18 The CM torsor

Over the course of the last three lectures we have established an equivalence of categories between complex tori $\mathbb{C}/L$ and elliptic curves $E/\mathbb{C}$:

$$\{\text{lattices } L \subseteq \mathbb{C}\} / \sim \longrightarrow \{\text{elliptic curves } E/\mathbb{C}\} / \sim$$

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

$$j(L) = j(E_L)$$

in which homothetic lattices correspond to isomorphic elliptic curves, and we have established ring isomorphisms

$$\text{End}(\mathbb{C}/L) \simeq \mathcal{O}(L) \simeq \text{End}(E_L)$$

where the ring

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

is necessarily equal to $\mathbb{Z}$ or an order $\mathcal{O}$ in an imaginary quadratic field. In the latter case, which we will assume throughout this lecture, the elliptic curve $E_L$ is said to have complex multiplication (CM) by $\mathcal{O}$, and the lattice $L$ is necessarily homothetic to an $\mathcal{O}$-ideal.

If we fix the order $\mathcal{O}$, the $\mathcal{O}$-ideals $L$ for which $\text{End}(E_L) \simeq \mathcal{O}$ are precisely those for which $\mathcal{O}(L) = \mathcal{O}$; in the previous lecture we defined such $\mathcal{O}$-ideals to be proper. Note that $\mathcal{O} \subseteq \mathcal{O}(L)$ always holds, since $L$ is an $\mathcal{O}$-ideal, but in general $\mathcal{O}(L)$ be be larger than $\mathcal{O}$.

The sets

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

are both in bijection with the ideal class group

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

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

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

and the group operation is given by multiplying representative ideals. As noted in the previous lecture it is not immediately obvious that $\text{cl}(\mathcal{O})$ is a group (associativity is clear but the existence of inverses is not); one of our first goals is to prove this.

**Remark 18.1.** Recall that that an order in a $\mathbb{Q}$-algebra $K$ of dimension $r$ is a subring of $K$ that is also a free $\mathbb{Z}$-module of rank $r$; see Definition 13.22. When $K$ is an imaginary quadratic field embedded in the complex numbers, every order $\mathcal{O}$ in $K$ is automatically a lattice in $\mathbb{C}$, since in this case $r = \dim K = 2$ and $K$ is not contained in $\mathbb{R}$. Not every lattice in $\mathbb{C}$ is an imaginary quadratic order, but every imaginary quadratic order $\mathcal{O}$ is a lattice in $\mathbb{C}$ (once we fix an embedding of its fraction field), as is every $\mathcal{O}$-ideal (as a free $\mathbb{Z}$-module an $\mathcal{O}$-ideal must have the same rank as $\mathcal{O}$ because it is closed under multiplication by $\mathcal{O}$). Notice that the equivalence relation we have defined on $\mathcal{O}$-ideals coincides with our notion of homothety for lattices.

Recalling that isomorphism classes of elliptic curves over an algebraically closed field are identified by their $j$-invariants, we now define the set

$$\text{Ell}_\mathcal{O}(\mathbb{C}) = \{j(E) : E \text{ is defined over } \mathbb{C} \text{ and } \text{End}(E) = \mathcal{O}\},$$

**Lecture by Andrew Sutherland**
and we then have a bijection of sets
\[ \text{cl}(\mathcal{O}) \xrightarrow{\sim} \text{Ell}_\mathcal{O}(\mathbb{C}) \]
\[ [a] \mapsto j(E_a) = j(a). \]

As you will prove in Problem Set 9, the ideal class group \( \text{cl}(\mathcal{O}) \) is finite, thus the set \( \text{Ell}_\mathcal{O}(\mathbb{C}) \) is finite. Its cardinality is the \textit{class number} \( h(\mathcal{O}) = \# \text{cl}(\mathcal{O}) \). Remarkably, not only are the sets \( \text{cl}(\mathcal{O}) \) and \( \text{Ell}_\mathcal{O}(\mathbb{C}) \) in bijection, the set \( \text{Ell}_\mathcal{O}(\mathbb{C}) \) admits a group action by \( \text{cl}(\mathcal{O}) \). In order to define this action, and to gain a better understanding of what it means for an \( \mathcal{O} \)-ideal to be proper, we first introduce the notion of a fractional \( \mathcal{O} \)-ideal.

### 18.1 Fractional ideals

**Definition 18.2.** Let \( \mathcal{O} \) be an integral domain with fraction field \( K \). For any \( \lambda \in K^\times \) and \( \mathcal{O} \)-ideal \( a \), the \( \mathcal{O} \)-module \( b = \lambda a := \{ \lambda \alpha : \alpha \in a \} \) is called a \textit{fractional} \( \mathcal{O} \)-ideal.\footnote{Some authors define fractional \( \mathcal{O} \)-ideals to be finitely generated \( \mathcal{O} \)-submodules of \( K \). Every finitely generated \( \mathcal{O} \)-module in \( K \) is a fractional ideal under our definition, and when \( \mathcal{O} \) is noetherian (which applies to orders in number fields), the definitions are equivalent.}

Multiplication of fractional ideals \( b = \lambda a \) and \( b' = \lambda a' \) is defined in the obvious way:
\[ bb' := (\lambda \lambda')aa', \]
where \( aa' \) is the product of the \( \mathcal{O} \)-ideals \( a \) and \( a' \).\footnote{One can also add fractional \( \mathcal{O} \)-ideals via \( b + b' := \{ b + b' : b \in b, b' \in b \} \), but we won’t need this.}

Without loss of generality we can assume \( \lambda = 1/\beta \) for some \( \beta \in \mathcal{O} \) (if \( \lambda = \alpha/\beta \), replace \( a \) with \( \alpha a \)), and in the case of interest to us, where \( K \) is a number field, we can assume \( \lambda = 1/b \) for some positive integer \( b \) (if \( f \in \mathbb{Z}[x] \) is the minimal polynomial of \( \beta \) then \( f(\beta) - f(0) \) is divisible by \( \beta \) with \( (f(\beta) - f(0))/\beta = -f(0)/\beta \in \mathcal{O} \), and we can take \( b = \pm f(0) > 0 \)).

Fractional \( \mathcal{O} \)-ideals that lie in \( \mathcal{O} \) are \( \mathcal{O} \)-ideals, and every \( \mathcal{O} \)-ideal is a fractional \( \mathcal{O} \)-ideal. Note that \( \mathcal{O} \) is itself an \( \mathcal{O} \)-ideal, hence a fractional \( \mathcal{O} \)-ideal, and it acts as the multiplicative identity with respect to multiplication of fractional \( \mathcal{O} \)-ideals. Fractional \( \mathcal{O} \)-ideals \( b \) for which there exists a fractional \( \mathcal{O} \)-ideal \( b^{-1} \) such that \( bb^{-1} = \mathcal{O} \) are said to be \textit{invertible}. Not every fractional \( \mathcal{O} \)-ideal is invertible (the zero ideal never is, and in general there may be nonzero fractional \( \mathcal{O} \)-ideals that are not invertible). The set of invertible fractional \( \mathcal{O} \)-ideals form a group under multiplication (this is sometimes called the \textit{ideal group} of \( \mathcal{O} \), even though its elements are fractional \( \mathcal{O} \)-ideals many of which are not \( \mathcal{O} \)-ideals).

### 18.2 Norms

Let \( \mathcal{O} \) be an order in an imaginary quadratic field \( K \). We want to define the norm of fractional \( \mathcal{O} \)-ideal \( b = \lambda a \), a rational number that is the product of the norms of \( \lambda \) and \( a \). We first define the norm of a field element \( \lambda \in K^\times \), and the norm of an \( \mathcal{O} \)-ideal \( a \).

**Definition 18.3.** Let \( K/k \) be a field extension and let \( \lambda \in K^\times \). The multiplication-by-\( \lambda \) map \( K \to K \) is an invertible linear transformation \( M_\lambda \in \text{GL}(K) \) of \( K \) as a \( k \)-vector space. The (field) \textit{norm} and \textit{trace} of \( \lambda \) are defined by
\[ N_{K/k}\lambda := \det M_\lambda \in k^\times \quad \text{and} \quad T_{K/k}\lambda := \text{tr} M_\lambda \in k. \]
One typically computes the norm and trace by fixing a basis for $K$ as a $k$ vector space and writing $M_{\lambda}$ as a matrix using this basis, but the norm and trace of $M_{\lambda}$ do not depend on the choice of basis. When $K$ is a number field and $k = \mathbb{Q}$ it is common to simply write $N := N_{K/\mathbb{Q}}$ and $T := T_{K/\mathbb{Q}}$ when the number field $K$ is clear from context, but note that for $\lambda \in \mathbb{Q}$ we have $N\lambda = \lambda^{[K:\mathbb{Q}]}$ and $T\lambda = [K : \mathbb{Q}]\lambda$, which depend on $K$, not just $\lambda$.

When $K \simeq \text{End}^0(E)$ is an imaginary quadratic field, Definition 18.3 coincides with our definition of the (reduced) norm and trace of an element of $\text{End}^0(E)$ (see Definition 13.6). When $K$ is an imaginary quadratic field embedded in $\mathbb{C}$ we have $N\alpha = \alpha\bar{\alpha}$ and $T\alpha = \alpha + \bar{\alpha}$, where $\bar{\alpha}$ denotes complex conjugation (equivalently, the action of the unique non-trivial element of $\text{Gal}(K/\mathbb{Q})$). Thus in this setting the complex conjugate

$$\bar{\alpha} = T\alpha - \alpha = \hat{\alpha}$$

is the dual of $\alpha \in \text{End}^0(E) = K \hookrightarrow \mathbb{C}$.

**Definition 18.4.** Let $\mathcal{O}$ be an order in a number field $K$ and let $a$ be a nonzero $\mathcal{O}$-ideal. The (absolute) norm of the ideal $a$ is

$$Na := [\mathcal{O} : a] = \#\mathcal{O}/a \in \mathbb{Z}_{>0}.$$  

We can also interpret $Na$ as the ratio of the volumes of fundamental parallelepipeds for $a$ and $\mathcal{O}$, viewed as lattices in the $\mathbb{Q}$-vector space $K$.

We now show that our two definitions of norm agree on principal $\mathcal{O}$-ideals.

**Lemma 18.5.** Let $\alpha$ be a nonzero element of an order $\mathcal{O}$ in a number field $K$. Then

$$N(\alpha) = |Na|,$$

where $(\alpha)$ denotes the principal $\mathcal{O}$-ideal generated by $\alpha$.

**Proof.** The lemma follows from the fact that the determinant of $M_{\alpha} \in \text{GL}(K) \simeq \text{GL}_n(\mathbb{Q})$ can be interpreted as the signed volume of the fundamental parallelepiped of the lattice $(\alpha)$ in the $\mathbb{Q}$-vector space $K \simeq \mathbb{Q}^n$, where $n = [K : \mathbb{Q}]$ is the degree of $K$. Notice that $N(\alpha) = [\mathcal{O} : (\alpha)] = [\mathcal{O} : \alpha\mathcal{O}] = [\mathcal{O}_K : \alpha\mathcal{O}_K]$ depends only on $\alpha$ and $K$, not the order $\mathcal{O}$ (N.B. this holds for principal ideals but not in general). \hfill $\Box$

**Warning 18.6.** Given that the field norm is multiplicative and that we can view the ideal norm as the absolute value of a determinant, it would be reasonable to expect the ideal norm to be multiplicative. **This is not always true.** As an example, consider the ideal $a = [2, 2i]$ in the order $\mathcal{O} = [1, 2i]$, which has norm $Na = [\mathcal{O} : a] = 2$. Then $a^2 = [4, 4i]$ and

$$Na^2 = 8 \neq 2^2 = (Na)^2.$$  

However, as we shall see, the ideal norm is multiplicative when $a$ and $b$ are both proper $\mathcal{O}$-ideals, and when either $a$ or $b$ is a principal ideal.

**Corollary 18.7.** Let $\mathcal{O}$ be an order in a number field, let $\alpha \in \mathcal{O}$ be nonzero, and let $a$ be a nonzero $\mathcal{O}$-ideal. Then

$$N(\alpha a) = N(\alpha)Na.$$

**Proof.** $N(\alpha a) = [\mathcal{O} : \alpha a] = [\mathcal{O} : a][\alpha : \alpha a] = [\mathcal{O} : a][\mathcal{O} : \alpha\mathcal{O}] = NaN(\alpha) = N(\alpha)Na.$ \hfill $\Box$
This allows us to make the following definition.

**Definition 18.8.** Let \( b = \frac{1}{a} \) be a nonzero fractional ideal in an order \( \mathcal{O} \) of a number field, with \( b \in \mathbb{Z}_{>0} \) (as above, we can always write \( b \) this way). The (absolute) **norm** of \( b \) is

\[
Nb := \frac{Na}{Nb} \in \mathbb{Q}_{>0}^x.
\]

Corollary 18.7 ensures that this does not depend on the choice of \( b \) and \( a \).

When \( b \subseteq \mathcal{O} \) we can take \( b = 1 \), in which case this agrees with Definition 18.4.

### 18.3 Proper and invertible fractional ideals

We now return to our original setting, where \( \mathcal{O} \) is an order in an imaginary quadratic field. Extending our terminology for \( \mathcal{O} \)-ideals, for any fractional \( \mathcal{O} \)-ideal \( b \) we define

\[
\mathcal{O}(b) := \{ \alpha : \alpha b \subseteq b \},
\]

and say that \( b \) is **proper** if \( \mathcal{O}(b) = \mathcal{O} \). In this section we will show that \( b \) is proper if and only if it is invertible (there is a fractional \( \mathcal{O} \)-ideal \( b^{-1} \) for which \( bb^{-1} = \mathcal{O} \)). Let us first note that for \( b = \lambda a \), whether \( b \) is proper or invertible depends only on the \( \mathcal{O} \)-ideal \( a \).

**Lemma 18.9.** Let \( \mathcal{O} \) be an order in an imaginary quadratic field, let \( a \) be a nonzero \( \mathcal{O} \)-ideal, and let \( b = \lambda a \) be a fractional \( \mathcal{O} \)-ideal. Then \( a \) is proper if and only if \( b \) is proper, and \( a \) is invertible if and only if \( b \) is invertible.

**Proof.** For the first statement, note that \( \{ \alpha : \alpha b \subseteq b \} = \{ \alpha : \alpha \lambda a \subseteq \lambda a \} = \{ \alpha : \alpha a \subseteq a \} \).

For the second, if \( a \) is invertible then \( b^{-1} = \lambda^{-1} a^{-1} \), and if \( b \) is invertible then \( a^{-1} = \lambda b^{-1} \), since \( aa^{-1} = a\lambda b^{-1} = bb^{-1} = \mathcal{O} \).

We now prove that the invertible \( \mathcal{O} \)-ideals are precisely the proper \( \mathcal{O} \)-ideals and give an explicit formula for the inverse when it exists. Our proof follows the presentation in [1, §7].

**Theorem 18.10.** Let \( \mathcal{O} \) be an order in an imaginary quadratic field and let \( a = [\alpha, \beta] \) be an \( \mathcal{O} \)-ideal. Then \( a \) is proper if and only if \( a \) is invertible. Whenever \( a \) is invertible we have \( a\bar{a} = (Na) \), where \( \bar{a} = [\bar{\alpha}, \bar{\beta}] \) and \( (Na) \) is the principal \( \mathcal{O} \)-ideal generated by the integer \( Na \); the inverse of \( a \) is then the fractional \( \mathcal{O} \)-ideal \( a^{-1} = \frac{1}{Na}\bar{a} \).

**Proof.** If \( a \) is invertible, then for any \( \gamma \in \mathbb{C} \) we have

\[
\gamma a \subseteq a \implies \gamma aa^{-1} \subseteq aa^{-1} \implies \gamma \mathcal{O} \subseteq \mathcal{O} \implies \gamma \in \mathcal{O},
\]

so \( \mathcal{O}(a) \subseteq \mathcal{O} \), and therefore \( a \) is a proper \( \mathcal{O} \)-ideal, since we always have \( \mathcal{O} \subseteq \mathcal{O}(a) \).

We now assume that \( a = [\alpha, \beta] \) is a proper \( \mathcal{O} \)-ideal and show that \( a\bar{a} = (Na) \), which implies \( a^{-1} = \frac{1}{Na}\bar{a} \). Let \( \tau = \beta/\alpha \), so that \( a = a[1, \tau] \), and let \( ax^2 + bx + c \in \mathbb{Z}[x] \) be the minimal polynomial of \( \tau \) made integral by clearing denominators, with \( \alpha > 0 \) minimal. The fractional ideal \([1, \tau]\) is homothetic to \( a \), so \( \mathcal{O}([1, \tau]) = \mathcal{O}(a) = \mathcal{O} \), since \( a \) is proper.

Let \( \mathcal{O} = [1, \omega] \). Then \( \omega \in [1, \tau] \) and \( \omega = m + n\tau \) for some \( m, n \in \mathbb{Z} \); after replacing \( \omega \) with \( \omega - m \), we may assume \( \omega = n\tau \). We also have \( \omega \tau \in [1, \tau] \), since \([1, \tau]\) is an \( \mathcal{O} \)-module, so \( n\tau^2 \in [1, \tau] \), which implies that \( a[n] \), by the minimality of \( a \) (Gauss’s lemma implies that we must have \( \{ f \in \mathbb{Z}[x] : f(\tau) = 0 \} = (ax^2 + bx + c) \)). We also have \( a\tau[1, \tau] \subseteq [1, \tau] \) (since

18.783 Spring 2019, Lecture #18, Page 4
\[
\alpha \tau \text{ and } \alpha \tau^2 = -b\tau + c \text{ lie in } [1, \tau]), \text{ so } \alpha \tau \in \mathcal{O}([1, \tau]) = \mathcal{O} = [1, \alpha \tau], \text{ and we must have } n = a \\
\text{and } \mathcal{O} = [1, \alpha \tau]. \text{ Thus}
\]
\[
N(a) = [\mathcal{O} : a] = [[1, \alpha \tau] : \alpha[1, \tau]] = \frac{1}{a}[[1, \alpha \tau] : \alpha[1, \alpha \tau]] = \frac{1}{a} [\mathcal{O} : \alpha \mathcal{O}] = \frac{N(a)}{a}.
\]
We also have
\[
\alpha \bar{a} = \alpha[1, \tau] \bar{a}[1, \tau] = N(\alpha)[1, \tau, \bar{\tau}, \tau \bar{\tau}].
\]
Using \(a \tau^2 + b\tau + c = 0\), we see that \(\tau + \bar{\tau} = -b/a\), and \(\tau \bar{\tau} = c/a\). We then have
\[
\alpha \bar{a} = N(\alpha)[1, \tau, \bar{\tau}, \tau \bar{\tau}] = \frac{N(\alpha)}{a} [a, a\tau, -b, c] = Na[1, a\tau] = (Na)\mathcal{O} = (Na)
\]
as claimed, where we have used \(\gcd(a, b, c) = 1\) to get \([a, a\tau, -b, c] = [1, a\tau]\), and it follows that \(a^{-1} = \frac{1}{Na}\bar{a}\). \(\square\)

**Corollary 18.11.** The ideal class group \(\text{cl}(\mathcal{O})\) is the group of invertible fractional \(\mathcal{O}\)-ideals modulo its subgroup of principal fractional \(\mathcal{O}\)-ideals (in particular \(\text{cl}(\mathcal{O})\) is a group).

**Proof.** Recall that \(\text{cl}(\mathcal{O}) = \{\text{proper } \mathcal{O}\text{-ideals}\}/\sim\), where \(\sim\) denotes homothety. Let \(G\) be the group of invertible fractional \(\mathcal{O}\)-ideals and \(H\) its subgroup of principal fractional \(\mathcal{O}\)-ideals.

Every invertible fractional \(\mathcal{O}\)-ideal \(\mathfrak{b} = \frac{1}{b} a\) is the product of an invertible principal fractional \(\mathcal{O}\)-ideal \(\frac{1}{b}\) and an invertible \(\mathcal{O}\)-ideal \(a\), by Lemma 18.9. It follows that \(G/H\) consists of all cosets \(aH\), where \(a\) is any invertible, equivalently, proper \(\mathcal{O}\)-ideal (by Theorem 18.10). Every nonzero principal fractional \(\mathcal{O}\)-ideal is invertible, since \((\alpha)^{-1} = (\bar{\alpha}^{-1})\), so \(H\) contains every nonzero principal fractional \(\mathcal{O}\)-ideal and for any two proper/invertible \(\mathcal{O}\)-ideals \(a, b\) we have \(a \sim b\) if and only if \(aH = bH\). It follows that \(\text{cl}(\mathcal{O}) = G/H\). \(\square\)

**Corollary 18.12.** Let \(\mathcal{O}\) be an order in an imaginary quadratic field and let \(a\) and \(b\) be invertible (equivalently, proper) fractional \(\mathcal{O}\)-ideals. Then \(N(ab) = NaNb\).

**Proof.** If \(a = \frac{1}{a'} a'\) and \(b = \frac{1}{b'} b'\) with \(a, b \in \mathbb{Z}_{>0}\) and \(a', b' \subseteq \mathcal{O}\) then \(N(ab) = \frac{Na'a'}{NaNb'}\), so it is enough to consider the case where \(a\) and \(b\) are invertible \(\mathcal{O}\)-ideals. We have
\[
(N(ab)) = ab\bar{a}b = ab\bar{a}b = a\bar{a}b\bar{a} = (Na)(Nb),
\]
and it follows that \(N(ab) = NaNb\), since \(Na, Nb, N(ab) \in \mathbb{Z}_{>0}\). \(\square\)

### 18.4 The action of the ideal class group on CM elliptic curves

Let \(\mathcal{O}\) be an order in an imaginary quadratic field. We are ready to define the action of \(\text{cl}(\mathcal{O})\) on \(\text{Ell}_\mathcal{O}(\mathbb{C}) = \{j(E) : E/\mathbb{C} \text{ with } \text{End}(E) = \mathcal{O}\}\), which we will do by defining an action of proper \(\mathcal{O}\)-ideals on elliptic curves \(E/\mathbb{C}\) with CM by \(\mathcal{O}\) (up to isomorphism).

Every \(E/\mathbb{C}\) with \(\text{End}(E) = \mathcal{O}\) is isomorphic to \(E_b\), for some proper \(\mathcal{O}\)-ideal \(b\). For any proper \(\mathcal{O}\)-ideal \(a\) we define the action of \(a\) on \(E_b\) via
\[
aE_b = E_{a^{-1}b} \tag{1}
\]
(we \(E_{a^{-1}b}\) rather than \(E_{ab}\) because \(ab \subseteq b\) but \(b \subseteq a^{-1}b\)). The action of the equivalence class \([a]\) on the isomorphism class \(j(E_b)\), is then defined by
\[
[a]j(E_b) = j(E_{a^{-1}b}), \tag{2}
\]
18.783 Spring 2019, Lecture #18, Page 5
which we can also write as

\[ [a]j(b) = j(a^{-1}b), \]

which does not depend on the choice of \( a \) and \( b \).

If \( a \) is a nonzero principal \( \mathcal{O} \)-ideal, then the lattices \( b \) and \( a^{-1}b \) are homothetic, and we have \( aE_b \simeq E_b \). Thus the identity element of \( \text{cl}(\mathcal{O}) \) acts trivially on \( \text{Ell}_\mathcal{O}(\mathbb{C}) \). For any proper \( \mathcal{O} \)-ideals \( a, b, \) and \( c \) we have

\[ a(bE_c) = aE_{b^{-1}c} = E_{a^{-1}b^{-1}c} = E_{(ba)^{-1}c} = (ba)c = (ab)E_c. \]

Thus we have a group action of \( \text{cl}(\mathcal{O}) \) on \( \text{Ell}_\mathcal{O}(\mathbb{C}) \).

For any proper \( \mathcal{O} \)-ideals \( a \) and \( b \), we have \([a]j(b) = j(a^{-1}b) = j(b)\) if and only if \( b \) is homothetic to \( a^{-1}b \), by Theorem 16.5, and in this case we have \( ab = \lambda b \) for \( \lambda \in K^\times \), and then \( a = \lambda \mathcal{O} \) is principal. This implies that the action of \( \text{cl}(\mathcal{O}) \) is not only faithful (only the identity fixes every element), it is free (every stabilizer is trivial).

The fact that the sets \( \text{cl}(\mathcal{O}) \) and \( \text{Ell}_\mathcal{O}(\mathbb{C}) \) have the same cardinality implies that the action must also be transitive: if we fix any \( j_0 \in \text{Ell}_\mathcal{O}(\mathbb{C}) \) the images \([a]j_0 \) of \( j_0 \) under the action of each \([a] \in \text{cl}(\mathcal{O}) \) must all be distinct, otherwise the action would not be free; there are only \#\( \text{Ell}_\mathcal{O}(\mathbb{C}) \) = \#\( \text{cl}(\mathcal{O}) \) possibilities, so the \( \text{cl}(\mathcal{O}) \)-orbit of \( j_0 \) is all of \( \text{Ell}_\mathcal{O}(\mathbb{C}) \).

A group action that is both free and transitive is said to be regular. Equivalently, the action of a group \( G \) on a set \( X \) is regular if and only if for all \( x, y \in X \) there is a unique \( g \in G \) for which \( gx = y \). In this situation the set \( X \) is said to be a \( G \)-torsor (or principal homogeneous space) for \( G \). We have thus shown that the set \( \text{Ell}_\mathcal{O}(\mathbb{C}) \) is a \( \text{cl}(\mathcal{O}) \)-torsor.

If we fix a particular element \( x \) of a \( G \)-torsor \( X \), we can then view \( X \) as a group that is isomorphic to \( G \) under the map that sends \( y \in X \) to the unique element \( g \in G \) for which \( gx = y \). Note that this involves an arbitrary choice of the identity element \( x \); rather than thinking of elements of \( X \) as group elements, it is more appropriate to think of the “differences” or “ratios” of elements of \( X \) as group elements. In the case of the \( \text{cl}(\mathcal{O}) \)-torsor \( \text{Ell}_\mathcal{O}(\mathbb{C}) \) there is an obvious choice for the identity element: the isomorphism class \( j(E_\mathcal{O}) \). But when we reduce to a finite field \( \mathbb{F}_q \) and work with the \( \text{cl}(\mathcal{O}) \)-torsor \( \text{Ell}_\mathcal{O}(\mathbb{F}_q) \), as we shall soon do, we cannot readily distinguish the element of \( \text{Ell}_\mathcal{O}(\mathbb{F}_q) \) that corresponds to \( j(E_\mathcal{O}) \), and make an arbitrary choice.

### 18.5 The CM action via isogenies

To better understand the \( \text{cl}(\mathcal{O}) \)-action on \( \text{Ell}_\mathcal{O}(\mathbb{C}) \) we now want to look at isogenies between elliptic curves with CM by \( \mathcal{O} \); but first let us consider the situation more generally.

Let \( \phi : E_1 \to E_2 \) be an isogeny of elliptic curves over \( \mathbb{C} \), and let \( L_1 \) and \( L_2 \) be corresponding lattices, so that \( E_1 = E_{L_1} \) and \( E_2 = E_{L_2} \). By Theorem 17.4, there is a unique \( \alpha = \alpha_\phi \) with \( \alpha L_1 \subseteq L_2 \) such that the following diagram commutes

\[
\begin{array}{ccc}
\mathbb{C}/L_1 & \longrightarrow & \mathbb{C}/L_2 \\
\downarrow & & \downarrow \\
\Phi_1 & \longrightarrow & \Phi_2 \\
\downarrow & & \downarrow \\
E_1(\mathbb{C}) & \longrightarrow & E_2(\mathbb{C}).
\end{array}
\]

As we are only interested in lattices up to homothety and elliptic curves up to isomorphism, we can replace \( L_1 \) with the homothetic lattice \( \alpha L_1 \) and \( E_1 \) by an isomorphic elliptic curve so
that $\alpha = 1$ and the isogeny $\phi$ is induced by the inclusion $L_1 \subseteq L_2$; note that this amounts to composing $\phi$ with an isomorphism and does not change its degree. Up to an isomorphism of elliptic curves and a homothety of lattices, every isogeny $\phi: E_1 \to E_2$ arises from an inclusion of lattices $L_1 \subseteq L_2$. In this situation it is clear what the kernel of $\phi$ is. By commutativity, since $\alpha = 1$, the kernel of $\phi$ consists of the images $\Phi_1(z)$ of points $z \in \mathbb{C}$ for which $\Phi_2(z) = 0$; these are precisely the $z \in L_2$ (which includes $L_1 \subseteq L_2$ but may also include $z \in L_2 - L_1$, since $L_2$ is a finer lattice). We have $\Phi_1(z) = 0$ if and only if $z \in L_1$, and it follows that

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

We are in characteristic zero, so $\phi$ is automatically separable and $\deg \phi = \# \ker \phi = [L_2 : L_1]$.

The discussion above applies to any isogeny of elliptic curves over $\mathbb{C}$; up to isomorphism they all arise from lattice inclusions; in particular, the inclusion $nL \subseteq L$ induces the multiplication-by-$n$ endomorphism of $E_L$.

Let us now specialize to the case where $E_1 / \mathbb{C}$ has CM by $\mathcal{O}$. Then $L_1$ is homothetic to a proper (hence invertible) $\mathcal{O}$-ideal $b$, so let us put $L_1 = b$ and $E_1 = E_b$. If $a$ is any invertible $\mathcal{O}$-ideal, the inclusion of lattices $b \subseteq a^{-1}b$ (given by $ab \subseteq b$) induces an isogeny

$$\phi_a: E_b \to E_{a^{-1}b} = aE_b$$

that corresponds to the action of $a$ on $E_b$ defined in (1). Moreover, if $E_2 = E_{L_2}$ has CM by $\mathcal{O}$, then $L_2$ is homothetic to an invertible $\mathcal{O}$-ideal $c$, and if we replace $b$ by the homothetic $\mathcal{O}$-ideal $(Nc)b$, then $c$ divides (hence contains) $b$, because $Nc = \mathcal{O}$, by Theorem 18.10. If we now put $a = bc^{-1}$, then the isogeny $\phi_a: E_b \to E_c = aE_b$ induced by the inclusion $b \subseteq c$ corresponds to the action of $a$ on $E_b$. After rescaling $a, b, c$ by integer multiples if necessary, we can assume $a$ is an invertible $\mathcal{O}$-ideal.

Thus all elliptic curves over $\mathbb{C}$ with CM by $\mathcal{O}$ are isogenous, and up to isomorphism, every isogeny between elliptic curves over $\mathbb{C}$ with CM by $\mathcal{O}$ is of the form $E_b \to aE_b$, where $a$ and $b$ are invertible $\mathcal{O}$-ideals.

**Definition 18.13.** Let $E/k$ be any elliptic curve with CM by an imaginary quadratic order $\mathcal{O}$, and let $a$ be an $\mathcal{O}$-ideal. The $a$-torsion subgroup of $E$ is defined by

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

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

**Theorem 18.14.** Let $\mathcal{O}$ be an imaginary quadratic order, let $E/\mathbb{C}$ be an elliptic curve with endomorphism ring $\mathcal{O}$, let $a$ be an invertible $\mathcal{O}$-ideal, and let $\phi_a$ be the corresponding isogeny from $E$ to $aE$. The following hold:

(i) $\ker \phi_a = E[a]$;

(ii) $\deg \phi_a = Na$.

**Proof.** By composing $\phi_a$ with an isomorphism if necessary, we assume without loss of generality that $E = E_b$ for some invertible $\mathcal{O}$-ideal $b$. Let $\Phi$ be the isomorphism from $\mathbb{C}/b \to E_b$...
that sends $z$ to $(\varphi(z), \varphi'(z))$. We have

$$\Phi^{-1}(E[a]) = \{ z \in \mathbb{C}/b : \alpha z = 0 \text{ for all } \alpha \in a \}$$
$$= \{ z \in \mathbb{C} : \alpha z \in b \text{ for all } \alpha \in a \}$$
$$= \{ z \in \mathbb{C} : za \subseteq b \}$$
$$= \{ z \in \mathbb{C} : zO \subseteq a^{-1}b \}$$
$$= (a^{-1}b)/b$$
$$= \ker \left( \mathbb{C}/b \xrightarrow{z \mapsto z} \mathbb{C}/a^{-1}b \right)$$
$$= \Phi^{-1}(\ker \varphi_a),$$

which proves (i). We then note that

$$#E[a] = [a^{-1}b : b] = [b : ab] = [O : aO] = [O : a] = Na,$$

which proves (ii).

Corollary 18.15. Let $O$ be an imaginary quadratic order and let $a$ be an invertible $O$-ideal. For every elliptic curve $E/\mathbb{C}$ with CM by $O$ the elliptic curves $E$ and $aE$ are related by an isogeny $\varphi_a : E \rightarrow aE$ of degree $Na$.

Proof. This follows immediately from the theorem and discussion above.

18.6 Discriminants

To streamline our work with imaginary quadratic orders, we define the discriminant of $O$, a negative integer that uniquely determines $O$. Since $O$ is a subring of an imaginary quadratic field that has rank 2 as a $\mathbb{Z}$-module, we can always write $O$ as $[1, \tau]$, where $\tau$ is an algebraic integer that does not lie in $\mathbb{Z}$; its minimal polynomial is necessarily of the form $x^2 + bx + c$ with discriminant $b^2 - 4c \in \mathbb{Z}_{<0}$.

Definition 18.16. Let $O = [1, \tau]$ be an imaginary quadratic order. The discriminant of $O$ is the discriminant of the minimal polynomial of $\tau$, which we can compute as

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

If $A$ is the area of a fundamental parallelogram of $O$ then

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

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

Since the discriminant $\text{disc}(O)$ is a negative integer of the form $b^2 - 4c$ with $b, c \in \mathbb{Z}$, it is necessarily a square modulo 4 (hence congruent to 0 or 1 mod 4).

Definition 18.17. A negative integer $D$ that is a square modulo 4 is an (imaginary quadratic) discriminant. Discriminants not of the form $u^2D'$ for some integer $u > 1$ and discriminant $D'$ are said to be fundamental. Every discriminant can be written uniquely as the product of a square and a fundamental discriminant.
There is a one-to-one relationship between imaginary quadratic discriminants and orders in imaginary quadratic fields; fundamental discriminants correspond to maximal orders.

**Theorem 18.18.** Let $D$ be an imaginary quadratic discriminant. There is a unique imaginary quadratic order $\mathcal{O}$ with $\text{disc}(\mathcal{O}) = D = u^2D_K$, where $D_K$ is the fundamental discriminant of the maximal order $\mathcal{O}_K$ in $K = \mathbb{Q}(\sqrt{D})$, and $u = [\mathcal{O}_K : \mathcal{O}]$.

**Proof.** Write $D = \text{disc}(\mathcal{O})$ as $D = u^2D_K$, with $u \in \mathbb{Z}_{>0}$ and $D_K$ a fundamental discriminant. Let $K = \mathbb{Q}(\sqrt{D})$, and let $\mathcal{O}_K$ be its ring of integers, the maximal order of $K$, by Theorem 13.26. Now define

$$\tau := \begin{cases} \frac{\sqrt{D_K}}{2} & \text{if } D_K \equiv 0 \text{ mod } 4; \\ \frac{1+\sqrt{D_K}}{2} & \text{if } D_K \equiv 1 \text{ mod } 4. \end{cases}$$

Then $\text{disc}([1, \tau]) = (\tau - \bar{\tau})^2 = D_K$, and $\tau + \bar{\tau}$ and $\tau \bar{\tau}$ are integers, so $\tau \in \mathcal{O}_K$ and $[1, \tau]$ is a suborder of $\mathcal{O}_K$. But $\mathcal{O}_K$ is the maximal order of $K$, so $\mathcal{O}_K = [1, \tau]$ and $\text{disc}(\mathcal{O}_K) = D_K$. The order $\mathcal{O} = [1, u\tau]$ then has discriminant $(u\tau - \bar{u}\tau)^2 = u^2D_K = D$.

Conversely, if $\mathcal{O} = [1, \omega]$ is any imaginary quadratic order of discriminant $D$, then $\omega$ is the root of a quadratic equation of discriminant $D$ and therefore an algebraic integer in the field $\mathbb{Q}(\sqrt{D}) = \mathbb{Q}(\sqrt{D_K}) = K$. We must have $\mathcal{O} \subseteq \mathcal{O}_K$, since $\mathcal{O}_K$ is the unique maximal order. The ratio of the squares of the areas of the fundamental parallelograms of $\mathcal{O}_K$ and $\mathcal{O}$ must be $D / D_K = u^2$, which implies $[\mathcal{O}_K : \mathcal{O}] = u$. Let $\mathcal{O}_K = [1, \tau]$ with $\tau$ defined as above. By Lemma 18.19 below, $u\mathcal{O}_K \subseteq \mathcal{O}$, so $u\tau \in \mathcal{O}$, and the lattice $[1, u\tau] \subseteq \mathcal{O}$ has index $u$ in $\mathcal{O}_K$ and is therefore equal to $\mathcal{O}$. It follows that $[1, u\tau]$ is the unique imaginary quadratic order of discriminant $D$.

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

**Lemma 18.19.** If $L'$ is an index $n$ sublattice of $L$ then $nL$ is an index $n$ sublattice of $L'$.

**Proof.** Without loss of generality, $L = [1, \tau]$ and $L' = [a, b + c\tau]$ (let $a$ be the least positive integer in $L'$). Comparing areas of fundamental parallelograms yields

$$n | \text{im } \tau | = |a \text{ im } c\tau| = |ac| |\text{im } \tau|$$

$$n = |ac|,$$

Thus $a|n$, so $n \in L'$, and $a(b + c\tau) - ba = ac\tau = \pm n\tau$, so $n\tau \in L'$; therefore $nL = [n, n\tau] \subseteq L'$. We have $[L : L'] = n$ and $[L : L'][L' : nL] = [nL : L] = n^2$, so $[L' : nL] = n$. \(\square\)

**References**