Notes on Elliptic Curves

1 Elliptic Curves

Definition 1.1. An **elliptic curve** is a pair (E, P), where E is a smooth projective curve of genus one over an algebraically closed field k, and $P \in E(k)$ is a fixed k-rational point, called the basepoint.

Proposition 1.2. *Let (E, P) be an elliptic curve. There exist functions $x, y \in k(E)$ such that the map $\phi : E \to \mathbb{P}^2$ given by*

$$a \mapsto \begin{cases} [x(a) : y(a) : 1], & \text{if } a \neq P \\ [0 : 1 : 0], & \text{if } a = P \end{cases}$$

*is an isomorphism of E onto a curve given by a **Weierstrass equation**:*

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6, \quad a_i \in k.$$

Proof (idea). By the Riemann-Roch theorem, for $n \geq 1$, we have $\dim L(nP) = n$. We look at $L(nP)$ for increasing n.

- $L(P)$: basis $\{1\}$.
- $L(2P)$: basis $\{1, x\}$.
- $L(3P)$: basis $\{1, x, y\}$.

Since $\dim L(6P) = 6$, the 7 functions $\{1, x, y, x^2, xy, y^2, x^3\}$ in $L(6P)$ must satisfy a linear relation:

$$A_1 + A_2x + A_3y + A_4x^2 + A_5xy + A_6y^2 + A_7x^3 = 0.$$

The function x has a pole of order 2 at P, and y has a pole of order 3 at P. By examining the pole orders at P, we can deduce that the terms y^2 (pole order 6) and x^3 (pole order 6) must both be present, so their coefficients must be non-zero. After rescaling, we get the desired Weierstrass equation.

Conversely, every smooth cubic curve given by a Weierstrass equation is an elliptic curve with basepoint $P = [0 : 1 : 0]$. □

The group structure on an elliptic curve comes from the Picard group.

Proposition 1.3. *The map $\alpha : E \to \mathrm{Pic}^0(E)$ given by $Q \mapsto [Q - P]$ is a bijection.*

Lemma 1.4. *Let C be a curve of genus 1. Then for $P, Q \in C$, we have $(P) \sim (Q)$ if and only if $P = Q$.*

Proof. The direction ($\Leftarrow$) is clear. For ($\Rightarrow$), choose $f \in k(C)$ such that $\operatorname{div}(f) = P - Q$. By Riemann-Roch, $\dim L(P) = 1$. But $L(P)$ contains the constant functions. Thus, f must be a constant, which implies $P - Q = 0$, so $P = Q$. □

Proof (of Proposition). **Injectivity:** This follows directly from the preceding lemma. If $\alpha(Q_1) = \alpha(Q_2)$, then $[Q_1 - P] = [Q_2 - P]$, which implies $Q_1 \sim Q_2$, so $Q_1 = Q_2$.

Surjectivity: Let $D \in \operatorname{Pic}^0(E)$. We want to find a point Q such that $[Q - P] = D$. This is equivalent to finding Q such that $Q \sim D + P$. The divisor $D + P$ has degree 1. By Riemann-Roch, $\dim L(D + P) = 1$. So there is a non-zero function $f \in L(D + P)$, meaning $\operatorname{div}(f) + D + P \geq 0$. Since $\deg(\operatorname{div}(f)) = 0$ and $\deg(D + P) = 1$, the divisor $\operatorname{div}(f) + D + P$ must be an effective divisor of degree 1, which must be a single point Q. Thus $Q \sim D + P$, and $\alpha(Q) = [Q - P] = D$. □

We can now transport the group structure of $\operatorname{Pic}^0(E)$ onto E. The identity element on E is P, denoted $\mathcal{O}$. For points $A, B \in E$, the sum $A \oplus B$ is defined by the relation $\alpha(A \oplus B) = \alpha(A) + \alpha(B)$.

Lemma 1.5 (Geometric Group Law)**.** *Let A, B, C be points on an elliptic curve E. Then $A \oplus B \oplus C = \mathcal{O}$ if and only if A, B, C are the intersection points of E with a line.*

Proof. ($\Rightarrow$) Suppose $A + B + C \sim 3P$. This means there exists $f \in k(E)$ such that $\operatorname{div}(f) = A + B + C - 3P$. This implies $f \in L(3P)$. The basis of $L(3P)$ is $\{1, x, y\}$, so f is a linear combination $f = c_1 + c_2x + c_3y$. The zeros of f are A, B, C. In projective coordinates, these points lie on the line $c_1Z + c_2X + c_3Y = 0$.

($\Leftarrow$) Suppose A, B, C lie on the line L defined by $c_1Z + c_2X + c_3Y = 0$. Let $f = c_1 + c_2x + c_3y$. The function f has a pole of order 3 at $P = \mathcal{O}$. By Bézout's Theorem, a line intersects a cubic curve at 3 points (counting multiplicity). Thus the only zeros of f are A, B, C. Therefore, $\operatorname{div}(f) = A + B + C - 3P$, which means $A + B + C \sim 3P$, so $A \oplus B \oplus C = \mathcal{O}$. □

Addition Law (Composition Law): To compute $Q \oplus R$:

1. Let L be the line through Q and R. (If $Q = R$, L is the tangent line to E at Q).
2. Let S be the third intersection point of L with E. From the lemma, $Q \oplus R \oplus S = \mathcal{O}$.
3. Let L' be the line through S and $\mathcal{O}$. Let the third intersection point be T.
4. From the lemma, $S \oplus \mathcal{O} \oplus T = \mathcal{O}$, which means $S \oplus T = \mathcal{O}$, so $T = -S$.
5. Combining these gives $Q \oplus R = -S = T$. We denote this point by $Q \oplus R$.

Remark 1.6 (Formulas for Addition). Let E be given by $y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$. Let $P_1 = (x_1, y_1)$ and $P_2 = (x_2, y_2)$ be two points on E. If $x_1 = x_2$ and $y_1 + y_2 + a_1x_2 + a_3 = 0$, then $P_1 \oplus P_2 = \mathcal{O}$. Otherwise, let

$$\lambda = \begin{cases} \frac{y_2 - y_1}{x_2 - x_1}, & \text{if } x_1 \neq x_2 \\ \frac{3x_1^2 + 2a_2x_1 + a_4 - a_1y_1}{2y_1 + a_1x_1 + a_3}, & \text{if } x_1 = x_2 \end{cases}$$

$$\nu = \begin{cases} \frac{y_1x_2 - y_2x_1}{x_2 - x_1}, & \text{if } x_1 \neq x_2 \\ \frac{-x_1^3 + a_4x_1 + 2a_6 - a_3y_1}{2y_1 + a_1x_1 + a_3}, & \text{if } x_1 = x_2 \end{cases}$$

Then $P_3 = P_1 \oplus P_2$ has coordinates (x_3, y_3):

$$x_3 = \lambda^2 + a_1\lambda - a_2 - x_1 - x_2,$$
$$y_3 = -(\lambda + a_1)x_3 - \nu - a_3.$$

Remark 1.7. Given a non-smooth curve E given by a Weierstrass equation (i.e., $\Delta = 0$), the set of non-singular points $E_{ns}(k)$ still forms an abelian group using the same composition law.

2 Elliptic Integrals, Weierstrass $\wp$-function, and Lattices

We consider integrating on an elliptic curve over $\mathbb{C}$, say the differential $\omega = \frac{dx}{y}$. The integral $\int_P^R \omega$ is path-dependent on the Riemann surface associated with the curve. If $E(\mathbb{C})$ is given in Legendre form $y^2 = x(x-1)(x-\lambda)$, the integral is $\int_\infty^z \frac{dt}{\sqrt{t(t-1)(t-\lambda)}}$. This is multi-valued, requiring branch cuts. The resulting object is a Riemann surface (a torus). Integrating around non-contractible loops on this surface adds periods. Let α, β be generators of $\pi_1(E(\mathbb{C}))$. We define the periods

$$\omega_1 = \int_\alpha \omega, \quad \omega_2 = \int_\beta \omega.$$

The integral $\int_P^Q \omega$ is well-defined modulo the lattice $\Lambda = \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2$. This gives an isomorphism of complex Lie groups:

$$E(\mathbb{C}) \cong \mathbb{C}/\Lambda.$$

We now explore the other direction of this correspondence.

Definition 2.1. A **lattice** in $\mathbb{C}$ is a subgroup of the form $\Lambda = \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2$ where $\omega_1, \omega_2 \in \mathbb{C}$ are linearly independent over $\mathbb{R}$.

Definition 2.2. An **elliptic function** (relative to a lattice Λ) is a meromorphic function $f(z)$ on $\mathbb{C}$ such that $f(z+\omega) = f(z)$ for all $z \in \mathbb{C}$ and all $\omega \in \Lambda$.

Definition 2.3. Let Λ be a lattice. The **Weierstrass $\wp$-function** is defined by the series

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

This is an elliptic function. The **Eisenstein series** of weight $2k$ is

$$G_{2k}(\Lambda) = \sum_{\omega \in \Lambda \setminus \{0\}} \omega^{-2k}, \quad \text{for } k \geq 2.$$

We define the invariants $g_2(\Lambda) = 60G_4(\Lambda)$ and $g_3(\Lambda) = 140G_6(\Lambda)$.

Theorem 2.4. *The field of elliptic functions for Λ is $\mathbb{C}(\wp(z), \wp'(z))$. The Weierstrass $\wp$-function and its derivative satisfy the differential equation:*

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

Proposition 2.5. *Let Λ be a lattice. The curve E given by $y^2 = 4x^3 - g_2x - g_3$ is an elliptic curve over $\mathbb{C}$. The map*

$$\phi : \mathbb{C}/\Lambda \to E(\mathbb{C}) \subset \mathbb{P}^2(\mathbb{C})$$

$$z \mapsto [\wp(z) : \wp'(z) : 1] \quad (\textit{and } 0 \mapsto [0:1:0])$$

is an isomorphism of complex Lie groups.

Definition 2.6. An **isogeny** between two elliptic curves E_1 and E_2 is a non-constant morphism of curves $\phi : E_1 \to E_2$ that preserves the basepoint, i.e., $\phi(\mathcal{O}_1) = \mathcal{O}_2$.

Theorem 2.7. *Let Λ_1, Λ_2 be lattices in $\mathbb{C}$, and let E_1, E_2 be the corresponding elliptic curves.*

a) The map from the set $\{\alpha \in \mathbb{C} \mid \alpha\Lambda_1 \subseteq \Lambda_2\}$ to the set of non-zero holomorphic maps $\phi : \mathbb{C}/\Lambda_1 \to \mathbb{C}/\Lambda_2$ with $\phi(0) = 0$, given by $\alpha \mapsto \phi_\alpha(z) = \alpha z \pmod{\Lambda_2}$, is a bijection.

b) The map in (a) induces a bijection between the set of isogenies $\phi : E_1 \to E_2$ and the set $\{\alpha \in \mathbb{C}^* \mid \alpha\Lambda_1 \subseteq \Lambda_2\}$.

Proof of (a). **Injectivity:** If $\phi_\alpha = \phi_\beta$, then $\alpha z \equiv \beta z \pmod{\Lambda_2}$ for all $z \in \mathbb{C}$. This means the map $z \mapsto (\alpha - \beta)z$ maps $\mathbb{C}$ into the discrete set Λ_2. For this map to be continuous, it must be constant, which implies $\alpha - \beta = 0$, so $\alpha = \beta$.

Surjectivity: Let $\phi : \mathbb{C}/\Lambda_1 \to \mathbb{C}/\Lambda_2$ be a holomorphic map with $\phi(0) = 0$. Since $\mathbb{C}$ is the universal cover of both tori and is simply connected, we can lift ϕ to a map $f : \mathbb{C} \to \mathbb{C}$ with $f(0) = 0$. By commutativity of the diagram, $f(z+\omega) \equiv f(z) \pmod{\Lambda_2}$ for all $\omega \in \Lambda_1$. This means $f(z+\omega) - f(z)$ is a function of ω only, since its derivative with respect to z is $f'(z+\omega) - f'(z) = 0$ (by discreteness). Differentiating $f(z+\omega) - f(z)$ with respect to z, we get $f'(z+\omega) = f'(z)$ for all $\omega \in \Lambda_1$. Thus f' is a holomorphic elliptic function with respect to Λ_1. By Liouville's theorem, f' must be constant, say $f'(z) = \alpha$. Integrating gives $f(z) = \alpha z + \gamma$. Since $f(0) = 0$, we have $\gamma = 0$. So $f(z) = \alpha z$. The condition $f(z+\omega) \equiv f(z) \pmod{\Lambda_2}$ implies $\alpha(z+\omega) \equiv \alpha z \pmod{\Lambda_2}$, which simplifies to $\alpha\omega \in \Lambda_2$ for all $\omega \in \Lambda_1$. This means $\alpha\Lambda_1 \subseteq \Lambda_2$. □

Proof of (b) sketch. An isogeny $\phi : E_1 \to E_2$ lifts to a holomorphic map $\tilde{\phi} : \mathbb{C}/\Lambda_1 \to \mathbb{C}/\Lambda_2$. By part (a), this corresponds to some $\alpha \in \mathbb{C}^*$ with $\alpha\Lambda_1 \subseteq \Lambda_2$. The map on the Weierstrass coordinates is given by $(x_1, y_1) = (\wp(z, \Lambda_1), \wp'(z, \Lambda_1))$ maps to $(x_2, y_2) = (\wp(\alpha z, \Lambda_2), \wp'(\alpha z, \Lambda_2))$. One needs to show that $\wp(\alpha z, \Lambda_2)$ and $\wp'(\alpha z, \Lambda_2)$ are rational functions of $\wp(z, \Lambda_1)$ and $\wp'(z, \Lambda_1)$. This is true because they are elliptic functions with respect to the lattice Λ_1. □

Corollary 2.8. *Two elliptic curves E_1, E_2 corresponding to lattices Λ_1, Λ_2 are isomorphic over $\mathbb{C}$ if and only if the lattices Λ_1 and Λ_2 are homothetic, i.e., there exists an $\alpha \in \mathbb{C}^*$ such that $\alpha\Lambda_1 = \Lambda_2$.*