

Contents

1 From Ellipse to Elliptic Curve

1.1 Elliptic Functions

Given an ellipse $\frac{x^2}{a^2} + \frac{y^2}{b^2} = 1$ with $a \geqslant b > 0$. We want to know the arc length of it. Setting $x = a\sin t, y = b\cos t, k = \frac{\sqrt{a^2-b^2}}{a}$, we get the arc length of the ellipse:

$$L = 4a\int_0^{\frac{\pi}{2}} \sqrt{1 - k^2\sin^2 t}dt \tag{1}$$

Now set $u = \sin t$. Then (1) becomes

$$L = 4a\int_0^1 \frac{1-k^2u^2}{\sqrt{(1-u^2)(1-k^2u^2)}}du$$

which cannot be evaluated in terms of elementary functions. Legendre studied integrals of the form $\int R(t)/\sqrt{P(t)}dt$, where R is a rational function and P is a polynomial of degree 4, which is now called the elliptic integral. He showed that the integral can be reduced to three integrals:

$$\int_0^\Phi \frac{du}{\sqrt{(1-u^2)(1-k^2u^2)}} \quad \int_0^\Phi \frac{u^2du}{\sqrt{(1-u^2)(1-k^2u^2)}} \quad \int_0^\Phi \frac{du}{(1+nu^2)\sqrt{(1-u^2)(1-k^2u^2)}}$$

where $0 \leqslant \Phi \leqslant 1$ [1]. Note that when $k = 0$, the first integral is the case of circle and becomes the inverse of the sine function. Observing that, Abel suggested that the inverse of such integral may be more convenient to use, which we now call elliptic functions. Following Abel's idea, Jacobi found that the inverse of the first integral is doubly periodic after extended to $\mathbb{C}$, which is similar to sine function with one period 2π. Moreover, the only single-valued functions that is either analytic or meromorphic with two periods are elliptic functions [2]. Thus, we have the following definition:

Definition 1.1 (Elliptic Functions)**.** Let $\Lambda \subset \mathbb{C}$ be a lattice, that is, a discrete subgroup of $\mathbb{C}$ that contains a $\mathbb{R}$-basis for $\mathbb{C}$. 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.

Definition 1.2. The fundamental parallelogram for Λ is a set of the form

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

where $a \in \mathbb{C}$ and $\{\omega_1, \omega_2\}$ is a basis for Λ. It is clear that the natural map $D \to \mathbb{C}/\Lambda$ is bijective.

Proposition 1.3. *A holomorphic elliptic function is constant. Similarly, an elliptic function with no zeros is constant.*

Proof. Suppose $f(z) \in \mathbb{C}(\Lambda)$ is holomorphic. Let D be its fundamental parallelogram. Then $\sup_{z\in\mathbb{C}} |f(z)| = \sup_{z\in\bar{D}} |f(z)|$. Since f is continuous and $\bar{D}$ is compact, f is constant by Liouville's theorem. If f has no zero, then $1/f$ is a holomorphic elliptic function, so is constant. □

Theorem 1.4. *Let $f \in \mathbb{C}(\Lambda)$ be an elliptic function relative to Λ. Then*

1. $\sum_{w\in\mathbb{C}/\Lambda} res_w(f) = 0$.
2. $\sum_{w\in\mathbb{C}/\Lambda} ord_w(f) = 0$.

Proof. (a) By residue theorem,

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

The integral is zero since f is an elliptic function.

(b) Apply (a) to the elliptic function f'/f, we have $\sum_{w\in\mathbb{C}/\Lambda} \text{res}_w(f'/f) = 0$. The result follows from the fact that $\text{res}_w(f'/f) = \text{ord}_w(f)$.

□

Definition 1.5 (Order of an elliptic function)**.** Let $f \in \mathbb{C}(\Lambda)$. The order of f is the number of poles (counting with multiplicities) in a fundamental parallelogram.

1.2 The Weierstrass $\wp$-function

Now there is a non-obvious series [2]

$$\sum_{m=-\infty}^{\infty} (z + m\pi) = (\sin z)^{-2}$$

Since all trigonometry is based on the sine function, such series may behave as a basis of the subject. Thus, we define a similar function of double period:

Definition 1.6 (Weierstrass $\wp$-function)**.** Let $\Lambda \subset \mathbb{C}$ be a lattice. The Weierstrass $\wp$-function (relative to Λ) is defined by the series

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

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

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

Theorem 1.7. *Let $\Lambda \subset \mathbb{C}$ be a lattice.*

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

(b) The Weierstrass $\wp$-function converges absolutely and uniformly on every compact subset of $\mathbb{C}/\Lambda$. The series defined 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. See [3, Theorem VI.3.1]. □

Similar to trigonometry, where every function is a rational combination of sine and cosine, every elliptic function is a rational function of the Weierstrass $\wp$-function and its derivative.

Theorem 1.8. *Let $\Lambda \subset \mathbb{C}$ be a lattice. Then*

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

Proof. See [3, Theorem VI.3.2]. □

Proposition 1.9. *Let $\Lambda \subset \mathbb{C}$ be a lattice, $n_1, \cdots, n_r \in \mathbb{Z}$ and $z_1, \cdots, z_r \in \mathbb{C}$ satisfy $\sum n_i = 0$ and $\sum n_i z_i \in \Lambda$. Then there exists an elliptic function $f \in \mathbb{C}(\Lambda)$ such that div$(f) = \sum n_i(z_i)$.*

Proof. See [3, Proposition VI.3.4]. □

The following theorem gives rise to elliptic curves.

Theorem 1.10. *(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

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

Proof. (a) For all z with $|z| < |\omega|$,

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

Replace this into the original formula of $\wp(z)$. Note that $\wp(z)$ is even, terms with odd powers vanishes. Then we get the desired formula.

(b) By (a), we can write out the first few terms of various Laurent expansions near $z = 0$:

$$\wp'(z)^2 = 4z^{-6} - 24G_4z^{-2} - 80G_6 + \cdots$$
$$\wp(z)^3 = z^{-6} + 9G_4z^{-2} + 15G_6 + \cdots$$
$$\wp(z) = z^{-2} + 3G_4z^2 + \cdots$$

We find that

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

is holomorphic near $z = 0$ and $f(0) = 0$. Since f is an elliptic function, f is holomorphic on $\mathbb{C}$, so $f \equiv 0$ on $\mathbb{C}$ by Proposition 1.3.

□

Thus, given any $z \in \mathbb{C} \setminus \Lambda$, we get a corresponding point on the curve $y^2 = 4x^3 - g_2x - g_3$, where $g_2 := g_2(\Lambda) := 60G_4(\Lambda), g_3 := g_3(\Lambda) := 140G_6(\Lambda)$, by setting $(x, y) = \big(\wp(z), \wp'(z)\big)$. If $z = 0$, since the order of pole of $\wp'(z)$ at $z = 0$ is greater than $\wp(z)$, this induces a map $\phi\colon \mathbb{C}/\Lambda \to E(\mathbb{C})$, where $E(\mathbb{C})$ is a projective curve in $\mathbb{P}^2(\mathbb{C})$ defined by $y^2z = 4x^3 - g_2xz^2 - g_3z^3$, given by $z \to [\wp(z), \wp'(z), 1]$, where $0 \mapsto [0, 1, 0]$.

Remark. *Actually there is a heuristic way to get such ODE by viewing $\wp$ as the inverse of an elliptic integral. Extend $I(\Phi) = \int_O^\Phi \frac{du}{\sqrt{(1-u^2)(1-k^2u^2)}}$ to complex numbers and temporarily ignore that the square root is not well-defined on the whole complex plane. Let*

$$v^2 = (1-u^2)(1-k^2u^2) = (u-\alpha)(u-\beta)(u-\gamma)(u-\delta)$$

and $x = \frac{1}{u-\alpha}, y = \frac{v}{(u-\alpha)^2}$. Then we have $y^2 = x^3 + ax^2 + bx + c$ for some $a, b, c \in \mathbb{C}$ and $I(\Phi) = \int_O^\Phi \frac{dx}{\sqrt{x^3+ax^2+bx+c}}$. Recall that $\wp$ is originated from the inverse of such integral. In fact, it is the inverse of $I(\Phi) = \int_O^\Phi \frac{dx}{\sqrt{f(x)}}$ according to [1], where $f(x) = x^3 - g_2x - g_3$. Since $\wp \circ I(\Phi) = \Phi$, $\wp'\big(I(\Phi)\big) = \sqrt{f(\Phi)} = \sqrt{f\Big(\wp\big(I(\Phi)\big)\Big)}$. Denoting $z = I(\Phi)$ we get the ODE.

1.3 Weierstrass Equations

To generalize the equation given in the previous subsection to arbitrary field, we consider a projective curve in $\mathbb{P}^2$ given by an equation of the form:

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

Here $O = [0, 1, 0]$ is the base point and $a_1, \cdots, a_6 \in \bar{K}$. Such an equation is called a Weierstrass equation. Let $x = X/Z, y = Y/Z$. We get a curve

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

with a point $O = [0, 1, 0]$ at infinity. If $a_1, \cdots, a_6 \in K$, then E is said to be defined over K.

Definition 1.11 (Elliptic Curves)**.** An elliptic curve is a smooth projective curve in $\mathbb{P}^2$ given by a Weierstrass equation with a based point $O = [0, 1, 0]$.

If $\mathrm{char}(K) \neq 2$, then we can make a coordinate change $y \mapsto \frac{1}{2}(y - a_1x - a_3)$. Then the equation becomes the form satisfied by Weierstrass $\wp$-function:

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

where $b_2 = a_1^2 + 4a_2, b_4 = 2a_4 + a_1a_3, b_6 = a_3^2 + 4a_6$. We also define the following quantities for future uses:

Definition 1.12. The discriminant, the j-invariant and the invariant differential associated to the given Weierstrass equation are defined as:

$$\Delta := -b_2^2 b_8 - 8b_4^3 - 27b_6^2 + 9b_2 b_4 b_6$$

$$j := (b_2^2 - 24b_4)^3/\Delta$$

$$\omega := \frac{dx}{2y + a_1 x + a_3} = \frac{dy}{3x^2 + 2a_2 x + a_4 - a_1 y}$$

Proposition 1.13. *(a) The curve given by a Weierstrass equation is nonsingular if and only if* $\Delta \neq 0$.

(b) Two elliptic curves are isomorphic over $\bar{K}$ *if and only if they have the same* j*-invariant.*

(c) If $j_0 \in \bar{K}$*, then there exists an elliptic curve defined over* $K(j_0)$ *whose* j*-invariant is equal to* j_0.

(d) The invariant differential of an elliptic curve is holomorphic and nonvanishing.

Proof. See [3, Proposition III.1.4] and [3, Proposition III.1.5]. □

Since we are discussing curves over an algebraic field $\mathbb{C}$, the right-hand side of Weierstrass equations can be factored into linear terms.

Definition 1.14 (Legendre Form)**.** A Weierstrass equation is in the Legendre form if it can be written as

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

Proposition 1.15. *Suppose that* $char(K) \neq 2$*. Then 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 $\lambda \in \bar{K}$ *with* $\lambda \neq 0, 1$.

Proof. Suppose that an elliptic curve E is given by

$$E : y^2 = 4x^3 + b_2 x^2 + 2b_4 x + b_6$$

Replacing y by $2y$ and factoring the right-hand side, we get

$$E : y^2 = (x - e_1)(x - e_2)(x - e_3)$$

for some $e_1, e_2, e_3 \in \bar{K}$. Since $\Delta = 16(e_1 - e_2)^2(e_1 - e_3)^2(e_2 - e_3)^2 \neq 0$, e_1, e_2, e_3 are distinct. Now we substitute $x = (e_2 - e_1)x' + e_1$ and $y = (e_2 - e_1)^{\frac{3}{2}}y'$, we get

$$(e_2 - e_1)^3(y')^2 = (e_2 - e_1)^3 x'(x' - 1)(x' - \lambda)$$
$$(y')^2 = x'(x' - 1)(x' - \lambda)$$

which is the desired Legendre form with $\lambda = \frac{e_3 - e_1}{e_2 - e_1} \in \bar{K}$ and $\lambda \neq 0, 1$. □

2 Basics of Elliptic Curves

2.1 Elliptic Curves

Since the invariant differential ω of an elliptic curve is holomorphic and nonvanishing, so $0 = \mathrm{div}(\omega) = 2g - 2$ by Riemann-Roch Theorem, where g is the genus of the curve. Thus, $g = 1$. Conversely, we have that every smooth projective curve with genus one is given by a Weierstrass equation.

Proposition 2.1. *Let E be a smooth projective curve of genus one over K with a bases point $O \in E$.*

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

$$\Phi \colon E \to \mathbb{P}^1, \qquad \phi = [x, y, 1]$$

gives an isomorphism of E/K onto a curve given by a Weierstrass equation and $\phi(O) = [0, 1, 0]$. Moreover, $K(E) = K(x, y)$ and $[K(E) : K(x)] = 2$.

(b) Conversely, every smooth cubic curve given by a Weierstrass equation over K is a smooth projective curve with genus one over K with a base point $O = [0, 1, 0]$.

Proof. We have proved (b) in the above paragraph. For (a), see [3, Proposition III.3.1(a)]. □

Thus, we have an alternative definition of elliptic curve of genus one, which is a smooth projective curve with a based point.

In addition, we can see that there is a similarity between Proposition 2.1(a) and Theorem 1.8 and the map $\phi\colon \mathbb{C}/\Lambda \to E(\mathbb{C})$ given by $z \to [\wp(z), \wp'(z), 1]$. In fact, we can show that ϕ is a bijection. We postpone the proof to Section 3.

2.2 Group Law

Since we have a bijection $\phi\colon \mathbb{C}/\Lambda \to E(\mathbb{C})$ and $\mathbb{C}/\Lambda$ is a compact Lie group, we can give an abelian group structure on $E(\mathbb{C})$ via ϕ. Actually this group operation admits a geometry meaning on elliptic curves:

Given points P, Q on an elliptic curve E, let L be the line connecting P, Q (if $P = Q$, then let L to be the tangent line). By Bézout's theorem, L intersects E at another point R. Let L' be the line connecting R, O. Then define the addition of P, Q to be the third point of $E \cap L'$.

Proposition 2.2. *The operation defined above makes E an abelian group.*

Proof. See [3, Proposition III.2.2]. □

Remark. *In history, the group law rises independently on the correspondence of tori and elliptic curves. It is discovered by Newton during his investigation of cubic curves [2]. So it is kind of surprising that these two groups are isomorphic.*

Proposition 2.3. *Let (E, O) be an elliptic curve and $Pic^0(E)$ be its Picard group of degree 0. Then*

$$\kappa\colon E \to Pic^0(E) \qquad P \to [(P) - (O)] \tag{2}$$

$$\sigma\colon Pic^0(E) \to E \qquad [D] \to P \tag{3}$$

where P is the unique point such that $D - (P) + (O) = div(f)$ for some $f \in \bar{K}(E)$, are isomorphisms between abelian groups.

Proof. First we show that σ is well-defined. For any $D \in \mathrm{Div}^0(E)$, let

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

By Riemann-Roch Theorem, $\dim \mathcal{L}\big(D+(O)\big) = 1$. Thus, there is an $f \in \bar{K}(E)^*$ such that $\mathrm{div}(f) \geqslant -D-(O)$. Since $\deg \mathrm{div}(f) = 0$, there is $P \in E$ such that $\mathrm{div}(f) = -D+(P)-(O)$. If there are P, Q such that $(P)-(Q) = \mathrm{div}(f)$ for some $f \in \mathrm{K}(E)^*$, $P = Q$ because $\dim \mathcal{L}\big((Q)\big) = 1$ and f is constant by Riemann-Roch Theorem again. For any $D_1, D_2 \in \mathrm{Div}^0(E)$, let P_1, P_2 be points associated to D_1, D_2 respectively. If $D_1 - D_2 = \mathrm{div}(f)$ for some $f \in \bar{K}(E)$, $(P_1)-(P_2) = \mathrm{div}(g)$ for some $g \in \bar{K}(E)$. Thus, $P_1 = P_2$ by the same argument as above.

It is obvious that κ, σ are inverse of each other. It remains to show that κ is a homomorphism, i.e., $(P+Q)+(O)-(P)-(Q) = 0$ in $\mathrm{Pic}^0(E)$. Suppose f, f' denotes the lines connecting P, Q and $P+Q, O$ and R is the third point of both lines. Since the line $Z = 0$ intersects with E only at O with multiplicity 3, we have

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

Thus, $(P+Q)-(P)-(Q)+(O) = \mathrm{div}(f'/f)$. □

Corollary 2.4. *Let E be an elliptic curve and let $D = \sum n_P(P) \in Div(E)$. Then D is a principal divisor if and only if $\sum n_P = 0$ and $\sum n_P P = O$.*

Proof. First, every principal divisor has degree 0. Let $D \in \mathrm{Div}^0(E)$. Making use of the map σ in Proposition 2.3, we have

$$D = 0 \text{ in } \mathrm{Pic}^0(E) \Leftrightarrow \sigma(D) = O \Leftrightarrow \sum n_P \sigma\big((P)-(O)\big) = O \Leftrightarrow \sum n_P P = O$$

□

2.3 Isogenies

Since elliptic curves are abelian groups, it is natural to consider the homomorphisms between elliptic curves.

Definition 2.5 (Isogeny)**.** Let E_1, E_2 be elliptic curves. An isogeny from E_1 to E_2 is a morphism $\psi\colon E_1 \to E_2$ such that $\psi(O) = O$.

Proposition 2.6. *Isogenies are homomorphisms between abelian groups.*

Proof. Note that we have the following commutative diagram:

$$\begin{array}{ccc} E_1 & \xrightarrow{\kappa_1} & \mathrm{Pic}^0(E_1) \\ {\scriptstyle\psi}\downarrow & & \downarrow{\scriptstyle\psi_*} \\ E_2 & \xrightarrow[\kappa_2]{} & \mathrm{Pic}^0(E_2) \end{array} \qquad \begin{array}{ccc} P & \longmapsto & [(P)-(O)] \\ \downarrow & & \downarrow \\ \psi(P) & \longmapsto & [\big(\psi(P)\big)-(O)] \end{array}$$

Since κ_1, κ_2 are isomorphisms and $\kappa_1, \psi_*, \kappa_2$ are homomorphisms between abelian groups, ψ is also a homomorphism. □

3 Elliptic Curves over $\mathbb{C}$

Now we turn our attention back to elliptic curves over $\mathbb{C}$. We have constructed a map from a torus $\mathbb{C}/\Lambda$ to an elliptic curve in Section 1. There is a striking result that this is actually an analytic isomorphism of compact Lie groups.

Proposition 3.1. *Let Λ be a lattice of $\mathbb{C}$ and $g_2 = g_2(\Lambda), g_3 = g_3(\Lambda)$ be the quantities defined in Section 1, i.e., $g_2 = 60G_4(\Lambda), g_3 = 140G_6(\Lambda)$.*

(a) The polynomial $4x^3 - g_2x - g_3$ has distinct roots.

(b) Let $E/\mathbb{C}$ be the curve $E : y^2 = 4x^3 - g_2x - g_3$, which is an elliptic curve by (a). Then the map $\phi\colon \mathbb{C}/\Lambda \to E(\mathbb{C}) \subset \mathbb{P}^2(\mathbb{C})$ given by $z \mapsto [\wp(z), \wp'(z), 1]$ is a complex analytic isomorphism of complex Lie groups.

Proof. (a) Suppose ω_1, ω_2 are basis of Λ. Let $\omega_3 = \omega_1 + \omega_2$. Since $\wp'$ is an odd elliptic function, for each i we have $\wp'\big(\frac{\omega_i}{2}\big) = -\wp'\big(-\frac{\omega_i}{2}\big) = \wp'\big(\frac{\omega_i}{2}\big)$. Thus, $\wp'\big(\frac{\omega_i}{2}\big) = 0$ for each i, implying that $f(x) = 4x^3 - g_2x - g_3$ vanishes at $\wp\big(\frac{\omega_i}{2}\big)$. It remains to show that these points are distinct.

Note that $\wp(z) - \wp\big(\frac{\omega_i}{2}\big)$ is an elliptic function with at least a double zero at $\frac{\omega_i}{2}$. Since $\wp(z) - \wp\big(\frac{\omega_i}{2}\big)$ has order 2 by Laurent series, these are exactly all the zeros by Theorem 1.4. Thus, $\wp\big(\frac{\omega_i}{2}\big) \neq \wp\big(\frac{\omega_i}{2}\big)$.

(b) To see that ϕ is surjective, first $\phi(0) = [0, 1, 0]$. For any $(x, y) \in E(\mathbb{C})$, $\wp(z) - x$ is a nonconstant elliptic function. Thus, by Proposition 1.3, it has a zero, say, $z = a$. Then $x = \wp(a)$. Thus, $y^2 = \wp'(a)^2$. By replacing a by $-a$ if necessary, we have $\wp'(a) = u$.

If $\phi(z_1) = \phi(z_2)$. Assume first that $2z_1 \notin \Lambda$. Then $\wp(z) - \wp(z_1)$ has at least two zeros at $z = \pm z_1$. Since it has order 2, these are exactly all the zeros. Thus, $z_2 \equiv \pm z_1 \pmod{\Lambda}$. Since $\wp'(z_1) = \wp'(z_2)$, the only possibility is that $z_1 = z_2$. Now if $2z_1 \in \Lambda$, similarly z_1 is the only zero of $\wp(z) - \wp(z_1)$ and z_1 is a double zero. Thus, $z_1 = z_2$. Hence, ϕ is a bijection.

We show that ϕ is analytic by considering its effect on cotangent space. Note that $\phi^*\left(\frac{dx}{y}\right) = \frac{d\wp(z)}{\wp'(z)} = dz$ and both $\frac{dx}{y}, dz$ are holomorphic and nonvanishing, so ϕ is a local analytic isomorphism. Since ϕ is bijection, ϕ is a global analytic isomorphism.

Finally, we show that ϕ is a homomorphism. For any $z_1, z_2 \in \mathbb{C}$, let $f \in \mathbb{C}(\Lambda)$ with divisor $\operatorname{div}(f) = (z_1 + z_2) - (z_1) - (z_2) + (0)$ by Proposition 1.9. Let $F = f \circ \phi^{-1}$. By Theorem 1.8, f is a rational function of $\wp(z), \wp'(z)$. Thus, F can be viewed as a function in $\mathbb{C}(x, y) = \mathbb{C}(E)$. Then $\operatorname{div}(F) = \big(\phi(z_1+z_2)\big) - \big(\phi(z_1)\big) - \big(\phi(z_2)\big) + (O)$. By Corollary 2.4, $\phi(z_1 + z_2) = \phi(z_1) + \phi(z_2)$ in E.

□

In fact, there are bijections of morphisms between tori, lattices and elliptic curves.

Theorem 3.2. *Let Λ_1, Λ_2 be two lattices in $\mathbb{C}$ and suppose $\alpha \in \mathbb{C}$ such that $\alpha\Lambda_1 \subset \Lambda_2$. Then scalar multiplication by α induces a well-defined holomorphic homomorphism $\psi_\alpha \colon \mathbb{C}/\Lambda_1 \to \mathbb{C}/\Lambda_2$ given by $\psi_\alpha(z) = \alpha z \pmod{\Lambda_2}$. Then we have*

(a) The map $\{\alpha \in \mathbb{C} : \alpha\Lambda_1 \subset \Lambda_2\} \to \{$holomorphic $\psi \colon \mathbb{C}/\Lambda_1 \to \mathbb{C}/\Lambda_2$ with $\psi(0) = 0\}$ given by $\alpha \mapsto \psi_\alpha$ is a bijection.

(b) Let E_1, E_2 be elliptic curves associated to lattices Λ_1, Λ_2 respectively. Then the map $\{$isogenies $\psi \colon E_1 \to E_2\} \to \{$holomorphic $\psi \colon \mathbb{C}/\Lambda_1 \to \mathbb{C}/\Lambda_2$ with $\psi(0) = 0\}$ given by $\psi \mapsto \phi_2^{-1} \circ \psi \circ \phi_1$ is a bijection, where ϕ_1, ϕ_2 are maps given in Proposition 3.1 corresponding to Λ_1, Λ_2 respectively.

Proof. (a) If $\psi_\alpha = \psi_\beta$ for some α, β, then $\alpha z \equiv \beta z \pmod{\Lambda_2}$ for all z. Thus, the map $z \mapsto (\alpha - \beta)z$ has image in Λ_2. Since Λ_2 is discrete, the map is constant, so $\alpha = \beta$.

Now for any holomorphic $\psi \colon \mathbb{C}/\Lambda_1 \to \mathbb{C}/\Lambda_2$ with $\psi(0) = 0$. Since $\mathbb{C}$ is simply connected, we can lift ψ to $f \colon \mathbb{C} \to \mathbb{C}$ with $f(0) = 0$. Then for any $\omega \in \Lambda_1, z \in \mathbb{C}$, $f(z + \omega) \equiv f(z) \pmod{\Lambda_2}$. Thus, $f(z + \omega) - f(z) \in \pmod{\Lambda_2}$. Similarly,

$f(z+\omega)-f(z)$ is constant. Thus, $f'(z+\omega)=f'(z)$ for all $z\in\mathbb{C},\omega\in\Lambda_1$. Therefore, f' is a holomorphic elliptic function. Thus, f' is constant by Proposition 1.3. Thus, $f(z)=\alpha z+\gamma$ for some $\alpha,\gamma\in\mathbb{C}$. Since $f(0)=0$, $\gamma=0$. Therefore, $f(z)=\alpha z$ and $\alpha\Lambda_1\subset\Lambda_2$, so $\psi=\psi_\alpha$.

(b) Since isogenies are locally rational functions, isogenies are analytic. Thus, the map is well-defined and injective.

To prove the surjectivity, it suffices to prove for ϕ_α by (a), where $\alpha\Lambda_1\subset\Lambda_2$. Then the map we expect between E_1,E_2 is given by

$$[\wp(z;\Lambda_1),\wp'(z;\Lambda_1),1]\mapsto[\wp(\alpha z;\Lambda_2),\wp'(\alpha z;\Lambda_2),1]$$

It remains to show that $\wp(\alpha z;\Lambda_2),\wp'(\alpha z;\Lambda_2)$ can be expressed as rational expressions in $\wp(z;\Lambda_1),\wp'(z;\Lambda_1)$, so it remains to show that $\wp(\alpha z;\Lambda_2),\wp'(\alpha z;\Lambda_2)$ are elliptic functions with respect to Λ_1 by Theorem 1.8. Then it follows from the fact that $\alpha\Lambda_1\subset\Lambda_2$.

□

Conversely, we claim that every elliptic curve is parametrized by some elliptic function as shown in Proposition 3.1. The existence of such lattice requires some techniques from other fields.

Theorem 3.3 (Uniformization Theorem)**.** *Let $A,B\in\mathbb{C}$ be complex numbers satisfies $4A^3-27B^2\neq0$. Then there exists a unique lattice $\Lambda\subset\mathbb{C}$ satisfying $g_2(\Lambda)=A$ and $g_3(\Lambda)=B$.*

Proof. The proof uses techniques from other fields. See [3, Theorem VI.5.1]. □

Definition 3.4 (Homothety)**.** Two lattices Λ_1,Λ_2 are said to be homothetic if there is $\alpha\in\mathbb{C}^*$ such that $\alpha\Lambda_1\subset\Lambda_2$.

Corollary 3.5. *Let $E/\mathbb{C}$ be an elliptic curve. There exists a lattice $\Lambda\subset\mathbb{C}$, unique up to homothety, and a complex analytic isomorphism of complex Lie groups: $\phi\colon\mathbb{C}/\Lambda\to E(\mathbb{C})$ given by $z\mapsto[\wp(z),\wp'(z),1]$.*

Proof. Existence is Proposition 3.1 and Theorem 3.3. Uniqueness is Theorem 3.2(a). □

Now we can give the inverse function of ϕ in Proposition 3.1. Heuristically, recall $\wp\colon\mathbb{C}\to\mathbb{P}^1$ is defined as the inverse function of an elliptic integral, which is $\int_0^z\frac{dx}{\sqrt{x^3-g_2x-g_3}}$. However,

the square root is not well-defined on the whole $\mathbb{P}^1$ space. Thus, we have to make branch cuts on it. By making some coordinate changes, we may assume that an elliptic curve is given in Legendre form $y^2 = x(x-1)(x-\lambda)$ and the Weierstrass $\wp$-function is the inverse function of $\int_0^z \frac{dx}{\sqrt{x(x-1)(x-\lambda)}}$ with $\lambda \notin \mathbb{R}_{\leqslant 0}$. Let

$$B := (\mathbb{R}_{\leqslant 0} \cup \infty) \cup L$$

where L is the straight line connecting $1, \lambda$ in $\mathbb{C}$. Then $\sqrt{x}$, $\sqrt{\frac{x-1}{x-\lambda}}$ are well-defined on $\mathbb{P}^1 \setminus B$. Thus, $\sqrt{x(x-1)(x-\lambda)}$ is well-defined on $\mathbb{P}^1 \setminus B$. Hence, we obtain a map $\mathbb{P}^1 \setminus B \to \mathbb{C}$. Note that there is a projection $\pi\colon E(\mathbb{C}) \to \mathbb{P}^1$ given by $(x, y) \to x$, which is a double cover ramifying at $0, 1, \lambda, \infty$. Thus, we get a composition

$$E(\mathbb{C}) \setminus \pi^{-1}(B) \xrightarrow{\pi} \mathbb{P}^1 \setminus B \xrightarrow{\text{“}\wp^{-1}\text{”}} \mathbb{C} \longrightarrow \mathbb{C}/\Lambda$$

$$(x, y) \longmapsto x \longmapsto \int_0^x \frac{d\tilde{x}}{\sqrt{\tilde{x}(\tilde{x}-1)(\tilde{x}-\lambda)}} \longmapsto [\int_0^x \frac{d\tilde{x}}{\sqrt{\tilde{x}(\tilde{x}-1)(\tilde{x}-\lambda)}}]$$

Note that $E(\mathbb{C}) \setminus \pi^{-1}(B) \cong (\mathbb{P}^1 \setminus B) \sqcup (\mathbb{P}^1 \setminus B)$ and $y^2 = x(x-1)(x-\lambda)$ on $E(\mathbb{C})$. Thus, we can lift the path integral from 0 to x in $\mathbb{P}^1 \setminus B$ to a path O to $P = (x, y)$. Now we see that it is natural to consider the map $E(\mathbb{C}) \to \mathbb{C}/\Lambda$ given by $P \mapsto \int_O^P \frac{dx}{y}$, and it turns out to be the desired inverse of ϕ in Proposition 3.1.

Proposition 3.6. *Let $E/\mathbb{C}$ be an elliptic curve with Weierstrass coordinate functions x, y.*

(a) Let α, β be closed paths on $E(\mathbb{C})$ giving a basis for $H_1(E; \mathbb{Z})$. Then the periods

$$\omega_1 = \int_\alpha \frac{dx}{y} \qquad \omega_2 = \int_\beta \frac{dx}{y}$$

are $\mathbb{R}$-linearly independent.

(b) Let Λ be the lattice generated by ω_1, ω_2. Then the map $\psi\colon E(\mathbb{C}) \to \mathbb{C}/\Lambda$ given by $P \mapsto \int_O^P \frac{dx}{y}$ is a complex analytic isomorphism of Lie groups. It is the inverse of the map ϕ given in Proposition 3.1.

Proof. (a) By Corollary 3.5 there is a lattice Λ and a map $\phi\colon \mathbb{C}/\Lambda \to E(\mathbb{C})$ given by $z \mapsto [\wp(z), \wp'(z), 1]$, which is an analytic isomorphism of compact Lie groups. Pulling back α, β, we have $\omega_1 = \int_{\phi^{-1}\circ\alpha} \frac{d\phi^*(x)}{\phi^*(y)} = \int_{\phi^{-1}\circ\alpha} dz$ and similarly $\omega_2 = \int_{\phi^{-1}\circ\beta} dz$. Since α, β

are basis of $H_1(E;\mathbb{Z})$, $\phi^{-1}\circ\alpha, \phi^{-1}\circ\beta$ are basis of $H_1(\mathbb{C}/\Lambda;\mathbb{Z})$. Note that $H_1(\mathbb{C}/\Lambda;\mathbb{Z})$ is naturally isomorphic to Λ via the map $\gamma \to \int_\gamma dz$. Thus, ω_1, ω_2 is a basis of Λ, which is $\mathbb{R}$-linearly independent.

(b) Since $F^*(dz) = d(z\circ F) = \frac{dx}{y}$ and $\phi^{-1}\left(\frac{dx}{y}\right) = dz$, $(F\circ\phi)^*(dz) = dz$. Since $F\circ\phi$ is an endomorphism of $\mathbb{C}/\Lambda$, $F\circ\phi = \psi_\alpha$ for some $\alpha \in \mathbb{C}^*$ by Theorem 3.2(a). Thus, $dz = (F\circ\phi)^*(dz) = \alpha dz$ implies that $\alpha = 1$. Thus, $F = \phi^{-1}$.

□

To sum up, we have the following equivalences of categories:

Theorem 3.7. *The following categories are equivalent:*

(a) Elliptic curves over $\mathbb{C}$ with isogenies.

(b) Tori $\mathbb{C}/\Lambda$ with complex analytic maps taking O to O.

(c) Lattices $\Lambda \subset \mathbb{C}$, up to homothety with Map$(\Lambda_1, \Lambda_2) = \{\alpha \in \mathbb{C}^* : \alpha\Lambda_1 \subset \Lambda_2\}$.

Proof. Equivalences of objects are given by Proposition 3.1(b), Corollary 3.5 and Proposition 3.6. Equivalences of maps is Theorem 3.2. □

Proposition 3.8. *Let $E/\mathbb{C}$ be an elliptic curve and fix a lattice Λ and an isomorphism $E(\mathbb{C}) \cong \mathbb{C}/\Lambda$.*

(a) There is a natural isomorphism $H_1(E;\mathbb{Z}) \to \Lambda$ given by $\gamma \to \int_\gamma dz$.

(b) There is a natural isomorphism $H_1(E;\mathbb{Z}/m\mathbb{Z}) \to E[m]$, where $E[m] = \ker[m]$ and $[m]$ is the endomorphism of E by multiplication of an integer m.

(c) For any prime l, there is a natural isomorphism $H_1(E;\mathbb{Z}_l) \to \lim E[l^n] =: T_l(E)$, which is the Tate module.

Proof. (a) We have proved this in Proposition 3.6.

(b) We have

$$H_1(E;\mathbb{Z}/m\mathbb{Z}) \cong H_1(E;\mathbb{Z}) \otimes \mathbb{Z}/m\mathbb{Z} \cong \Lambda \otimes \mathbb{Z}/m\mathbb{Z} \cong \Lambda/m\Lambda \cong E[m]$$

(c) By taking limits in (b).

□

References

[1] Jose Barrios. A brief history of elliptic integral addition theorems. https://scholar.rose-hulman.edu/cgi/viewcontent.cgi?article=1148&context=rhumj, 2009. 1.1, 1.2

[2] Adrian Rice and Ezra Brown. Why ellipses are not elliptic curves. *Mathematics magazine*, 85(3):163–176, 2012. 1.1, 1.2, 2.2

[3] Joseph H. Silverman. *The Arithmetic of Elliptic Curves*. Graduate Texts in Mathematics, 106. Springer New York, 2nd ed. 2009. edition, 2009. (document), 1.7, 1.8, 1.9, 1.13, 2.1, 2.2, 3.3