18.783 Elliptic Curves
Lecture 17

Andrew Sutherland

November 4, 2025

Complex multiplication

We have an equivalence of categories between complex tori $\mathbb{C}/L$ and elliptic curves $E/\mathbb{C}$ that relates homothety classes of lattices L to isomorphism classes of $E/\mathbb{C}$ via

$$\begin{aligned} \{\text{lattices } L \subseteq \mathbb{C}\}/_{\sim} &\xrightarrow{\sim} \{\text{elliptic curves } E/\mathbb{C}\}/_{\simeq} \\ L &\longmapsto E_L \colon y^2 = 4x^3 - g_2(L)x - g_3(L) \\ j(L) &= j(E_L) \end{aligned}$$

with ring isomorphisms

$$\mathrm{End}(\mathbb{C}/L) \simeq \mathrm{End}(E_L) \simeq \mathcal{O}(L) := \{\alpha \in \mathbb{C} : \alpha L \subseteq L\}$$

The ring $\mathcal{O}(L) \simeq \mathrm{End}(E_L)$ is either $\mathbb{Z}$, or it is an order $\mathcal{O}$ in an imaginary quadratic field and E_L has complex multiplication by $\mathcal{O}$ and L is homothetic to an $\mathcal{O}$-ideal.

Proper $\mathcal{O}$-ideals and the ideal class group

The $\mathcal{O}$-ideals L for which $\mathrm{End}(E_L) \simeq \mathcal{O}$ are proper, meaning that $\mathcal{O}(L) = \mathcal{O}$.
Note that $\mathcal{O} \subseteq \mathcal{O}(L)$ always holds, but in general $\mathcal{O}(L)$ may be larger than $\mathcal{O}$.

The sets

$$\{L \subseteq \mathbb{C} : \mathcal{O}(L) = \mathcal{O}\}/_{\sim} \longleftrightarrow \{E/\mathbb{C} : \mathrm{End}(E) = \mathcal{O}\}/_{\simeq}$$

are both in bijection with the ideal class group

$$\mathrm{cl}(\mathcal{O}) := \{\text{proper } \mathcal{O}\text{-ideals } \mathfrak{a}\}/_{\sim}$$

where the equivalence relation on proper $\mathcal{O}$-ideals is defined by

$$\mathfrak{a} \sim \mathfrak{b} \qquad \Longleftrightarrow \qquad \alpha\mathfrak{a} = \beta\mathfrak{b} \text{ for some nonzero } \alpha, \beta \in \mathcal{O},$$

and the group operation is $[\mathfrak{a}][\mathfrak{b}] = [\mathfrak{a}\mathfrak{b}]$.

Fractional ideals and class groups in general

Let $\mathcal{O}$ be an integral domain with fraction field K.
For any $\lambda \in K^\times$ and $\mathcal{O}$-ideal $\mathfrak{a}$, the $\mathcal{O}$-module

$$\lambda\mathfrak{a} := \{\lambda a : a \in \mathfrak{a}\} \subseteq K$$

is a fractional $\mathcal{O}$-ideal. We can assume $\lambda = \frac{1}{a}$ for some $a \in \mathcal{O}$.
The product of two fractional ideals is another fractional ideal:

$$(\lambda\mathfrak{a})(\lambda\mathfrak{a}') := (\lambda\lambda')\mathfrak{a}\mathfrak{a}'.$$

A fractional $\mathcal{O}$-ideal I is invertible if $IJ = \mathcal{O}$ for some fractional $\mathcal{O}$-ideal J.
The set of invertible fractional $\mathcal{O}$-ideals forms a group $\mathcal{I}_\mathcal{O}$ under multiplication.

For every $\lambda \in K^\times$ the fractional $\mathcal{O}$-ideal $(\lambda) := \lambda\mathcal{O}$ is invertible, with inverse (λ^{-1}).
Such fractional $\mathcal{O}$-ideals are principal, and they form a subgroup $\mathcal{P}_\mathcal{O} \subseteq \mathcal{I}_\mathcal{O}$.
We now define $\mathrm{cl}(\mathcal{O}) := \mathcal{I}_\mathcal{O}/\mathcal{P}_\mathcal{O}$ (we will prove our definitions of $\mathrm{cl}(\mathcal{O})$ are compatible).

The (absolute) norm of an ideal

Let K/k be a finite extension of fields. Multiplication by $\lambda \in K^\times$ is an invertible linear transformation $M_\lambda \in \mathrm{GL}(K)$ of K as a k-vector space. The norm and trace of λ are

$$\mathrm{N}_{K/k}\lambda := \det M_\lambda \in k^\times \qquad \mathrm{T}_{K/k}\lambda := \mathrm{tr}\, M_\lambda \in k.$$

When $k = \mathbb{Q}$ we may write $\mathrm{N} := N_{K/\mathbb{Q}}$ and $\mathrm{T} := T_{K/\mathbb{Q}}$, and if K is an imaginary quadratic field embedded in $\mathbb{C}$, we have $\mathrm{N}\alpha = \alpha\bar{\alpha}$ and $\mathrm{T}\alpha = \alpha + \bar{\alpha}$.

Definition

Let $\mathcal{O}$ be an order in a number field K. The norm of a nonzero $\mathcal{O}$-ideal $\mathfrak{a}$ is the index

$$\mathrm{N}\mathfrak{a} := [\mathcal{O} : \mathfrak{a}] = \#(\mathcal{O}/\mathfrak{a}) \in \mathbb{Z}_{>0}.$$

For any nonzero $\alpha \in \mathcal{O}$ we have $\mathrm{N}(\alpha) = |\mathrm{N}\alpha|$, since $\det M_\alpha$ is the signed volume of the fundamental parallelepiped of the lattice (α) in the $\mathbb{Q}$-vector space K.

Norms of fractional ideals

Proposition

Let $\mathcal{O}$ be an order in a number field, $\alpha \in \mathcal{O}$ nonzero, and $\mathfrak{a}$ a nonzero $\mathcal{O}$-ideal. Then

$$\mathrm{N}(\alpha\mathfrak{a}) = \mathrm{N}(\alpha)\mathrm{N}\mathfrak{a}$$

Proof.$\mathrm{N}(\alpha\mathfrak{a}) = [\mathcal{O} : \alpha\mathfrak{a}] = [\mathcal{O} : \mathfrak{a}][\mathfrak{a} : \alpha\mathfrak{a}] = [\mathcal{O} : \mathfrak{a}][\mathcal{O} : \alpha\mathcal{O}] = \mathrm{N}\mathfrak{a}\mathrm{N}(\alpha) = \mathrm{N}(\alpha)\mathrm{N}\mathfrak{a}$.

Every fractional ideal in a number field can be written as $\frac{1}{a}\mathfrak{a}$ with $a \in \mathbb{Z}_{>0}$
(if $\alpha \in \mathcal{O}$ has minpoly $f \in \mathbb{Z}[x]$ then $\beta = (f(\alpha) - f(0))/\alpha \in \mathcal{O}$ and $\alpha\beta = f(0) \in \mathbb{Z}$).

Definition

Let $\mathfrak{b} = \frac{1}{a}\mathfrak{a}$ be a nonzero fractional ideal in an order $\mathcal{O}$ of a number field with $a \in \mathbb{Z}_{>0}$.
The (absolute) norm of $\mathfrak{b}$ is

$$\mathrm{N}\mathfrak{b} := \frac{\mathrm{N}\mathfrak{a}}{\mathrm{N}a} \in \mathbb{Q}_{>0}.$$

Proper and invertible fractional ideals

Let $\mathcal{O}$ be an order in an imaginary quadratic field. For any fractional $\mathcal{O}$-ideal $\mathfrak{b}$ we define $\mathcal{O}(\mathfrak{b}) := \{\alpha \in K : \alpha\mathfrak{b} \subseteq \mathfrak{b}\}$ and call $\mathfrak{b}$ proper if $\mathcal{O}(\mathfrak{b}) = \mathcal{O}$.

Lemma

Let $\mathfrak{a}$ be a nonzero $\mathcal{O}$-ideal and let $\mathfrak{b} = \lambda\mathfrak{a}$ with $\lambda \in K^\times$.
Then $\mathfrak{b}$ is proper $\Leftrightarrow$ $\mathfrak{a}$ is proper, and $\mathfrak{b}$ is invertible $\Leftrightarrow$ $\mathfrak{a}$ is invertible.

Proof. *First claim: $\{\alpha : \alpha\mathfrak{b} \subseteq \mathfrak{b}\} = \{\alpha : \alpha\lambda\mathfrak{a} \subseteq \lambda\mathfrak{a}\} = \{\alpha : \alpha\mathfrak{a} \subseteq \mathfrak{a}\}$.*
Second: if $\mathfrak{a}$ is invertible then $\mathfrak{b}^{-1} = \alpha^{-1}\mathfrak{a}^{-1}$, and if $\mathfrak{b}$ is invertible then $\mathfrak{a}^{-1} = \alpha\mathfrak{b}^{-1}$.

Theorem

Let $\mathfrak{a} = [\alpha, \beta]$ be an $\mathcal{O}$-ideal. Then $\mathfrak{a}$ is proper if and only if $\mathfrak{a}$ is invertible. Whenever $\mathfrak{a}$ is invertible we have $\mathfrak{a}\bar{\mathfrak{a}} = (\mathrm{N}\mathfrak{a})$, where $\bar{\mathfrak{a}} = [\bar{\alpha}, \bar{\beta}]$ and $(\mathrm{N}\mathfrak{a})$ is the principal $\mathcal{O}$-ideal generated by the integer $\mathrm{N}\mathfrak{a}$; the inverse of $\mathfrak{a}$ is the fractional $\mathcal{O}$-ideal $\mathfrak{a}^{-1} = \frac{1}{\mathrm{N}\mathfrak{a}}\bar{\mathfrak{a}}$.

Proof. *To the board!*

The ideal class group

The fact that proper and invertible fractional ideals coincide implies that our two definitions of the ideal class group $\mathrm{cl}(\mathcal{O})$ as

- equivalence classes of proper $\mathcal{O}$-ideals
- the group of invertible fractional ideals modulo principal ideals

coincide. In particular, $\mathrm{cl}(\mathcal{O})$ is a group!

Corollary

Let $\mathcal{O}$ be an order in an imaginary quadratic field and let $\mathfrak{a}$ and $\mathfrak{b}$ be invertible (equivalently, proper) fractional $\mathcal{O}$-ideals. Then $\mathrm{N}(\mathfrak{a}\mathfrak{b}) = \mathrm{N}\mathfrak{a}\mathrm{N}\mathfrak{b}$.

Proof. *It suffices to consider the case where $\mathfrak{a}$ and $\mathfrak{b}$ are invertible $\mathcal{O}$-ideals. We have*

$$(\mathrm{N}(\mathfrak{a}\mathfrak{b})) = \mathfrak{a}\mathfrak{b}\overline{\mathfrak{a}\mathfrak{b}} = \mathfrak{a}\mathfrak{b}\bar{\mathfrak{a}}\bar{\mathfrak{b}} = \mathfrak{a}\bar{\mathfrak{a}}\mathfrak{b}\bar{\mathfrak{b}} = (\mathrm{N}\mathfrak{a})(\mathrm{N}\mathfrak{b}),$$

and it follows that $\mathrm{N}(\mathfrak{a}\mathfrak{b}) = \mathrm{N}\mathfrak{a}\mathrm{N}\mathfrak{b}$, since $\mathrm{N}\mathfrak{a}, \mathrm{N}\mathfrak{b}, \mathrm{N}(\mathfrak{a}\mathfrak{b}) \in \mathbb{Z}_{>0}$.

Warning: The ideal norm is not multiplicative in general! (we used invertibility).

The class group action on CM elliptic curves

Let $\mathcal{O}$ be an order in an imaginary quadratic field and let

$$\mathrm{Ell}_{\mathcal{O}} := \{j(E/\mathbb{C}) : \mathrm{End}(E) = \mathcal{O}\}.$$

Every $E/\mathbb{C}$ with $\mathrm{End}(E) = \mathcal{O}$ is isomorphic to $E_{\mathfrak{b}}$ for some proper $\mathcal{O}$-ideal $\mathfrak{b}$.
For any proper $\mathcal{O}$-ideal $\mathfrak{a}$ let

$$\mathfrak{a}E_{\mathfrak{b}} := E_{\mathfrak{a}^{-1}\mathfrak{b}}.$$

We use $E_{\mathfrak{a}^{-1}\mathfrak{b}}$ rather than $E_{\mathfrak{a}\mathfrak{b}}$ because $\mathfrak{a}\mathfrak{b} \subseteq \mathfrak{b}$ but we want $\mathfrak{b} \subseteq \mathfrak{a}^{-1}\mathfrak{b}$. We now define the action of $[\mathfrak{a}] \in \mathrm{cl}(\mathcal{O})$ via

$$[\mathfrak{a}]j(E_{\mathfrak{b}}) := j(E_{\mathfrak{a}^{-1}\mathfrak{b}}), \tag{1}$$

which we can also write as

$$[\mathfrak{a}]j(\mathfrak{b}) := j(\mathfrak{a}^{-1}\mathfrak{b}).$$

Note that this definition does not depend on the choice of representatives $\mathfrak{a}$ and $\mathfrak{b}$.

The class group action on CM elliptic curves

If $\mathfrak{a}$ is a nonzero principal $\mathcal{O}$-ideal then $\mathfrak{b}$ and $\mathfrak{a}^{-1}\mathfrak{b}$ are homothetic and $\mathfrak{a}E_{\mathfrak{b}} \simeq E_{\mathfrak{b}}$.
It follows that the identity element of $\mathrm{cl}(\mathcal{O})$ acts trivially on the set $\mathrm{Ell}_{\mathcal{O}}(\mathbb{C})$.

For any proper $\mathcal{O}$-ideals $\mathfrak{a}, \mathfrak{b}, \mathfrak{c}$ we have

$$\mathfrak{a}(\mathfrak{b}E_{\mathfrak{c}}) = \mathfrak{a}E_{\mathfrak{b}^{-1}\mathfrak{c}} = E_{\mathfrak{a}^{-1}\mathfrak{b}^{-1}\mathfrak{c}} = E_{(\mathfrak{b}\mathfrak{a})^{-1}\mathfrak{c}} = (\mathfrak{b}\mathfrak{a})E_{\mathfrak{c}} = (\mathfrak{a}\mathfrak{b})E_{\mathfrak{c}}.$$

We thus have a group action of $\mathrm{cl}(\mathcal{O})$ on $\mathrm{Ell}_{\mathcal{O}}(\mathbb{C})$, and it has the following properties:

- free: every stabilizer is trivial, since $[\mathfrak{a}]j(\mathfrak{b}) = j(\mathfrak{b}) \Leftrightarrow \mathfrak{b} \sim \mathfrak{a}^{-1}\mathfrak{b} \Leftrightarrow \mathfrak{a} \sim \mathcal{O}$.
- transitive: for every $j(\mathfrak{a}), j(\mathfrak{b})$ we have $[\mathfrak{c}]j(\mathfrak{a}) = j(\mathfrak{b})$ for some $[\mathfrak{c}] \in \mathrm{cl}(\mathcal{O})$.

Such group actions are regular. If X is a G-set, the G-action is regular if for every $x, y \in X$ there is a **unique** $g \in G$ for which $gx = y$, and we call X a G-torsor.

If we fix $x_1 \in X$, we can make X a group isomorphic to G by defining x_g to be the unique $g \in G$ for which $gx_1 = x_g$, and defining $x_g x_h := x_{gh}$.
If we don't want to fix x_1, we can instead think of ratios (or differences) of elements.

Isogenies of elliptic curves over $\mathbb{C}$

Let $\phi\colon E_1 \to E_2$ be an isogeny of elliptic curves over $\mathbb{C}$, and let L_1 and L_2 be corresponding lattices, so $E_1 = E_{L_1}$ and $E_2 = E_{L_2}$. Recall that there is a unique $\alpha = \alpha_\phi$ with $\alpha L_1 \subseteq L_2$ such that the following diagram commutes:

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

Since we only care about lattices up to homothety, we can replace L_1 with αL_1 to make $\alpha = 1$. In other words, up to isomorphism, every isogeny $\phi\colon E_1 \to E_2$ over $\mathbb{C}$ is induced by a lattice inclusion $L_1 \subseteq L_2$, and we then have

$$\#\ker\phi = [L_2 : L_1].$$

The CM action via isogenies

Now assume $E_1/\mathbb{C}$ has CM by $\mathcal{O}$. Then L_1 is homothetic to an invertible $\mathcal{O}$-ideal $\mathfrak{b}$, and we may assume $L_1 = \mathfrak{b}$ and $E_1 = E_{\mathfrak{b}}$. If $\mathfrak{a}$ is an invertible $\mathcal{O}$-ideal the inclusion $\mathfrak{b} \subseteq \mathfrak{a}^{-1}\mathfrak{b}$ induces an isogeny

$$\phi_{\mathfrak{a}}\colon E_{\mathfrak{b}} \to E_{\mathfrak{a}^{-1}\mathfrak{b}} = \mathfrak{a}E_{\mathfrak{b}}$$

If E_2 also has CM by $\mathcal{O}$ then L_2 is homothetic to an invertible $\mathcal{O}$-ideal $\mathfrak{c}$.
If we replace $\mathfrak{b}$ by $(\mathrm{N}\mathfrak{c})\mathfrak{b}$ then $\mathfrak{c}$ divides (hence contains) $\mathfrak{b}$, since $\mathrm{N}\mathfrak{c} = \mathfrak{c}\bar{\mathfrak{c}}$.
If we now put $\mathfrak{a} = \mathfrak{b}\mathfrak{c}^{-1}$ then the isogeny

$$\phi_{\mathfrak{a}}\colon E_{\mathfrak{b}} \to E_{\mathfrak{c}} = \mathfrak{a}E_{\mathfrak{b}}$$

induced by the inclusion $\mathfrak{b} \subseteq \mathfrak{c}$ corresponds to the action of $\mathfrak{a}$ on $E_{\mathfrak{b}}$.

Now $\mathrm{Ell}_{\mathcal{O}}(\mathbb{C})$ is a $\mathrm{cl}(\mathcal{O})$-torsor. Thus all elliptic curves $E/\mathbb{C}$ with CM by $\mathcal{O}$ are isogenous, and every isogeny between two such E has the form $E_{\mathfrak{b}} \to \mathfrak{a}E_{\mathfrak{b}}$.

Isogeny kernels

Definition

Let E/k be any elliptic curve with CM by an imaginary quadratic order $\mathcal{O}$, and let $\mathfrak{a}$ be an $\mathcal{O}$-ideal. The $\mathfrak{a}$-*torsion subgroup* of E is defined by

$$E[\mathfrak{a}] := \{P \in E(\bar{k}) : \alpha(P) = 0 \text{ for all } \alpha \in \mathfrak{a}\},$$

where we are viewing each $\alpha \in \mathfrak{a} \subseteq \mathcal{O} \simeq \mathrm{End}(E)$ as an endomorphism.

Theorem

Let $\mathcal{O}$ be an imaginary quadratic order, let $E/\mathbb{C}$ be an elliptic curve with CM by $\mathcal{O}$, let $\mathfrak{a}$ be an invertible $\mathcal{O}$-ideal, and let $\phi_{\mathfrak{a}}\colon E \to \mathfrak{a}E$ be the corresponding isogeny. Then

(i) $\ker \phi_{\mathfrak{a}} = E[\mathfrak{a}]$;

(ii) $\deg \phi_{\mathfrak{a}} = \mathrm{N}\mathfrak{a}$.

Proof. *To the board!*

Imaginary quadratic discriminants

Definition

Let $\mathcal{O} = [1, \tau]$ be an imaginary quadratic order. The discriminant of $\mathcal{O}$ is the discriminant of the minimal polynomial of τ, which we can compute as

$$\operatorname{disc}(\mathcal{O}) = (\tau + \bar{\tau})^2 - 4\tau\bar{\tau} = (\tau - \bar{\tau})^2 = \det \begin{pmatrix} 1 & \tau \\ 1 & \bar{\tau} \end{pmatrix}^2.$$

If A is the area of a fundamental parallelogram of $\mathcal{O}$ then

$$\operatorname{disc}(\mathcal{O}) = (\tau - \bar{\tau})^2 = -4|\operatorname{im}\tau|^2 = -4A^2,$$

thus the discriminant does not depend on our choice of τ, it is intrinsic to the lattice $\mathcal{O}$.

Imaginary quadratic discriminants

Negative integers $D \equiv 0, 1 \bmod 4$ are (imaginary quadratic) discriminants.
If D is not $u^2 D_0$ for some $u > 1$ and $D_0 \equiv 0, 1 \bmod 4$ then D is fundamental.

Theorem

Let D be an imaginary quadratic discriminant. There is a unique imaginary quadratic order $\mathcal{O}$ with $\operatorname{disc}(\mathcal{O}) = D = u^2 D_K$, where D_K is the fundamental discriminant of the maximal order $\mathcal{O}_K$ in $K = \mathbb{Q}(\sqrt{D_K})$, and $u = [\mathcal{O}_K : \mathcal{O}]$.

Proof. *See notes.*

The index $u = [\mathcal{O}_K : \mathcal{O}]$ is the conductor of the order $\mathcal{O}$.

18.783 / 18.7831 Elliptic Curves
Fall 2025