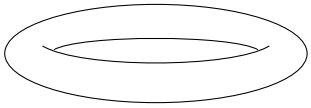
Elliptic Curves over $\mathbb{C}$ and Complex Multiplication

In last lecture, we introduced elliptic curves from an abstract algebraic perspective. In this lecture, we give a more geometric description of elliptic curves defined over the complex numbers. This description allows us to concretely think about points on an elliptic curve, visualize the set of torsion points, and more importantly it gives us a way to parameterize all elliptic curves over $\mathbb{C}$ and observe the ones with complex multiplication.

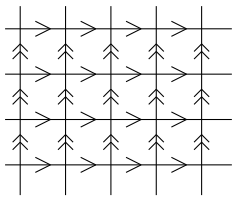
1 Elliptic Curves over $\mathbb{C}$ and Lattices

Recall from last lecture that an elliptic curve E is a smooth, projective, genus 1 algebraic curve. The set of complex points on a genus 1 curve over $\mathbb{C}$ is topologically a torus with complex analytic topology.

The universal cover of a torus is a 2-dimensional plane and the covering map is given by $\mathbb{R}^2$ moding out all translations $(x, y) \mapsto (x + m, y + n)$, $m, n \in \mathbb{Z}$.



torus T



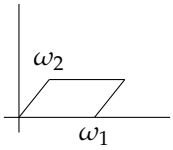
covering map $\mathbb{R}^2/\mathbb{Z}^2$

The set of $\mathbb{C}$-points on an elliptic curve $E/\mathbb{C}$ can also be described this way.

Definition 1.1. A *lattice* $\Lambda \subset \mathbb{C}$ is a discrete subgroup of $\mathbb{C}$ which contains an $\mathbb{R}$-basis for $\mathbb{C}$.

Question: why is such a Λ isomorphic to $\mathbb{Z}^2$?

Let $\{\omega_1, \omega_2\}$ be a set of generators of Λ, i.e. $\Lambda = \{n_1\omega_1 + n_2\omega_2 : n_1, n_2 \in \mathbb{Z}\}$.



The quotient $\mathbb{C}/\Lambda$ is a complex Lie group with the addition on $\mathbb{C}$. Given two lattices Λ_1, Λ_2, any maps between quotients $\mathbb{C}/\Lambda_1 \to \mathbb{C}/\Lambda_2$ are given by complex numbers $\alpha \in \mathbb{C}$ such that $\alpha\Lambda_1 \subset \Lambda_2$ by

$$\phi_\alpha(z) := \alpha z \bmod \Lambda_2.$$

Two lattices Λ_1, Λ_2 are called *homothetic* if $\Lambda_1 = \alpha\Lambda_2$ for some $\alpha \in \mathbb{C}$. This is an equivalence relation between lattices in $\mathbb{C}$.

We will show the complex points of an elliptic curve $E(\mathbb{C})$ is isomorphic to $\mathbb{C}/\Lambda$ for some lattice Λ as complex Lie groups. Moreover, the following categories are equivalent.

Objects: elliptic curves over $\mathbb{C}$, up to isomorphism	$\Longleftrightarrow$	Objects: lattices $\Lambda \subset \mathbb{C}$, up to homothety
Maps: isogenies		Maps: $\{\alpha \in \mathbb{C} : \alpha\Lambda_1 \subset \Lambda_2\}$

1.1 Functions on $\mathbb{C}/\Lambda$

Recall points on an elliptic curve E defined over $\mathbb{C}$ satisfies a Weierstrass equation $y^2 = x^3 + Ax + B$. Thus to identify the set of points $E(\mathbb{C})$ and points in $\mathbb{C}/\Lambda$ where Λ is a lattice, we want to construct functions f, g on $\mathbb{C}/\Lambda$ such that the values of $f(z), g(z)$ satisfy $f(z)^2 = g(z)^3 + Ag(z) + B$ for $z \in \mathbb{C}/\Lambda$.

Definition 1.2. Let $\Lambda \subset \mathbb{C}$ be a lattice. The *Weierstrass $\wp$-function* relative to Λ is defined by the series

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

The series in the definition of $\wp(z)$ converges absolutely and uniformly on every compact subset of $\mathbb{C} \setminus \Lambda$. The Weierstrass $\wp$-function is a meromorphic function on $\mathbb{C}$ having a double pole with residue 0 at every lattice point and no other poles. It satisfies condition

$$\wp(z+\omega) = \wp(z), \quad \text{for all } \omega \in \Lambda, z \in \mathbb{C}.$$

Meromorphic functions on $\mathbb{C}$ satisfying this condition are called *elliptic functions*. Elliptic functions are functions on $\mathbb{C}/\Lambda$. The set of all elliptic functions is a field which we denote by $\mathbb{C}(\Lambda)$.

The derivative $\wp'(z)$ of the Weierstrass $\wp$-function is also an elliptic function. Moreover, the field $\mathbb{C}(\Lambda) = \mathbb{C}(\wp(z), \wp'(z))$. Every elliptic function is a rational combination of $\wp(z)$ and $\wp'(z)$.

1.2 Associate an Elliptic Curve to a Lattice Λ

Next we show that $\wp(z)$ and $\wp'(z)$ satisfies an equation of the form $\wp'(z)^2 = 4\wp(z)^3 + A\wp(z) + B$.

Definition 1.3. Let $\Lambda \subset \mathbb{C}$ be a lattice. The *Eisenstein series* of weight $2k$ is the series

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

The Eisenstein series is absolutely convergent for all $k > 1$. Thus, for a fixed lattice Λ and $k > 1$, the values $G_{2k}(\Lambda)$ are constants associated to Λ which we simply denote by G_{2k}.

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

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

The only holomorphic elliptic functions are constant functions. Thus, using the Laurent series of $\wp(z)$ and $\wp'(z)$, we could compare the order of pole at $z = 0$ to conclude the following statement. For a fixed lattice Λ, the Weierstrass $\wp$-function and the Eisenstein series G_4, G_6 satisfy the following differential equation

$$\wp'(z)^2 = 4\wp(z)^3 - 60G_4\wp(z) - 140G_6, \quad \text{for all } z \in \mathbb{C} \setminus \Lambda.$$

Now we can associate to a lattice $\Lambda \subset \mathbb{C}$ an elliptic curve $E/\mathbb{C}$.

Theorem 1.4. *Given a lattice $\Lambda \subset \mathbb{C}$, let $E/\mathbb{C}$ be the curve*

$$E : y^2 = 4x^3 - 60G_4 x - 140G_6.$$

It is an elliptic curve and the map

$$\begin{aligned} \phi : \mathbb{C}/\Lambda &\to E \\ z &\mapsto (\wp(z), \wp'(z)) \end{aligned}$$

is a complex analytic isomorphism of complex Lie groups.

1.3 Associate a Lattice to an Elliptic Curve

By using Weierstrass $\wp$-function, we could associate a lattice $\Lambda \subset \mathbb{C}$ with an elliptic curve $E/\mathbb{C}$. Moreover, the points $E(\mathbb{C})$ are identified with $\mathbb{C}/\Lambda$ with addition being the group law induced from $\mathbb{C}$. Next we will show every elliptic curve $E/\mathbb{C}$ arises from this way. Thus, this identification gives us a way to concretely visualize the torsion points on E.

Let $E/\mathbb{C}$ be an elliptic curve defined by Weierstrass equation $y^2 = x^3 + Ax + B$. From last lecture, we see that $\frac{dx}{y}$ is a holomorphic differential on E which is invariant under translation.

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

$$\omega_1 := \int_\alpha \frac{dx}{y}, \quad \omega_2 := \int_\beta \frac{dx}{y}$$

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

Moreover, let $\Lambda \subset \mathbb{C}$ be the lattice generated by ω_1, ω_2. Then the map

$$F : E(\mathbb{C}) \to \mathbb{C}/\Lambda, \quad F(P) = \int_O^P \frac{dx}{y} \mod \Lambda$$

is a complex analytic isomorphism of Lie groups.

2 CM Elliptic Curves over $\mathbb{C}$

2.1 From a Proper Fractional Ideal to a CM elliptic curve

Recall from previous lecture that for an elliptic curve $E/\mathbb{C}$, its endomorphism ring $\mathrm{End}(E)$ is either isomorphic to $\mathbb{Z}$ or an order $\mathcal{O}$ of an imaginary quadratic field K. We will now discuss the structure of orders in imaginary quadratic fields and their proper fractional ideals. This will allow us to construct CM elliptic curves by constructing their corresponding lattices.

Definition 2.1. An order $\mathcal{O}$ of an imaginary quadratic field K is a subring such that $\mathcal{O}$ is a rank 2 free $\mathbb{Z}$-module.

Let $\mathcal{O}_K$ be the ring of integers of K. For any order $\mathcal{O} \subset K$, we have $\mathcal{O} \subset \mathcal{O}_K$ with finite index and K is the field of fractions of $\mathcal{O}$. The ring $\mathcal{O}_K$ is referred to as the maximal order of K.

A *fractional* ideal of $\mathcal{O}$ is a subset of K which is a nonzero finitely generated $\mathcal{O}$-module. It is of the form $\alpha\mathfrak{a}$ for some $\alpha \in K^*$ and $\mathfrak{a}$ an $\mathcal{O}$-ideal. Moreover, a nonzero fractional $\mathcal{O}$-ideal is a free $\mathbb{Z}$-module of rank 2.

Thus, under an embedding $K \hookrightarrow \mathbb{C}$, the image of a fractional $\mathcal{O}$-ideal $\mathfrak{a}$ is a lattice $\Lambda_\mathfrak{a} \subset \mathbb{C}$ such that $\alpha\Lambda_\mathfrak{a} \subset \Lambda_\mathfrak{a}$ for any $\alpha \in \mathcal{O}$. From the previous discussion, it corresponds to an elliptic curve E with $\mathcal{O} \subset \mathrm{End}(E)$. Next we discuss for which fractional $\mathcal{O}$-ideals we exactly have $\mathcal{O} = \mathrm{End}(E)$.

A fractional $\mathcal{O}$-ideal $\mathfrak{a}$ is called *proper* if $\mathcal{O} = \{\alpha \in K \mid \alpha\mathfrak{a} \subset \mathfrak{a}\}$.

A fractional $\mathcal{O}$-ideal $\mathfrak{a}$ is called *invertible* if there exists a fractional $\mathcal{O}$-ideal $\mathfrak{b}$ such that $\mathfrak{a}\mathfrak{b} = \mathcal{O}$.

Let $\mathcal{O}$ be an order of an imaginary quadratic field. Then a fractional $\mathcal{O}$-ideal is proper if and only if it is invertible. For the maximal order of an imaginary quadratic field, every fractional ideal is proper. The set of all proper fractional $\mathcal{O}$-ideals which we denote by $I(\mathcal{O})$ forms a group under multiplication.

By definition, the lattice of a proper fractional $\mathcal{O}$-ideal in $\mathbb{C}$ gives rise to an elliptic curve E such that $\mathcal{O} = \mathrm{End}(E)$. We will discuss later that every such elliptic curve arises from this way.

As we want to classify elliptic curves up to isomorphism, lattices up to homothety, we discuss this equivalence relation among proper fractional $\mathcal{O}$-ideals.

A fractional $\mathcal{O}$-ideal $\mathfrak{a}$ is called *principal* if it is of the form $\alpha\mathcal{O}$ for some $\alpha \in K^*$. Principal fractional ideals are proper and invertible. They form a subgroup of $I(\mathcal{O})$ which we denote by $P(\mathcal{O})$.

Let $\mathfrak{a}, \mathfrak{b}$ be proper fractional $\mathcal{O}$-ideals, under an embedding $K \hookrightarrow \mathbb{C}$, the lattices $\Lambda_\mathfrak{a}$ and $\Lambda_\mathfrak{b}$ are homothetic if and only if $\mathfrak{a}\mathfrak{b}^{-1}$ is principal.

So naturally, we consider the quotient group $C(\mathcal{O}) := I(\mathcal{O}/P(\mathcal{O}))$ which is a finite group called the ideal class group of order $\mathcal{O}$ and its order $h(\mathcal{O})$ is referred to as the class number of $\mathcal{O}$. We will see that the ideal class group $C(\mathcal{O})$ parameterizes isomorphism classes of elliptic curves with $\mathrm{End}(E) = \mathcal{O}$.

2.2 From a CM Elliptic Curve to a Proper Fractional Ideal

We have seen that a proper fractional ideal of an order in an imaginary quadratic gives rise to a CM elliptic curve. Now we will show every CM elliptic curve arises from this way.

Given a lattice $\Lambda \subset \mathbb{C}$, the endomorphisms of $\mathbb{C}/\Lambda$ is the set $\{\phi_\alpha \mid \alpha \in \mathbb{C},\ \alpha\Lambda \subset \Lambda\}$. A lattice Λ corresponds to a CM elliptic curve if there exists $\alpha \in \mathbb{C} \setminus \mathbb{Z}$, such that $\alpha\Lambda \subset \Lambda$. We say such a lattice has CM.

Theorem 2.2. *A lattice Λ has CM if and only if it is homothetic to a lattice of a proper fractional ideal of an order $\mathcal{O}$ in an imaginary quadratic field K.*

Proof. By definition, the lattice of a proper fractional $\mathcal{O}$-ideal under an embedding $\mathcal{O} \hookrightarrow \mathbb{C}$ has its endomorphism ring being $\mathcal{O}$. Thus, it has CM.

So we focus on proving the converse.

For any lattice $\mathbb{Z}\omega_1 + \mathbb{Z}\omega_2$, we can find a homothetic lattice $\Lambda = \mathbb{Z} + \mathbb{Z}\tau$ for some $\tau \in \mathbb{C}$.

So for a $\alpha \in \mathrm{End}(\Lambda)$, we have $\alpha = a + b\tau$ and $\alpha\tau = c + d\tau$ for $a, b, c, d \in \mathbb{Z}$. This implies that τ satisfies a quadratic equation

$$(a + b\tau)\tau = c + d\tau.$$

Since $\{1, \tau\}$ generates a lattice, we know τ is not real. Thus, the field $K := \mathbb{Q}(\tau)$ is imaginary quadratic. Moreover,

$$\mathcal{O} := \{\beta \in K \mid \beta\Lambda \subset \Lambda\}$$

is an order of K for which Λ is a proper fraction $\mathcal{O}$-ideal. □