A Brief Introduction to Elliptic Curves and Modular Curves

November 23, 2022

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 $0 \leqslant \Phi \leqslant 1$ [3]. 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 meromorphic single-valued functions with two periods are elliptic functions [3]. 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.

Now we need some properties of elliptic functions for further uses.

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.

Theorem 1.3. *Let $f \in \mathbb{C}(\Lambda)$ be an elliptic function relative to a lattice Λ. Let D be a fundamental parallelogram for Λ such that f has no zeros or poles on ∂D. Then*

(a) $\sum_{\omega \in D} \mathit{res}_\omega(f) = 0.$

(b) $\sum_{\omega \in D} \mathit{ord}_\omega(f) = 0.$

(c) $\sum_{\omega \in D} \mathit{ord}_\omega(f)\omega \in \Lambda.$

Proof. (a) By the residue theorem and the periodicity of f, we have

$$\sum_{\omega \in D} \mathrm{res}_\omega(f) = \frac{1}{2\pi i} \int_{\partial D} f(z)dz = 0$$

(b) Since f is periodic, f' is also periodic. By the argument principle,

$$\sum_{\omega \in D} \mathrm{ord}_\omega(f) = \int_{\partial D} \frac{f'(z)}{f(z)} dz = \sum_{\omega \in D} \mathrm{res}_\omega(f'/f) = 0$$

(c) By residue theorem,

$$\begin{aligned}\sum_{\omega \in D} \mathrm{ord}_\omega(f)\omega &= \frac{1}{2\pi i} \int_{\partial D} \frac{zf'(z)}{f(z)} dz \\ &= \frac{1}{2\pi i} \left(\int_a^{a+\omega_1} + \int_{a+\omega_1}^{a+\omega_1+\omega_2} + \int_{a+\omega_1+\omega_2}^{a+\omega_2} + \int_{a+\omega_2}^{a} \right) \frac{zf'(z)}{f(z)} dz\end{aligned}$$

By change of variable and the periodicity of f,

$$\sum_{\omega \in D} \mathrm{ord}_\omega(f)\omega = -\frac{\omega_2}{2\pi i} \int_a^{a+\omega_1} \frac{f'(z)}{f(z)} dz + \frac{\omega_1}{2\pi i} \int_a^{a+\omega_2} \frac{f'(z)}{f(z)} dz$$

Note that for any meromorphic function $g(z)$ with $g(a) = g(b)$, $\frac{1}{2\pi i} \int_a^b \frac{g'(z)}{g(z)} dz$ is the winding number around 0 of the path

$$[0,1] \to \mathbb{C}, \quad t \mapsto g\big((1-t)a + tb\big)$$

which is an integer. Thus, $\sum_{\omega \in D} \mathrm{ord}_\omega(f)\omega \in \Lambda$.

□

1.2 Weierstrass Equations

Given a lattice Λ on $\mathbb{C}$, we have the Weierstrass $\wp$-function and the Eisenstein series

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

We know that the Weierstrass $\wp$-function satisfies the ODE:

$$\big(\wp'(z)\big)^2 = 4\wp(z)^3 - g_2\wp(z) - g_3$$

where $g_2 = g_2(\Lambda) = 60G_4(\Lambda)$ and $g_3 = g_3(\Lambda) = 140G_6(\Lambda)$. Thus, given any $z \in \mathbb{C}\setminus\Lambda$, we get a corresponding point on the curve $y^2 = 4x^3 - g_2x - g_3$ 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

$$\begin{aligned} \phi\colon \mathbb{C}/\Lambda &\to E(\mathbb{C}) \\ z &\to [\wp(z), \wp'(z), 1],\ z \neq 0 \\ 0 &\mapsto [0, 1, 0] \end{aligned} \tag{2}$$

where $E(\mathbb{C})$ is a projective curve in $\mathbb{P}^2(\mathbb{C})$ defined by $y^2z = 4x^3 - g_2xz^2 - g_3z^3$.

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.

To generalize the equation given in the previous subsection to arbitrary field K, we consider a projective curve in $\mathbb{P}^2$ over K 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 1.4 (Elliptic Curves)**.** An elliptic curve E is a smooth projective curve in $\mathbb{P}^2$ given by a Weierstrass equation with a based point $O = [0,1,0]$.

By smooth we mean that for a Weierstrass equation $f(X,Y,Z)$, the matrix

$$\left(\frac{\partial f}{\partial X}(P), \frac{\partial f}{\partial Y}(P), \frac{\partial f}{\partial Z}(P)\right)$$

is nonzero for every $P \in E$.

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

Definition 1.5. The discriminant, the j-invariant and the invariant differential associated to the given Weierstrass equation are defined as:

$$\Delta := -b_2^2(b_2b_6 - b_4^2) - 8b_4^3 - 27b_6^2 + 9b_2b_4b_6$$
$$j := (b_2^2 - 24b_4)^3/\Delta$$

Note that when $b_2 = 0, b_4 = -\frac{1}{2}g_2, b_6 = -g_3$, $\Delta = g_2^3 - 27g_3^2$ and $j = \frac{(12g_2)^3}{\Delta}$ are in accord with the ones given by modular forms. Then we have the following statements similar to the case when $K = \mathbb{C}$.

Proposition 1.6. *(a) The curve given by a Weierstrass equation is smooth 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*.*

Proof. See [4, Proposition III.1.4]. □

2 Group Laws on Elliptic Curves

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:

Theorem 2.1 (Bézout's Theorem)**.** *Let* C, C' *be two distinct curves in* $\mathbb{P}^2$ *with degree* m, n *respectively. Assume that* C, C' *have no common component. Then* C *intersects* C' *at exactly* mn *points, counting with multiplicity.*

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, the tangent line at O is $Z = 0$). 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 with the identity* O*.*

Proof. The only non-trivial part is the associativity. For the proof of the associativity, one way is to deduce the explicit formula of the addition and then verify by direct calculation. For the explicit formula, see [4, Section III.2]. The second way is to prove that the elliptic curve is isomorphic to its Picard group as sets by $P \mapsto (P) - (O)$ and satisfying $(P + Q) + (O) = (P) + (Q)$ in the Picard group. Then we can conclude by the associativity of the Picard group. For details, see [4, Proposition III.3.4]. The method we use here is a more geometric one. We first need a lemma in algebraic geometry.

Lemma 2.3. *Let* C *be an irreducible cubic smooth curve in* $\mathbb{P}^2$*. Let* C', C'' *be two cubic curves in* $\mathbb{P}^2$*. Suppose* $C' \cap C$ *and* $C'' \cap C$ *agree on eight points. Then they will agree on the remaining point.*

Proof. See [2, Chapter 5, Proposition 3]. □

Suppose $P, Q, R \in E$. Suppose L_1 is the line connecting P, Q and intersecting with E at another point S', M_1 is the line connecting S, S', O, L_2 is the line connecting S, R and intersecting with E at another point T. Then $T = (P + Q) + R$.

On the other hand, suppose M_2 is the line connecting Q, R and intersecting with E at another point U', L_3 is the line connecting $U, U\prime, O$, M_3 is the line connecting P, U and intersecting with E at another point T'. Then $T' = P + (Q + R)$.

Let $C' = L_1L_2L_3$ and $C'' = M_1M_2M_3$, where $L_1L_2L_3, M_1M_2, M_3$ denotes the curve given by the multiplication of the formulas of the three lines. Then we conclude by the lemma above. □

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 [3]. So it is kind of surprising that these two groups are isomorphic.*

Definition 2.4 (Isogeny)**.** For two elliptic curves E_1, E_2, isogenies are group homomorphisms between E_1, E_2.

Theorem 2.5. *The map*

$$\begin{aligned} \phi\colon \mathbb{C}/\Lambda &\to E(\mathbb{C}) \\ z &\to [\wp(z), \wp'(z), 1],\ z \neq 0 \\ 0 &\mapsto [0, 1, 0] \end{aligned} \tag{3}$$

is a group isomorphism.

Proof. Pick any $z_1, z_2 \in \mathbb{C}/\Lambda$.

If z_1 or z_2 is 0 in $\mathbb{C}/\Lambda$, the case is trivial since $[0, 1, 0]$ is the identity element in $E(\mathbb{C})$.

If $z_1, z_2 \neq 0$ and $z_1 + z_2 = 0$, note that the line connecting $[x_0 : y_0 : 1]$ and $[0 : 1 : 0]$ in $\mathbb{P}^2$ is $x - x_0z = 0$, intersecting with E at $[x_0 : -y_0 : 1]$, so in $E(\mathbb{C})$

$$\begin{aligned} [\wp(z_1) : \wp'(z_1) : 1] + [\wp(z_2) : \wp'(z_2) : 1] &= [\wp(z_1) : \wp'(z_1) : 1] + [\wp(z_1) : -\wp'(z_1) : 1] \\ &= [0 : 1 : 0] = \phi(z_1 + z_2) \end{aligned}$$

If $z_1, z_2 \neq 0$ and $z_1 + z_2 \neq 0$, we are going to show that in $E(\mathbb{C})$,

$$[\wp(z_1) : \wp'(z_1) : 1] + [\wp(z_2) : \wp'(z_2) : 1] = [\wp(z_1 + z_2) : \wp'(z_1 + z_2) : 1]$$

Thus, we are going to prove that $\big(\wp(z_1), \wp'(z_1)\big), \big(\wp(z_2), \wp'(z_2)\big), \big(\wp(-z_1-z_2), \wp'(-z_1-z_2)\big)$ lie on a line in $\mathbb{C}^2$. Let $ax+by+c$ be the line in $\mathbb{C}^2$ connecting $\big(\wp(z_1), \wp'(z_1)\big), \big(\wp(z_2), \wp'(z_2)\big)$. If $z_1 \neq z_2$, the elliptic function $f = a\wp(z) + b\wp'(z) + c$ has two distinct zeros z_1, z_2. Since f is dominant by $\wp'$, f has three poles in some fundamental parallelogram. By Theorem 1.3(b), f has three zeros in the same fundamental parallelogram. By Theorem 1.3(c), the third zero of f is $-z_1 - z_2$ modulo Λ. If $z_1 = z_2$, we need to show that f has a double zero on z_1. Suppose the three zeros of f are z_1, z_3, z_4. Since $z_1 + z_2 \neq 0$, $b \neq 0$. Since $ax+by+c$ is the tangent line at $\wp(z_1)$, $\wp(z_1)$ is at least a double zero of $4x^3 + g_2x + g_3 - (\frac{ax+c}{b})^2 = 4(x-x_1)(x-x_2)(x-x_3)$. We may assume that $x_1 = x_2 = \wp(z_1)$. Then z_1 is at least a double zero of the elliptic function $4(\wp(z) - \wp(z_1))^2(\wp(z) - x_3)$. Note that the six zeros of $4(\wp(z) - \wp(z_1))^2(\wp(z) - x_3)$ are $\pm z_1, \pm z_3, \pm z_4$. Since $z_1 \neq -z_1$, we may assume $z_1 = \pm z_3$. If $z_1 = -z_3$, $\wp'(z_1) = 0$. Let $\omega_3 = \omega_1 + \omega_2$. Then for each i,

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

Note that $\wp(z) - \wp(\omega_i/2)$ is an elliptic curve with double zero on $\omega_i/2$, so $\omega_1/2, \omega_2/2, \omega_3/2$ are distinct in $\mathbb{C}/\Lambda$. Thus, $\omega_1/2, \omega_2/2, \omega_3/2$ are the three zeros of $\wp'$, contradicting to $2z_1 \neq 0$ in $\mathbb{C}/\lambda$, so $z_1 = z_3$. □

3 Elliptic Curves over $\mathbb{C}$

3.1 Complex Multiplication

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

Theorem 3.1. *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 2 corresponding to Λ_1, Λ_2 respectively.

Proof. See [4, Theorem III.4.1]. The proof depends on some properties of Riemann surfaces, $\wp$-fucntions and isogenies not mentioned in this note. □

Definition 3.2 (Order)**.** Let L be a number field, i.e. a finite extension over $\mathbb{Q}$. An order $\mathcal{O}$ of L is a subring of L that is a finitely generated abelian group and satisfies $\mathcal{O} \otimes \mathbb{Q} = L$.

Theorem 3.3. *Let $E/\mathbb{C}$ be an elliptic curve, and let ω_1, ω_2 be generators for the lattice Λ associated to E. Then one of the following is true:*

(i) End$(E) = \mathbb{Z}$.

(ii) The field $\mathbb{Q}(\omega_1/\omega_2)$ is an imaginary quadratic extension of $\mathbb{Q}$, and End(E) is isomorphic to an order in $\mathbb{Q}(\omega_1/\omega_2)$.

Proof. Let $\mathcal{O} = \{\alpha \in \mathbb{C} \colon \alpha\Lambda \subset \Lambda\}$. By Theorem 3.1, we know that $\operatorname{End}(E) = \mathcal{O}$. Let $\tau = \frac{\omega_1}{\omega_2}$. Since Λ is homothetic to $\mathbb{Z} + \mathbb{Z}\tau$, we may assume that $\Lambda = \mathbb{Z} + \mathbb{Z}\tau$. For any $\alpha \in \mathcal{O}$, we have

$$\alpha = a + b\tau \qquad \alpha\tau = c + d\tau$$

for some $a, b, c, d \in \mathbb{Z}$, so $\mathbb{Z} \subset \mathcal{O} \subset \mathbb{Z} + \mathbb{Z}\tau \subset \mathbb{Q}(\tau)$. Thus, $\mathcal{O}$ is a finitely generated abelian group.

If $\mathcal{O} \neq \mathbb{Z}$, pick $\alpha \in \mathcal{O} - \mathbb{Z}$, then $b \neq 0$. By eliminating α, we get

$$b\tau^2 + (a - d)\tau - c = 0$$

Since $\tau \notin \mathbb{R}$, $\mathbb{Q}(\tau)/\mathbb{Q}$ is an imaginary quadratic extension. Since $b\tau \in \mathcal{O}$, $\mathcal{O} \otimes \mathbb{Q} = \mathbb{Q}(\tau)$. Therefore, $\mathcal{O}$ is an order in $\mathbb{Q}(\tau)$. □

Definition 3.4 (Complex Multiplication)**.** Let E/K be an elliptic curve. Then we say that E has complex multiplication if $\operatorname{End}(E) \neq \mathbb{Z}$.

3.2 The Inverse Map from Elliptic Curve to Tori

In this section we discuss the inverse map of 2. This section may be skipped due to time limit.

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

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

Proposition 3.6. *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

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

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

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

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

Now we can give the inverse function of ϕ in 2. Heuristically, recall $\wp\colon \mathbb{C} \to \mathbb{P}^1$ is defined as the inverse function of an elliptic integral, which is $\int_0^z \frac{dx}{\sqrt{4x^3-g_2x-g_3}}$. 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

$$\begin{tikzcd}
E(\mathbb{C}) \setminus \pi^{-1}(B) \arrow[r, "\pi"] & \mathbb{P}^1 \setminus B \arrow[r, "``\wp^{-1}\text{''}"] & \mathbb{C} \arrow[r] & \mathbb{C}/\Lambda \\
(x, y) \arrow[r, mapsto] & x \arrow[r, mapsto] & \int_0^x \frac{d\tilde{x}}{\sqrt{\tilde{x}(\tilde{x}-1)(\tilde{x}-\lambda)}} \arrow[r, mapsto] & \left[\int_0^x \frac{d\tilde{x}}{\sqrt{\tilde{x}(\tilde{x}-1)(\tilde{x}-\lambda)}}\right]
\end{tikzcd}$$

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 2.

Proposition 3.7. *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 2.

Proof. (a) By surjectivity of the j-function 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 3.1. Thus, $dz = (F \circ \phi)^*(dz) = \alpha dz$ implies that $\alpha = 1$. Thus, $F = \phi^{-1}$.

□

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. 1.2

[2] William Fulton. Algebraic curves. http://www.math.lsa.umich.edu/~wfulton/CurveBook.pdf, 2008. 2.3

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

[4] Joseph H. Silverman. *The Arithmetic of Elliptic Curves*. Graduate Texts in Mathematics, 106. Springer New York, 2nd ed. 2009. edition, 2009. 1.6, 2.2, 3.1