18.783 Elliptic Curves
Lecture 16

Andrew Sutherland

November 7, 2023

Uniformization Theorem

Given a lattice $L \subseteq \mathbb{C}$, let

$$E_L \colon y^2 = 4x^3 - g_2(L)x - g_3(L),$$

denote the corresponding elliptic curve, equipped with the map

$$\begin{aligned} \Phi_L \colon \mathbb{C}/L &\to E_L(\mathbb{C}) \\ z &\mapsto \begin{cases} (\wp(z), \wp'(z)) & z \notin L, \\ 0 & z \in L. \end{cases} \end{aligned}$$

Over the course of the last two lectures we proved the following theorem.

Theorem (Uniformization Theorem)

The map $L \mapsto E_L$ defines a bijection between between homethety classes of lattices $L \subseteq \mathbb{C}$ and isomorphism classes of elliptic curves $E/\mathbb{C}$ in which each Φ_L is an analytic group isomorphism (in fact, an isomorphism of complex Lie groups).

Morphisms of complex tori

Definition

A morphism $\varphi\colon \mathbb{C}/L_1 \to \mathbb{C}/L_2$ of complex tori is a map induced by a holomorphic function $f\colon \mathbb{C} \to \mathbb{C}$ such that the following diagram commutes:

$$\begin{tikzcd}
\mathbb{C} \arrow[r, "f"] \arrow[d, "\pi_1"] & \mathbb{C} \arrow[d, "\pi_2"] \\
\mathbb{C}/L_1 \arrow[r, "\varphi"] & \mathbb{C}/L_2
\end{tikzcd}$$

Morphisms of complex tori

Definition

A morphism $\varphi\colon \mathbb{C}/L_1 \to \mathbb{C}/L_2$ of complex tori is a map induced by a holomorphic function $f\colon \mathbb{C} \to \mathbb{C}$ such that the following diagram commutes:

$$\begin{tikzcd}
\mathbb{C} \arrow[r, "f"] \arrow[d, "\pi_1"] & \mathbb{C} \arrow[d, "\pi_2"] \\
\mathbb{C}/L_1 \arrow[r, "\varphi"] & \mathbb{C}/L_2
\end{tikzcd}$$

Example

For each $\alpha \in \mathbb{C}$ the holomorphic map $z \mapsto \alpha z$ defines an analytic endomorphism of $\mathbb{C}$. When $\alpha L_1 \subseteq L_2$ this induces a holomorphic group homomorphism

$$\begin{aligned} \varphi_\alpha\colon \mathbb{C}/L_1 &\to \mathbb{C}/L_2 \\ z + L_1 &\mapsto \alpha z + L_2 \end{aligned}$$

Every morphism of complex tori is multiplication-by-α

Theorem

Let $\varphi\colon \mathbb{C}/L_1 \to \mathbb{C}/L_2$ *be a holomorphic map with* $\varphi(0) = 0$.
There is a unique $\alpha \in \mathbb{C}$ *for which* $\varphi = \varphi_\alpha$.

Proof.

To the board! $\square$

Every morphism of complex tori is multiplication-by-α

Theorem

Let $\varphi\colon \mathbb{C}/L_1 \to \mathbb{C}/L_2$ be a holomorphic map with $\varphi(0) = 0$.
There is a unique $\alpha \in \mathbb{C}$ for which $\varphi = \varphi_\alpha$.

Proof.

To the board! □

Corollary

For any two lattices $L_1, L_2 \subseteq \mathbb{C}$ the map

$$\Big\{\alpha \in \mathbb{C} : \alpha L_1 \subseteq L_2\Big\} \to \Big\{\text{morphisms}\, \varphi\colon \mathbb{C}/L_1 \to \mathbb{C}/L_2\Big\}$$
$$\alpha \mapsto \varphi_\alpha$$

is an isomorphism of groups. If $L_1 = L_2$ it is an isomorphism of commutative rings.

Morphisms of complex tori and isogenies of elliptic curves

For $i = 1, 2$ let $L_i \subseteq \mathbb{C}$ be a lattice, let $E_i := E_{L_i}$ be the corresponding elliptic curve. Let $\wp_i(z) := \wp(z; L_i)$, and let $\Phi_i \colon \mathbb{C}/L_i \to E_i(\mathbb{C})$.

Theorem

For any $\alpha \in \mathbb{C}$, the following are equivalent:

(i) $\alpha L_1 \subseteq L_2$;

(ii) $\wp_2(\alpha z) = u(\wp_1(z))/v(\wp_1(z))$ *for some polynomials* $u, v \in \mathbb{C}[x]$;

(iii) *There is a unique* $\phi_\alpha \in \operatorname{Hom}(E_1, E_2)$ *such that the following diagram commutes:*

$$\begin{tikzcd}
\mathbb{C} \arrow[r] \arrow[d, "\alpha"] & \mathbb{C}/L_1 \arrow[r, "\Phi_1"] & E_1(\mathbb{C}) \arrow[d, "\phi_\alpha"] \\
\mathbb{C} \arrow[r] & \mathbb{C}/L_2 \arrow[r, "\Phi_2"] & E_2(\mathbb{C})
\end{tikzcd}$$

For every $\phi \in \operatorname{Hom}(E_1, E_2)$ there is a unique $\alpha = \alpha_\phi$ satisfying (1)–(3).
The maps $\phi \mapsto \alpha_\phi$ and $\alpha \mapsto \phi_\alpha$ are inverse isomorphisms between the abelian groups $\operatorname{Hom}(E_1, E_2)$ and $\{\alpha \in \mathbb{C} : \alpha L_1 \subseteq L_2\}$.

Morphisms of complex tori and isogenies of elliptic curves

To prove our theorem relating morphisms of complex tori and elliptic curves, we need the following lemma.

Recall that $\mathbb{C}(L)$ is the field of elliptic functions for the lattice $L \subseteq \mathbb{C}$. The Weierstrass $\wp$-function $\wp(z) = \wp(z; L)$ and its derivative $\wp'(z)$ are both elements of $\mathbb{C}(L)$

Lemma

Let $L \subseteq \mathbb{C}$ be a lattice. The following hold:

(i) $\mathbb{C}(L) = \mathbb{C}(\wp, \wp')$;

(ii) $\mathbb{C}(L)^{\text{even}} = \mathbb{C}(\wp)$;

(iii) *if $f \in \mathbb{C}(L)^{\text{even}}$ is holomorphic on $\mathbb{C} - L$ then $f \in \mathbb{C}[\wp]$.*

Proof.

To the board! ☐

Endomorphism rings of complex tori and elliptic curves

We now specialize to the case $L = L_2 = L_1$, and put $E = E_L$, in which case the group $\{\alpha \in \mathbb{C} \colon \alpha L \subseteq L\} \simeq \mathrm{Hom}(E, E) = \mathrm{End}(E)$ becomes a ring, not just a group.

Corollary

Let $L \subseteq \mathbb{C}$ be a lattice and let $E := E_L$. The following hold:

(i) *The maps $\alpha \mapsto \phi_\alpha$ and $\phi \mapsto \alpha_\phi$ are inverse ring isomorphisms between $\{\alpha \in \mathbb{C} : \alpha L \subseteq L\}$ and $\mathrm{End}(E)$;*

(ii) *the involution $\phi \mapsto \hat{\phi}$ of $\mathrm{End}(E)$ corresponds to complex conjugation $\alpha \mapsto \bar{\alpha}$ in $\{\alpha \in \mathbb{C} : \alpha L \subseteq L\}$;*

(iii) $\mathrm{T}(\alpha) := \alpha + \bar{\alpha} = \mathrm{tr}\, \phi_\alpha$ *and* $\mathrm{N}(\alpha) := \alpha\bar{\alpha} = \deg \phi_\alpha = \deg u = \deg v + 1$, *where* $u, v \in \mathbb{C}[x]$ *are as in the morphism/isogeny Theorem.*

Proof.

To the board! ☐

Complex multiplication

The corollary explains the origin of the term complex multiplication (CM).

When $\mathrm{End}(E_L)$ is bigger than $\mathbb{Z}$ the extra endomorphisms in $\mathrm{End}(E_L)$ are all multiplication-by-α maps in $\mathrm{End}(\mathbb{C}/L)$, for some $\alpha \in \mathbb{C} - \mathbb{R}$ that is an algebraic integer in an imaginary quadratic field.

Corollary

Let E be an elliptic curve defined over $\mathbb{C}$. Then $\mathrm{End}(E)$ is commutative and therefore isomorphic to either $\mathbb{Z}$ or an order in an imaginary quadratic field.

Proof.

$\mathrm{End}(E_L) \simeq \{\alpha \in \mathbb{C} : \alpha L \subseteq L\}$ is commutative, so it cannot be an order in a quaternion algebra. □

The corollary also applies to elliptic curves over $\mathbb{Q}$, number fields, or any field embedded in $\mathbb{C}$. It extends to all fields of characteristic 0 (via the Lefschetz principle).

Elliptic curves with complex multiplication

We have shown that for any lattice $L \subseteq \mathbb{C}$ we have ring isomorphisms

$$\operatorname{End}(E_L) \simeq \{\alpha \in \mathbb{C} : \alpha L \subseteq L\} \simeq \operatorname{End}(\mathbb{C}/L).$$

We have been treating the isomorphism on the left as an equality, and it will be convenient to do the same for the isomorphism on the right.

Elliptic curves with complex multiplication

We have shown that for any lattice $L \subseteq \mathbb{C}$ we have ring isomorphisms

$$\operatorname{End}(E_L) \simeq \{\alpha \in \mathbb{C} : \alpha L \subseteq L\} \simeq \operatorname{End}(\mathbb{C}/L).$$

We have been treating the isomorphism on the left as an equality, and it will be convenient to do the same for the isomorphism on the right.

The endomorphism algebra $\operatorname{End}^0(E_L)$ is isomorphic to either $\mathbb{Q}$ or an imaginary quadratic field, so we can always embed $\operatorname{End}^0(E_L)$ in $\mathbb{C}$.

Viewing $\operatorname{End}(E_L)$ as a subring of $\operatorname{End}^0(E_L)$, we have $\operatorname{End}(E_L) = \{\alpha \in \mathbb{C} : \alpha L \subseteq L\}$.

When $\operatorname{End}(\mathbb{C}/L)$ is an imaginary quadratic order $\mathcal{O}$, we can embed $\operatorname{End}^0(E_L)$ in $\mathbb{C}$ so that each multiplication-by-α endomorphism of $\mathbb{C}/L$ is $\phi_\alpha \in \operatorname{End}(E_L)$ (versus $\hat{\phi}_\alpha$).

This is the normalized identification of $\operatorname{End}(E_L)$ with $\operatorname{End}(\mathbb{C}/L) = \mathcal{O}$, which we use.

Tori with complex multiplication

Given an imaginary quadratic order $\mathcal{O}$, is there a lattice $L \subseteq \mathbb{C}$ with $\mathrm{End}(\mathbb{C}/L) = \mathcal{O}$?

Tori with complex multiplication

Given an imaginary quadratic order $\mathcal{O}$, is there a lattice $L \subseteq \mathbb{C}$ with $\mathrm{End}(\mathbb{C}/L) = \mathcal{O}$?

Consider $L = \mathcal{O}$. If $\alpha \in \mathrm{End}(E_{\mathcal{O}})$, then $\alpha\mathcal{O} \subseteq \mathcal{O}$, so $\alpha \in \mathcal{O}$ (note $1 \in \mathcal{O}$).
Conversely, if $\alpha \in \mathcal{O}$, then $\alpha\mathcal{O} \subseteq \mathcal{O}$ and $\alpha \in \mathrm{End}(E_{\mathcal{O}})$; thus $\mathrm{End}(E_{\mathcal{O}}) = \mathcal{O}$.

The same holds for any lattice homothetic to $\mathcal{O}$. Indeed, the set $\{\alpha \in \mathbb{C} \colon \alpha L \subseteq L\}$ does not change if we replace L with $L' = \lambda L$ for any $\lambda \in \mathbb{C}^\times$, so we are really only interested in lattices up to homethety (and elliptic curves up to isomorphism).

Tori with complex multiplication

Given an imaginary quadratic order $\mathcal{O}$, is there a lattice $L \subseteq \mathbb{C}$ with $\operatorname{End}(\mathbb{C}/L) = \mathcal{O}$?

Consider $L = \mathcal{O}$. If $\alpha \in \operatorname{End}(E_{\mathcal{O}})$, then $\alpha\mathcal{O} \subseteq \mathcal{O}$, so $\alpha \in \mathcal{O}$ (note $1 \in \mathcal{O}$). Conversely, if $\alpha \in \mathcal{O}$, then $\alpha\mathcal{O} \subseteq \mathcal{O}$ and $\alpha \in \operatorname{End}(E_{\mathcal{O}})$; thus $\operatorname{End}(E_{\mathcal{O}}) = \mathcal{O}$.

The same holds for any lattice homothetic to $\mathcal{O}$. Indeed, the set $\{\alpha \in \mathbb{C} \colon \alpha L \subseteq L\}$ does not change if we replace L with $L' = \lambda L$ for any $\lambda \in \mathbb{C}^\times$, so we are really only interested in lattices up to homethety (and elliptic curves up to isomorphism).

But are there any lattices L not homothetic to $\mathcal{O}$ for which we have $\operatorname{End}(E_L) = \mathcal{O}$?

We may assume $L = [1, \tau]$ and write $\mathcal{O} = [1, \omega]$, for an imaginary quadratic integer ω.

If $\operatorname{End}(E_L) = \mathcal{O}$, then $\omega \cdot 1 = \omega \in L$, so $\omega = m + n\tau$, for some $m, n \in \mathbb{Z}$ with $n \neq 0$.

Thus $nL = [n, n\tau] = [n, \omega - m] \subseteq [1, \omega] = \mathcal{O}$, so L is homothetic to a sublattice of $\mathcal{O}$. This sublattice is closed under multiplication by $\mathcal{O}$, so L is homothetic to an $\mathcal{O}$-ideal.

Proper orders

The situation is a bit more complicated than it appears. While every lattice L for which $\mathrm{End}(E_L) = \mathcal{O}$ is an $\mathcal{O}$-ideal, the converse does not hold (unless $\mathcal{O}$ is the maximal order $\mathcal{O}_K$). If we start with an arbitrary $\mathcal{O}$-ideal L, then the set

$$\mathcal{O}(L) := \{\alpha \in \mathbb{C} : \alpha L \subseteq L\} = \{\alpha \in K : \alpha L \subseteq L\}$$

is an order in K, but it is not necessarily true that $\mathcal{O}(L)$ is equal to $\mathcal{O}$.
For $\mathcal{O} \neq \mathcal{O}_K$ we can always find an $\mathcal{O}$-ideal L for which $\mathcal{O}(L)$ strictly contains $\mathcal{O}$.

Proper orders

The situation is a bit more complicated than it appears. While every lattice L for which $\mathrm{End}(E_L) = \mathcal{O}$ is an $\mathcal{O}$-ideal, the converse does not hold (unless $\mathcal{O}$ is the maximal order $\mathcal{O}_K$). If we start with an arbitrary $\mathcal{O}$-ideal L, then the set

$$\mathcal{O}(L) := \{\alpha \in \mathbb{C} : \alpha L \subseteq L\} = \{\alpha \in K : \alpha L \subseteq L\}$$

is an order in K, but it is not necessarily true that $\mathcal{O}(L)$ is equal to $\mathcal{O}$.
For $\mathcal{O} \neq \mathcal{O}_K$ we can always find an $\mathcal{O}$-ideal L for which $\mathcal{O}(L)$ strictly contains $\mathcal{O}$.

Definition

Let $\mathcal{O}$ be an order in an imaginary quadratic field K, and let L be an $\mathcal{O}$-ideal. We say that L is a *proper* $\mathcal{O}$-ideal if $\mathcal{O}(L) = \mathcal{O}$.

The ideal class group

Recall that the product of two $\mathcal{O}$-ideals $\mathfrak{a}$ and $\mathfrak{b}$ is the ideal generated by all products ab with $a \in \mathfrak{a}$ and $b \in \mathfrak{b}$, and that ideal multiplication is commutative and associative.

It is enough to consider products of generators, so if $\mathfrak{a} = [a_1, a_2]$ and $\mathfrak{b} = [b_1, b_2]$, then $\mathfrak{a}\mathfrak{b}$ is the ideal generated by the four elements $a_1b_1, a_1b_2, a_2b_1, a_2b_2 \in \mathcal{O}$.

Since $\mathfrak{a}\mathfrak{b}$ is an additive subgroup of $\mathcal{O}$, it is a free $\mathbb{Z}$-module of rank 2 and can be written as $[c_1, c_2] = [a_1b_1, a_1b_2, a_2b_1, a_2b_2]$ for some $c_1, c_2 \in \mathcal{O}$.

The ideal class group

Recall that the product of two $\mathcal{O}$-ideals $\mathfrak{a}$ and $\mathfrak{b}$ is the ideal generated by all products ab with $a \in \mathfrak{a}$ and $b \in \mathfrak{b}$, and that ideal multiplication is commutative and associative.

It is enough to consider products of generators, so if $\mathfrak{a} = [a_1, a_2]$ and $\mathfrak{b} = [b_1, b_2]$, then $\mathfrak{ab}$ is the ideal generated by the four elements $a_1b_1, a_1b_2, a_2b_1, a_2b_2 \in \mathcal{O}$.

Since $\mathfrak{ab}$ is an additive subgroup of $\mathcal{O}$, it is a free $\mathbb{Z}$-module of rank 2 and can be written as $[c_1, c_2] = [a_1b_1, a_1b_2, a_2b_1, a_2b_2]$ for some $c_1, c_2 \in \mathcal{O}$.

Call two $\mathcal{O}$-ideals $\mathfrak{a}$ and $\mathfrak{b}$ equivalent if $\alpha\mathfrak{a} = \beta\mathfrak{b}$ for some $\alpha, \beta \in \mathcal{O}$.
Equivalence is compatible with multiplication of ideals:

$$\alpha\mathfrak{a} = \beta\mathfrak{b} \text{ and } \gamma\mathfrak{c} = \delta\mathfrak{d} \quad \Longrightarrow \quad \alpha\gamma\mathfrak{ac} = \beta\delta\mathfrak{cd}.$$

Definition

Let $\mathcal{O}$ be an order in an imaginary quadratic field. The ideal class group $\mathrm{cl}(\mathcal{O})$ is the multiplicative group of equivalence classes of proper $\mathcal{O}$-ideals.

A preview of things to come...

Theorem

Let $\mathcal{O}$ *be an order in an imaginary quadratic field. The ideal classes of* $\mathrm{cl}(\mathcal{O})$ *are in bijection with the homethety classes of lattices* $L \subseteq \mathbb{C}$ *for which* $\mathrm{End}(E_L) \simeq \mathcal{O}$*.*