**18.783 Elliptic Curves** **Spring 2017**
**Lecture #17** **04/12/2017**

# 17 Complex multiplication

Over the course of the last two lectures we established a one-to-one correspondence between lattices $L \subseteq \mathbb{C}$ (up to homethety) and elliptic curves $E/\mathbb{C}$ (up to isomorphism), given by the map that sends each lattice $L$ to the elliptic curve

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

together with an explicit isomorphism

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

where $\wp(z)$ is the Weierstrass $\wp$-function for the lattice $L$.

To complete our understanding of the categorical equivalence of complex tori and elliptic curves, we want to relate morphisms of complex tori to isogenies of elliptic curves. In particular, we want to be able to explicitly understand how to relate the endomorphism ring of a complex torus to the endomorphism ring of the corresponding elliptic curve.

A complex torus $\mathbb{C}/L$ is both a complex manifold and a group in which the group operations are defined by holomorphic maps (this makes it a complex Lie group). A morphism in the category of complex tori must respect both structures: we require morphisms of complex tori to be holomorphic maps that are also group homomorphisms (just as isogenies are morphisms of algebraic varieties that are also homomorphisms of abelian groups).

## 17.1 Morphisms of complex tori

We have not formally defined what it means to be a holomorphic map of complex manifolds (or even a complex manifold), but for maps $\varphi\colon \mathbb{C}/L_1 \to \mathbb{C}/L_2$ of complex tori it simply means that $\varphi$ is induced by a holomorphic function $f\colon \mathbb{C} \to \mathbb{C}$ that makes the following diagram commute:

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

where $\pi_1$ and $\pi_2$ are quotient maps.[1]

Each $\alpha \in \mathbb{C}$ determines a holomorphic multiplication-by-$\alpha$ map $z \mapsto \alpha z$ that is an endomorphism of $\mathbb{C}$ (as a group under addition). Whenever $\alpha L_1 \subseteq L_2$ this induces a group homomorphism

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

that is also a holomorphic map of complex manifolds.

Remarkably, every morphism of complex tori arises in this way. In fact, every holomorphic map that fixes zero arises in this way; this is analogous to the fact that every morphism of elliptic curves that fixes zero is automatically a group homomorphism.

[1] We should note that in general holomorphic maps of complex manifolds are defined locally on charts and need not be induced by a single global map; complex tori are a particularly simple special case.

*Lecture by Andrew Sutherland*

**Theorem 17.1.** *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.* Let $\pi_i\colon \mathbb{C} \to \mathbb{C}/L_i$ be quotient maps and let $f\colon \mathbb{C} \to \mathbb{C}$ be a holomorphic function for which $\varphi(\pi_1(z)) = \pi_2(f(z))$. For all $z \in \mathbb{C}$ and $\omega \in L_1$ we have

$$\pi_2(f(z+\omega)) = \varphi(\pi_1(z+\omega)) = \varphi(\pi_1(z)) = \pi_2(f(z)),$$

thus $f(z+\omega) - f(z) \in \ker \pi_2 = L_2$. For each $\omega \in L$ the function $g_\omega(z) := f(z+\omega) - f(z)$ is a continuous map from the connected set $\mathbb{C}$ to a discrete set $L_2$; its image must be connected and therefore consists of a single point. It follows that $g_\omega(z)$ is constant and $g_\omega'(z) = 0$, which implies that $f'(z+\omega) = f'(z)$ for all $z \in \mathbb{C}$ and $\omega \in L_1$. Thus $f'(z)$ is periodic with respect to $L_1$ and is therefore a holomorphic elliptic function, hence constant (see Remark 15.10).

It follows that $f(z) = \alpha z + \beta$, for some $\alpha, \beta \in \mathbb{C}$, and $\pi_2(f(0)) = \varphi(\pi_1(0)) = \varphi(0) = 0$, so $\beta = f(0) \in L_2$ and $\alpha L_1 \subseteq L_2$. For all $z \in \mathbb{C}$ we have $\varphi(\pi_1(z)) = \pi_2(f(z) = \pi_2(\alpha z)$, thus $\varphi = \varphi_\alpha$. The value of $\alpha$ is unique: if $\varphi = \varphi_\gamma$ for some $\gamma \in \mathbb{C}$ then $(\alpha - \gamma)z \in L_2$ for all $z \in \mathbb{C}$, which implies $\alpha - \gamma = ((\alpha-\gamma)z)' = 0$ (as argued above), and therefore $\gamma = \alpha$. □

As noted above, a morphism $\varphi\colon \mathbb{C}/L_1 \to \mathbb{C}/L_2$ of complex tori is a holomorphic map that is also a group homomorphism; in particular, $\varphi(0) = 0$, so Theorem 17.1 applies and we have the following corollary.

**Corollary 17.2.** *For any two lattices $L_1, L_2 \subseteq \mathbb{C}$ the map*

$$\begin{gathered}\bigl\{\alpha \in \mathbb{C} : \alpha L_1 \subseteq L_2\bigr\} \to \bigl\{\text{morphisms } \varphi\colon \mathbb{C}/L_1 \to \mathbb{C}/L_2\bigr\}\\ \alpha \mapsto \varphi_\alpha\end{gathered}$$

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

The set $\{\alpha \in \mathbb{C} : \alpha L_1 \subseteq L_2\}$ on the LHS contains 0 and is closed under addition and negation and is thus an additive subgroup of $\mathbb{C}$, and if $L_1 = L_2$ it is also closed under multiplication and forms a subring of $\mathbb{C}$. The set of morphism on the RHS, which we could have written as $\operatorname{Hom}(\mathbb{C}/L_1, \mathbb{C}/L_2)$, is an additive group under pointwise addition, and when $L_1 = L_2$ it is the endomorphism ring $\operatorname{End}(\mathbb{C}/L_1)$ with multiplication given by composition.

*Proof.* Theorem 17.1 gives us a bijection of sets, we just need to check that it is a group/ring homomorphism. For $i = 1, 2$, let $\pi_i\colon \mathbb{C} \to \mathbb{C}/L_i$ be the projection maps as above. If $\alpha L_1 \subseteq L_2$ and $\beta L_1 \subseteq L_2$ then for all $z \in \mathbb{C}$ we have

$$\varphi_{\alpha+\beta}(\pi_1(z)) = \pi_2((\alpha+\beta)z) = \pi_2(\alpha z) + \pi_2(\beta z) = \varphi_\alpha(\pi_1(z)) + \varphi_\beta(\pi_1(z)) = (\varphi_\alpha + \varphi_\beta)(\pi_1(z)),$$

thus the map $\alpha \mapsto \varphi_\alpha$ defines a homomorphism of additive groups. If $L_1 = L_2$ and we put $\pi = \pi_1 = \pi_2$ then we also have

$$\varphi_{\alpha\beta}(\pi(z)) = \pi(\alpha\beta z) = \varphi_\alpha(\pi(\beta z)) = \varphi_\alpha(\varphi_\beta(\pi(z)) = (\varphi_\alpha\varphi_\beta)(\pi(z)),$$

which shows that $\alpha \mapsto \varphi_\alpha$ is a ring homomorphism. □

We will henceforth identify $\operatorname{Hom}(\mathbb{C}/L_1, \mathbb{C}/L_2)$ with $\{\alpha \in \mathbb{C} : \alpha L_1 \subseteq L_2\}$ and $\varphi_\alpha$ with $\alpha$; we thus view any $\alpha$ for which $\alpha L_1 \subseteq L_2$ both as a complex number and a morphism $\mathbb{C}/L_1 \to \mathbb{C}/L_2$. We will also freely use $z \in \mathbb{C}$ to denote its image under the quotient map $\pi_1\colon \mathbb{C} \to \mathbb{C}/L_1$ and use $\alpha z$ to denote $\varphi_\alpha(\pi_1(z) = \pi_2(\alpha z)$ whenever the context is clear.

## 17.2 Morphisms of complex tori and isogenies of elliptic curves over $\mathbb{C}$

Let $L_1, L_2 \subseteq \mathbb{C}$ be lattices. In order to complete the proof that complex tori and elliptic curves over $\mathbb{C}$ are equivalent categories, we need to give an explicit isomorphism $\operatorname{Hom}(\mathbb{C}/L_1, \mathbb{C}/L_2) \simeq \operatorname{Hom}(E_{L_1}, E_{L_2})$. To do this we need to first prove a lemma about fields of elliptic functions.

Recall that the set of all elliptic functions for a given lattice $L$ forms a field $\mathbb{C}(L)$ that includes the constant functions $\mathbb{C} \subseteq \mathbb{C}(L)$. We now show that the extension $\mathbb{C}(L)/\mathbb{C}$ is generated by the Weierstrass $\wp$-function and its derivative, and the subfield $\mathbb{C}(L)^{\text{even}}$ of even functions (the $f \in \mathbb{C}(L)$ for which $f(-z) = f(z)$) is generated by the $\wp$-function alone.

**Lemma 17.3.** *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.* Every $f \in \mathbb{C}(L)$ can be written as the sum of an even function and an odd function:

$$f(z) = \frac{f(z) + f(-z)}{2} + \frac{f(z) - f(-z)}{2}.$$

Any odd function $g \in \mathbb{C}(L)$ can be written as

$$g(z) = \frac{g(z)}{\wp'(z)}\wp'(z),$$

where $g(z)/\wp'(z)$ is an even function; thus (i) follows from (ii).

We now show that (ii) follows from (iii). Let $f \in \mathbb{C}(L)^{\text{even}}$ and let $m$ be the number of poles of $f$ that lie in $\mathcal{F}_0 - \{0\}$, where $\mathcal{F}$ is the standard fundamental parallelogram for $L$. The integer $m$ is a nonnegative and bounded by the order of $f$. If $m > 0$ then $f(z)$ has a pole at some nonzero $w \in \mathcal{F}_0$, say of order $n$. Now consider the even elliptic function

$$g(z) := (\wp(z) - \wp(w))^n,$$

which is holomorphic on $\mathbb{C} - L$ and has a zero of order at least $n$ at $w$. The function $gf \in \mathbb{C}(L)^{\text{even}}$ is holomorphic at $w$, and every pole of $gf$ in $\mathbb{C} - L$ must be a pole of $f$, so it has strictly fewer than $m$ poles in $\mathcal{F}_0 - \{0\}$. Repeating this process $m$ times yields a polynomial $Q \in \mathbb{C}[x]$ such that $Q(\wp)f \in \mathbb{C}(L)^{\text{even}}$ is holomorphic on $\mathbb{C} - L$; If we assume (iii), then $\mathbb{Q}(\wp)f = P(\wp)$ for some $P \in C[x]$ and $f = Q(\wp)/P(\wp) \in \mathbb{C}(\wp)$, implying (ii).

We now prove (iii). Let $f \in \mathbb{C}(L)^{\text{even}}$ be nonzero and holomorphic on $\mathbb{C} - L$. If the order of $f$ is zero then $f$ is constant (by Liouville's theorem, since an elliptic function is necessarily bounded). Otherwise $f$ must have a pole at 0 and its Laurent series expansion at 0 has the form

$$f(z) = \sum_{k=-n}^{\infty} a_{2k} z^{2k},$$

with $a_{-2n} \neq 0$, where $2n$ is order of $f$ (which must be even). The function

$$f(z) - a_{-2n}\wp^n(z)$$

is an even elliptic function holomorphic on $\mathbb{C} - L$ of order at most $2(n-1)$. Repeating this at most $n$ times yields a polynomial $P \in \mathbb{C}[x]$ such that $f - P(\wp) \in \mathbb{C}$, and (iii) follows. □

**Theorem 17.4.** *For $i = 1, 2$ let $L_i \subseteq \mathbb{C}$ be a lattice, let $E_i := E_{L_i}$ be the corresponding elliptic curve,define $\wp_i(z) := \wp(z; L_i)$, and let $\Phi_i \colon \mathbb{C}/L_i \to E_i(\mathbb{C})$ be the isomorphism that sends $z \notin L_i$ to $(\wp_i(z), \wp_i'(z))$ and $z \in L_i$ to $0$. For any $\alpha \in \mathbb{C}$, the following are equivalent:*

(1) *$\alpha L_1 \subseteq L_2$;*

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

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

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

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

*Proof.* Properties (1)–(3) clearly hold for $\alpha = 0$, so we assume $\alpha \neq 0$.

(1) $\Rightarrow$ (2): Let $\omega \in L_1$. We have $\wp_2(\alpha(z + \omega)) = \wp_2(\alpha z + \alpha\omega) = \wp_2(\alpha z)$. Thus $\wp_2(\alpha z)$ is periodic with respect to $L_1$, and it is meromorphic, so it is an elliptic function for $L_2$. It is an even function, so it is a rational function $u(\wp_1(z))/v(\wp_1(z))$ of $\wp_1(z)$, by Lemma 17.3.

(2) $\Rightarrow$ (3): Let $\wp_2(\alpha z) = u(\wp_1(z))/v(\wp_1(z))$ and define

$$\phi_\alpha := \left(\frac{u(x)}{v(x)}, \frac{s(x)}{t(x)}y\right),$$

where $u, v \in \mathbb{C}[x]$ are given by (2) and $s := (u'v - v'u)$ and $t := \alpha v^2$, so that

$$\wp_2'(\alpha z) = \frac{1}{\alpha}(\wp_2(\alpha z))' = \frac{1}{\alpha}\left(\frac{u(\wp_1(z))}{v(\wp_1(z)}\right)' = \frac{s(\wp_1(z))}{t(\wp_1(z))}\wp_1'(z).$$

We then have

$$\phi_\alpha(\Phi_1(z)) = \phi_\alpha(\wp_1(z), \wp_1'(z) = \left(\frac{u(\wp_1(z))}{v(\wp_1(z))}, \frac{s(\wp_1(z))}{t(\wp_1(z))}\wp_1'(z)\right) = (\wp_2(\alpha z), \wp_2'(\alpha z)) = \Phi_2(\alpha z),$$

so the diagram in (3) commutes. If $\phi \in \operatorname{Hom}(E_1, E_2)$ also satisfies $\phi(\Phi_1(z)) = \Phi_2(\alpha z)$ then

$$(\phi - \phi_\alpha)(\Phi_1(z)) = \phi(\Phi_1(z)) - \phi_\alpha(\Phi_1(z)) = \Phi_2(\alpha z) - \Phi_2(\alpha z) = 0,$$

and $\phi = \phi_\alpha$; thus $\phi_\alpha$ is the only element of $\operatorname{Hom}(E_1, E_2)$ that makes the diagram commute.

(3) $\Rightarrow$ (1): For all $\omega \in L_1$ we have $\Phi_2(\alpha\omega) = \phi_\alpha(\Phi_1(\omega)) = \phi_\alpha(0) = 0$, which implies $\alpha\omega \in L_2$, thus $\alpha L_1 \subseteq L_2$.

For any $\phi \in \operatorname{Hom}(E_1, E_2)$, the map $\Phi_2^{-1} \circ \phi \circ \Phi_1$ is an element of $\operatorname{Hom}(\mathbb{C}/L_1, \mathbb{C}/L_2)$ and is therefore induced by the multiplication-by-$\alpha$ map $\alpha \to \alpha z$ for a unique $\alpha = \alpha_\phi$ satisfying $\alpha L_1 \subseteq L_2$, by Corollary 17.2. The maps $\alpha \mapsto \phi_\alpha$ and $\phi \mapsto \alpha_\phi$ are thus inverse bijections.

We now show that the map $\Psi\colon \operatorname{Hom}(E_1, E_2) \to \{\alpha \in \mathbb{C} : \alpha L_2 \subseteq L_2\}$ defined by $\phi \mapsto \alpha_\phi$ is a group homomorphism. We have $\Psi(0) = 0$, and for all $\phi_1, \phi_2 \in \operatorname{Hom}(E_1, E_2)$

$$\Psi(\phi_1 + \phi_2) \;=\; \Phi_2^{-1} \circ (\phi_1 + \phi_2) \circ \Phi_1 \;=\; \Phi_2^{-1} \circ \phi_1 \circ \Phi_1 + \Phi_2^{-1} \circ \phi_2 \circ \Phi_1 \;=\; \Psi(\phi_1) + \Psi(\phi_2).$$

Thus $\Psi$ is a group homomorphism and therefore an isomorphism, since it is a bijection. □

## 17.3 Endomorphism rings of complex tori and elliptic curves over $\mathbb{C}$

We now specialize to the case $L = L_2 = L_1$, and put $E = E_L$, in which case the group $\{\alpha \in \mathbb{C}\colon \alpha L_{\subseteq} L\} \simeq \operatorname{Hom}(E, E) = \operatorname{End}(E)$ is also a ring.

**Corollary 17.5.** *Let $L \subseteq \mathbb{C}$ be a lattice and let $E := E_L$. The maps $\alpha \mapsto \phi_\alpha$ and $\phi \to \alpha_\phi$ are inverse ring isomorphisms between $\{\alpha \in \mathbb{C} : \alpha L \subseteq L\}$ and $\operatorname{End}(E)$, the involution $\phi \mapsto \hat{\phi}$ of $\operatorname{End}(E)$ corresponds to complex conjugation $\alpha \mapsto \bar{\alpha}$ in $\{\alpha \in \mathbb{C} : \alpha L \subseteq L\}$, and we have $\mathrm{T}(\alpha) := \alpha + \bar{\alpha} = \operatorname{tr}\phi_\alpha$ 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 (2) of Theorem 17.4.*

*Proof.* Let $\Phi\colon \mathbb{C}/L \to E(\mathbb{C})$ and $\Psi\colon \operatorname{End}(E) \to \{\alpha \in \mathbb{C} : \alpha L \subseteq L\}$ be as in Theorem 17.4 and its proof (so $\Psi(\phi) = \alpha_\phi$); they are both group isomorphisms. For $\phi_1, \phi_2 \in \operatorname{End}(E)$ we have

$$\Psi(\phi_1\phi_2) \;=\; \Phi^{-1} \circ (\phi_1 \circ \phi_2) \circ \Phi \;=\; (\Phi^{-1} \circ \phi_1 \circ \Phi) \circ (\Phi^{-1} \circ \phi_2 \circ \Phi) \;=\; \Psi(\phi_1)\Psi(\phi_2),$$

thus $\Psi$ is a ring homomorphism and therefore a ring isomorphism, since it is a bijection.

For any $\phi \in \operatorname{End}(E)$, the complex number $\alpha := \alpha_\phi$ satisfies the characteristic equation

$$x^2 - (\operatorname{tr}\phi)x + \deg\phi = 0,$$

which has integer coefficients and discriminant $\operatorname{tr}(\phi)^2 - 4\deg(\phi) \le 0$. Thus $\alpha \in \mathbb{Z}$ or $\alpha$ is an algebraic integer in an imaginary quadratic field, and in either case its complex conjugate $\bar{\alpha}$ satisfies the same quadratic equation and we have $\bar{\alpha}\alpha = \deg\phi = \hat{\phi}\phi$, which implies $\bar{\alpha} = \hat{\phi}$ ($\{\alpha \in \mathbb{C}\colon \alpha L \subseteq L\} \simeq \operatorname{End}(E)$ has no zero divisors, so the cancellation law applies), and we have $\mathrm{T}(\alpha) = \alpha + \bar{\alpha} = \phi + \hat{\phi} = \operatorname{tr}\phi$ and $\mathrm{N}(\alpha) = \alpha\bar{\alpha} = \phi\hat{\phi} = \deg\phi$.

Finally, for any $\alpha \in \{\alpha \in \mathbb{C} : \alpha L \subseteq L\}$ we can apply (2) in Theorem 17.4 to write write $v(\wp(z))\wp(\alpha z) = u(\wp(z))$ for some $u, v \in \mathbb{C}[x]$. The functions $u(\wp(z))$ and $v(\wp(z))$ have poles of order $2\deg u$ and $2\deg v$ at 0, respectively, while $\wp(\alpha z)$ has a pole of order 2 at 0, so we must have $\deg u = \deg v + 1$ and

$$\deg\phi = \max(\deg u, \deg v) = \deg u = \deg v + 1,$$

where $\phi = \phi_\alpha := \left(\frac{u(x)}{v(x)}, \frac{s(x)}{t(x)}y\right)$ is as in the proof of Theorem 17.4. □

**Remark 17.6.** Theorem 17.4 and Corollary 17.5 explain the origin of the term *complex multiplication* (CM). When $\operatorname{End}(E_L)$ is bigger than $\mathbb{Z}$ the extra endomorphisms in $\operatorname{End}(E_L)$ all correspond to multiplication-by-$\alpha$ maps in $\operatorname{End}(\mathbb{C}/L)$, for some $\alpha \in \mathbb{C} - \mathbb{R}$ that is an algebraic integer in an imaginary quadratic field.

**Corollary 17.7.** *Let $E$ be an elliptic curve defined over $\mathbb{C}$. Then $\operatorname{End}(E)$ is commutative and therefore isomorphic to either $\mathbb{Z}$ or an order in an imaginary quadratic field.*

*Proof.* Let $L$ be the lattice corresponding to $E$. The ring $\operatorname{End}(E) \simeq \{\alpha \in \mathbb{C} : \alpha L \subseteq L\}$ is clearly commutative, and therefore not an order in a quaternion algebra. The result then follows from our classification of endomorphism rings of elliptic curves in Lecture 13. □

**Remark 17.8.** Corollary 17.7 applies to elliptic curves over $\mathbb{Q}$, number fields, or any field that can be embedded in $\mathbb{C}$. It can be extended to all fields of characteristic 0 via the Lefschetz principle; see [1, Thm. VI.6.1].

## 17.4 Elliptic curves with a given endomorphism ring

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

$$\operatorname{End}(E_L) \simeq \{\alpha \in \mathbb{C} : \alpha L \subseteq L\} \simeq \operatorname{End}(\mathbb{C}/L). \tag{1}$$

As noted above, we have been treating the isomorphism on the right 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 $\mathbb{C}$. Once we have done this, provided that we regard $\operatorname{End}(E_L)$ as a subring of $\operatorname{End}^0(E_L)$ (via the canonical injection $\phi \mapsto \phi \otimes 1$), we actually have an equality $\operatorname{End}(E_L) = \{\alpha \in \mathbb{C} : \alpha L \subseteq L\}$; moreover, when $\operatorname{End}(\mathbb{C}/L)$ is an imaginary quadratic order $\mathcal{O}$, we can choose the embedding of $\operatorname{End}^0(E_L)$ into $\mathbb{C}$ so that each multiplication-by-$\alpha$ endomorphism of $\mathbb{C}/L$ is identified with $\phi_\alpha \in \operatorname{End}(E_L)$ (as opposed to $\hat{\phi}_\alpha$). This is known as the *normalized identification* of $\operatorname{End}(E_L)$ with $\operatorname{End}(\mathbb{C}/L) = \mathcal{O}$, which we henceforth assume.

We now want to focus on the CM case, where $\operatorname{End}(E_L)$ is an order $\mathcal{O}$ in an imaginary quadratic field $K$. The order $\mathcal{O}$ is a lattice, and we would like to understand how the lattices $L$ and $\mathcal{O}$ are related. In particular, for which lattices $L$ do we have $\operatorname{End}(E_L) = \mathcal{O}$?

An obvious candidate is $L = \mathcal{O}$. If $\alpha \in \operatorname{End}(E_{\mathcal{O}})$, then $\alpha\mathcal{O} \subseteq \mathcal{O}$ and therefore $\alpha \in \mathcal{O}$, since the ring $\mathcal{O}$ contains 1. Conversely, if $\alpha \in \mathcal{O}$, then $\alpha\mathcal{O} \subseteq \mathcal{O}$, since $\mathcal{O}$ is closed under multiplication, and therefore $\alpha \in \operatorname{End}(E_{\mathcal{O}})$; 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). The question now before us is this: are there any lattices $L$ not homothetic to $\mathcal{O}$ for which we have $\operatorname{End}(E_L) = \mathcal{O}$?

Given that we are only considering lattices up to homethety, we may assume without loss of generality that $L = [1, \tau]$, and we can always write $\mathcal{O} = [1, \omega]$ for some imaginary quadratic integer $\omega$. If $\operatorname{End}(E_L) = \mathcal{O}$, then we must have $\omega \cdot 1 = \omega \in L$, so $\omega = m + n\tau$, for some $m, n \in \mathbb{Z}$. Thus $nL = [n, \omega - m] = [n, \omega]$, which means that $L$ is homothetic to a sublattice of $\mathcal{O}$ (of index $n$). This sublattice must be closed under multiplication by $\mathcal{O}$, which implies that $L$ is homothetic to an $\mathcal{O}$-ideal (recall that an $\mathcal{O}$-ideal is an additive subgroup of $\mathcal{O}$ closed under multiplication by $\mathcal{O}$, equivalently, any $\mathcal{O}$-submodule of $\mathcal{O}$).

But the situation is a bit more complicated than it appears, for two reasons. First, two sublattices $[m, \omega]$ and $[n, \omega]$ of $\mathcal{O}$ may be homothetic even when $m \neq n$. For example, if $\mathcal{O} = \mathbb{Z}[i]$ and $\omega = i$, then

$$(1 + i)[m, i] = [m + mi, i - 1] = [2m, 2mi] = 2m[1, i],$$

so $[m, i] = \frac{2m}{1+i}[1, i]$ is homothetic to $\mathcal{O}$, as is $[n, i] = \frac{2n}{1+i}[1, i]$.

The second complication is that while every lattice $L$ for which $\operatorname{End}(E_L) = \mathcal{O}$ 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 $L$, it is clear that the set

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

is an order in $K$: note that $\mathcal{O} \subseteq \mathcal{O}(L) = \operatorname{End}(E_L)$, since the $\mathcal{O}$-ideal $L$ is closed under multiplication by $\mathcal{O}$, and this implies that $\operatorname{End}^0(E_L) = K$. But it is not necessarily true that $\mathcal{O}(L)$ is equal to $\mathcal{O}$; if $\mathcal{O} \neq \mathcal{O}_K$ we can always find an $\mathcal{O}$-ideal $L$ for which $\mathcal{O}(L)$ strictly contains $\mathcal{O}$ (see Problem Set 9). This motivates the following definition.

**Definition 17.9.** 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 $\mathcal{O}(L) = \mathcal{O}$.

Given that we are only interested in lattices up to homethety, we shall regard two $\mathcal{O}$-ideals as *equivalent* if they are homothetic as lattices. A homethety $L' = \lambda L$ between lattices that are $\mathcal{O}$-ideals can always be written with $\lambda = a/b$ for some $a, b \in \mathcal{O}$. To see this, note that if $L = [\omega_1, \omega_2]$ then we can take $\alpha = \lambda\omega_1 \in \mathcal{O}$ and $\beta = \omega_1$. Thus homothetic $\mathcal{O}$-ideals $L$ and $L'$ always satisfy an equation $\alpha L = \beta L'$ for some $\alpha, \beta \in \mathcal{O}$. This motivates the following definition.

**Definition 17.10.** Let $\mathcal{O}$ be an order in an imaginary quadratic field $K$ Two $\mathcal{O}$-ideals $\mathfrak{a}$ and $\mathfrak{b}$ are said to be *equivalent* if they are homothetic as lattices, equivalently, $\mathfrak{a} = \beta\mathfrak{b}$ for some nonzero $\alpha, \beta \in \mathcal{O}$; we can also write this as $(\alpha)\mathfrak{a} = (\beta)\mathfrak{b}$, where $(\alpha)$ and $(\beta)$ denote principal ideals and $(\alpha)\mathfrak{a}$ and $(\beta)\delta$ are products of ideals.

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 $a_1b_1, a_1b_2, a_2b_1, a_2b_2$. Since $\mathfrak{ab}$ is an additive subgroup of $\mathcal{O}$, it is necessarily a free $\mathbb{Z}$-module of rank 2 and can be written as a lattice $[c_1, c_2]$, where $c_1$ and $c_2$ are $\mathcal{O}$-linear combinations of $a_1b_1, a_1b_2, a_2b_1, a_2b_2$. Note that ideal multiplication respects equivalence:

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

**Definition 17.11.** Let $\mathcal{O}$ be an order in an imaginary quadratic field. The *ideal class group* $\operatorname{cl}(\mathcal{O})$ is the multiplicative group of equivalence classes of proper $\mathcal{O}$-ideals.

It is not *a priori* clear that the set $\operatorname{cl}(\mathcal{O})$ is actually a group. It is clearly closed under an associative multiplication and contains an identity element (the class of principal ideals), hence an abelian monoid, but it is not obvious that every element has an inverse. We will give an explicit proof of this in the next lecture (See Problem Set 9 for an alternative proof that also shows that $\operatorname{cl}(\mathcal{O})$ is finite). Even without necessarily knowing that $\operatorname{cl}(\mathcal{O})$ is a group, our discussion above makes the following proposition clear.

**Theorem 17.12.** *Let $\mathcal{O}$ be an order in an imaginary quadratic field. There is a one-to-one correspondence between elements of the ideal class group* $\operatorname{cl}(\mathcal{O})$ *and homethety classes of lattices $L \subseteq \mathbb{C}$ for which* $\operatorname{End}(E_L) \simeq \mathcal{O}$.

## References

[1] J.H. Silverman, *The arithmetic of elliptic curves*, second edition, Springer 2009.