

17 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} :

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

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 $\mathcal{O}(L)$ can be larger than \mathcal{O} .

The sets

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

are both in bijection with the *ideal class group*

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

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

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

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 17.1. 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 12.22. 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

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

and we then have a bijection of sets

$$\begin{aligned} \text{cl}(\mathcal{O}) &\xrightarrow{\sim} \text{Ell}_{\mathcal{O}}(\mathbb{C}) \\ [\mathfrak{a}] &\longmapsto j(E_{\mathfrak{a}}) = j(\mathfrak{a}). \end{aligned}$$

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 *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.

17.1 Fractional ideals

Definition 17.2. 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 $\mathfrak{b} = \lambda\mathfrak{a} := \{\lambda\alpha : \alpha \in \mathfrak{a}\}$ is called a *fractional \mathcal{O} -ideal*.¹ Multiplication of fractional ideals $\mathfrak{b} = \lambda\mathfrak{a}$ and $\mathfrak{b}' = \lambda'\mathfrak{a}'$ is defined in the obvious way:

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

where $\mathfrak{a}\mathfrak{a}'$ is the product of the \mathcal{O} -ideals \mathfrak{a} and \mathfrak{a}' .²

Without loss of generality we can assume $\lambda = 1/\beta$ for some $\beta \in \mathcal{O}$ (if $\lambda = \alpha/\beta$, replace \mathfrak{a} with $\alpha\mathfrak{a}$), 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 β then $f(\beta) - f(0)$ is divisible by β 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 \mathfrak{b} for which there exists a fractional \mathcal{O} -ideal \mathfrak{b}^{-1} such that $\mathfrak{b}\mathfrak{b}^{-1} = \mathcal{O}$ are said to be *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 *ideal group of \mathcal{O}* , even though its elements are fractional \mathcal{O} -ideals many of which are not \mathcal{O} -ideals).

17.2 Norms

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

Definition 17.3. Let K/k be a field extension and let $\lambda \in K^{\times}$. The multiplication-by- λ map $K \rightarrow K$ is an invertible linear transformation $M_{\lambda} \in \text{GL}(K)$ of K as a k -vector space. The (field) *norm* and *trace* of λ are defined by

$$N_{K/k}\lambda := \det M_{\lambda} \in k^{\times} \quad \text{and} \quad T_{K/k}\lambda := \text{tr } M_{\lambda} \in k.$$

¹Some 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.

²One can also add fractional \mathcal{O} -ideals via $\mathfrak{b} + \mathfrak{b}' := \{b + b' : b \in \mathfrak{b}, b' \in \mathfrak{b}'\}$, but we won't need this.

One typically computes the norm and trace by fixing a basis for K as a k vector space and writing M_λ as a matrix using this basis, but the norm and trace of M_λ 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 λ .

When $K \simeq \text{End}^0(E)$ is an imaginary quadratic field, Definition 17.3 coincides with our definition of the (reduced) norm and trace of an element of $\text{End}^0(E)$ (see Definition 12.6). 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 17.4. Let \mathcal{O} be an order in a number field K and let \mathfrak{a} be a nonzero \mathcal{O} -ideal. The (absolute) *norm* of the ideal \mathfrak{a} is

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

We can also interpret $N\mathfrak{a}$ as the ratio of the volumes of fundamental parallelepipeds for \mathfrak{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 17.5. *Let α be a nonzero element of an order \mathcal{O} in a number field K . Then*

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

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

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 (α) 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 α and K , not the order \mathcal{O} (N.B. this holds for principal ideals but not in general). \square

Warning 17.6. 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 $\mathfrak{a} = [2, 2i]$ in the order $\mathcal{O} = [1, 2i]$, which has norm $N\mathfrak{a} = [\mathcal{O} : \mathfrak{a}] = 2$. Then $\mathfrak{a}^2 = [4, 4i]$ and

$$N\mathfrak{a}^2 = 8 \neq 2^2 = (N\mathfrak{a})^2.$$

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

Corollary 17.7. *Let \mathcal{O} be an order in a number field, let $\alpha \in \mathcal{O}$ be nonzero, and let \mathfrak{a} be a nonzero \mathcal{O} -ideal. Then*

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

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

This allows us to make the following definition.

Definition 17.8. Let $\mathfrak{b} = \frac{1}{b}\mathfrak{a}$ 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 \mathfrak{b} this way). The (absolute) *norm* of \mathfrak{b} is

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

Corollary 17.7 ensures that this does not depend on the choice of b and \mathfrak{a} .

When $\mathfrak{b} \subseteq \mathcal{O}$ we can take $b = 1$, in which case this agrees with Definition 17.4.

17.3 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 \mathfrak{b} we define

$$\mathcal{O}(\mathfrak{b}) := \{\alpha : \alpha\mathfrak{b} \subseteq \mathfrak{b}\},$$

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

Lemma 17.9. *Let \mathcal{O} be an order in an imaginary quadratic field, let \mathfrak{a} be a nonzero \mathcal{O} -ideal, and let $\mathfrak{b} = \lambda\mathfrak{a}$ be a fractional \mathcal{O} -ideal. Then \mathfrak{a} is proper if and only if \mathfrak{b} is proper, and \mathfrak{a} is invertible if and only if \mathfrak{b} is invertible.*

Proof. For the first statement, note that $\{\alpha : \alpha\mathfrak{b} \subseteq \mathfrak{b}\} = \{\alpha : \alpha\lambda\mathfrak{a} \subseteq \lambda\mathfrak{a}\} = \{\alpha : \alpha\mathfrak{a} \subseteq \mathfrak{a}\}$. For the second, if \mathfrak{a} is invertible then $\mathfrak{b}^{-1} = \lambda^{-1}\mathfrak{a}^{-1}$, and if \mathfrak{b} is invertible then $\mathfrak{a}^{-1} = \lambda\mathfrak{b}^{-1}$, since $\mathfrak{a}\mathfrak{a}^{-1} = \mathfrak{a}\lambda\mathfrak{b}^{-1} = \mathfrak{b}\mathfrak{b}^{-1} = \mathcal{O}$. \square

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 17.10. *Let \mathcal{O} be an order in an imaginary quadratic field and 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 $\mathfrak{a}\bar{\mathfrak{a}} = (N\mathfrak{a})$, where $\bar{\mathfrak{a}} = [\bar{\alpha}, \bar{\beta}]$ and $(N\mathfrak{a})$ is the principal \mathcal{O} -ideal generated by the integer $N\mathfrak{a}$; the inverse of \mathfrak{a} is then the fractional \mathcal{O} -ideal $\mathfrak{a}^{-1} = \frac{1}{N\mathfrak{a}}\bar{\mathfrak{a}}$.*

Proof. If \mathfrak{a} is invertible, then for any $\gamma \in \mathbb{C}$ we have

$$\gamma\mathfrak{a} \subseteq \mathfrak{a} \implies \gamma\mathfrak{a}\mathfrak{a}^{-1} \subseteq \mathfrak{a}\mathfrak{a}^{-1} \implies \gamma\mathcal{O} \subseteq \mathcal{O} \implies \gamma \in \mathcal{O},$$

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

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

$a\tau$ and $a\tau^2 = -b\tau - c$ lie in $[1, \tau]$, so $a\tau \in \mathcal{O}([1, \tau]) = \mathcal{O} = [1, n\tau]$, and we must have $n = a$ and $\mathcal{O} = [1, a\tau]$. Thus

$$N(\mathfrak{a}) = [\mathcal{O} : \mathfrak{a}] = [[1, a\tau] : \alpha[1, \tau]] = \frac{1}{a} [[1, a\tau] : \alpha[1, a\tau]] = \frac{1}{a} [\mathcal{O} : \alpha\mathcal{O}] = \frac{N(\alpha)}{a}.$$

We also have

$$\mathfrak{a}\bar{\mathfrak{a}} = \alpha[1, \tau]\bar{\alpha}[1, \bar{\tau}] = N(\alpha)[1, \tau, \bar{\tau}, \tau\bar{\tau}].$$

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

$$\mathfrak{a}\bar{\mathfrak{a}} = N(\alpha)[1, \tau, \bar{\tau}, \tau\bar{\tau}] = \frac{N(\alpha)}{a} [a, a\tau, -b, c] = N\mathfrak{a}[1, a\tau] = (N\mathfrak{a})\mathcal{O} = (N\mathfrak{a})$$

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 $\mathfrak{a}^{-1} = \frac{1}{N\mathfrak{a}}\bar{\mathfrak{a}}$. \square

Corollary 17.11. *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 $\mathfrak{b} = \frac{1}{b}\mathfrak{a}$ is the product of an invertible principal fractional \mathcal{O} -ideal $(\frac{1}{b})$ and an invertible \mathcal{O} -ideal \mathfrak{a} , by Lemma 17.9. It follows that G/H consists of all cosets $\mathfrak{a}H$, where \mathfrak{a} is any invertible, equivalently, proper \mathcal{O} -ideal (by Theorem 17.10). Every nonzero principal fractional \mathcal{O} -ideal is invertible, since $(\alpha)^{-1} = (\alpha^{-1})$, so H contains every nonzero principal fractional \mathcal{O} -ideal and for any two proper/invertible \mathcal{O} -ideals $\mathfrak{a}, \mathfrak{b}$ we have $\mathfrak{a} \sim \mathfrak{b}$ if and only if $\mathfrak{a}H = \mathfrak{b}H$. It follows that $\text{cl}(\mathcal{O}) = G/H$. \square

Corollary 17.12. *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 $N(\mathfrak{a}\mathfrak{b}) = N\mathfrak{a}N\mathfrak{b}$.*

Proof. If $\mathfrak{a} = \frac{1}{a}\mathfrak{a}'$ and $\mathfrak{b} = \frac{1}{b}\mathfrak{b}'$ with $a, b \in \mathbb{Z}_{>0}$ and $\mathfrak{a}', \mathfrak{b}' \subseteq \mathcal{O}$ then $N(\mathfrak{a}\mathfrak{b}) = \frac{N(\mathfrak{a}'\mathfrak{b}')}{N\mathfrak{a}N\mathfrak{b}}$, so it is enough to consider the case where \mathfrak{a} and \mathfrak{b} are invertible \mathcal{O} -ideals. We have

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

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

17.4 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 $E_{\mathfrak{b}}$, for some proper \mathcal{O} -ideal \mathfrak{b} . For any proper \mathcal{O} -ideal \mathfrak{a} we define the action of \mathfrak{a} on $E_{\mathfrak{b}}$ via

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

(we $E_{\mathfrak{a}^{-1}\mathfrak{b}}$ rather than $E_{\mathfrak{a}\mathfrak{b}}$ because $\mathfrak{a}\mathfrak{b} \subseteq \mathfrak{b}$ but $\mathfrak{b} \subseteq \mathfrak{a}^{-1}\mathfrak{b}$). The action of the equivalence class $[\mathfrak{a}]$ on the isomorphism class $j(E_{\mathfrak{b}})$, is then defined by

$$[\mathfrak{a}]j(E_{\mathfrak{b}}) = j(E_{\mathfrak{a}^{-1}\mathfrak{b}}), \quad (2)$$

which we can also write as

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

which does not depend on the choice of \mathfrak{a} and \mathfrak{b} .

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

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

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

For any proper \mathcal{O} -ideals \mathfrak{a} and \mathfrak{b} , we have $[\mathfrak{a}]j(\mathfrak{b}) = j(\mathfrak{a}^{-1}\mathfrak{b}) = j(\mathfrak{b})$ if and only if \mathfrak{b} is homothetic to $\mathfrak{a}^{-1}\mathfrak{b}$, by Theorem 15.5, and in this case we have $\mathfrak{a}\mathfrak{b} = \lambda\mathfrak{b}$ for $\lambda \in K^{\times}$, and then $\mathfrak{a} = \lambda\mathcal{O}$ 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 $[\mathfrak{a}]j_0$ of j_0 under the action of each $[\mathfrak{a}] \in \text{cl}(\mathcal{O})$ 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.

17.5 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 $\phi: E_1 \rightarrow E_2$ 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 16.4, there is a unique $\alpha = \alpha_{\phi}$ with $\alpha L_1 \subseteq L_2$ such that the following diagram commutes

$$\begin{array}{ccc} \mathbb{C}/L_1 & \xrightarrow{\alpha} & \mathbb{C}/L_2 \\ \downarrow \Phi_1 & & \downarrow \Phi_2 \\ E_1(\mathbb{C}) & \xrightarrow{\phi} & E_2(\mathbb{C}). \end{array}$$

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 αL_1 and E_1 by an isomorphic elliptic curve so

that $\alpha = 1$ and the isogeny ϕ is induced by the inclusion $L_1 \subseteq L_2$; note that this amounts to composing ϕ with an isomorphism and does not change its degree. Up to an isomorphism of elliptic curves and a homothety of lattices, every isogeny $\phi: E_1 \rightarrow E_2$ arises from an inclusion of lattices $L_1 \subseteq L_2$. In this situation it is clear what the kernel of ϕ is. By commutativity, since $\alpha = 1$, the kernel of ϕ 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 ϕ 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 \mathfrak{b} , so let us put $L_1 = \mathfrak{b}$ and $E_1 = E_{\mathfrak{b}}$. If \mathfrak{a} is any invertible \mathcal{O} -ideal, the inclusion of lattices $\mathfrak{b} \subseteq \mathfrak{a}^{-1}\mathfrak{b}$ (given by $\mathfrak{a}\mathfrak{b} \subseteq \mathfrak{b}$) induces an isogeny

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

that corresponds to the action of \mathfrak{a} on $E_{\mathfrak{b}}$ 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 \mathfrak{c} , and if we replace \mathfrak{b} by the homothetic \mathcal{O} -ideal $(N\mathfrak{c})\mathfrak{b}$, then \mathfrak{c} divides (hence contains) \mathfrak{b} , because $N\mathfrak{c} = \mathfrak{c}\bar{\mathfrak{c}}$, by Theorem 17.10. If we now put $\mathfrak{a} = \mathfrak{b}\mathfrak{c}^{-1}$, then the isogeny $\phi_{\mathfrak{a}}: E_{\mathfrak{b}} \rightarrow E_{\mathfrak{c}} = \mathfrak{a}E_{\mathfrak{b}}$ induced by the inclusion $\mathfrak{b} \subseteq \mathfrak{c}$ corresponds to the action of \mathfrak{a} on $E_{\mathfrak{b}}$. After rescaling \mathfrak{a} , \mathfrak{b} , \mathfrak{c} by integer multiples if necessary, we can assume \mathfrak{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 $E_{\mathfrak{b}} \rightarrow \mathfrak{a}E_{\mathfrak{b}}$, where \mathfrak{a} and \mathfrak{b} are invertible \mathcal{O} -ideals.

Definition 17.13. 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 $\alpha \in \mathfrak{a} \subseteq \mathcal{O} \simeq \text{End}(E)$ as an endomorphism.

Theorem 17.14. Let \mathcal{O} be an imaginary quadratic order, let E/\mathbb{C} be an elliptic curve with endomorphism ring \mathcal{O} , let \mathfrak{a} be an invertible \mathcal{O} -ideal, and let $\phi_{\mathfrak{a}}$ be the corresponding isogeny from E to $\mathfrak{a}E$. The following hold:

- (i) $\ker \phi_{\mathfrak{a}} = E[\mathfrak{a}]$;
- (ii) $\deg \phi_{\mathfrak{a}} = N\mathfrak{a}$.

Proof. By composing $\phi_{\mathfrak{a}}$ with an isomorphism if necessary, we assume without loss of generality that $E = E_{\mathfrak{b}}$ for some invertible \mathcal{O} -ideal \mathfrak{b} . Let Φ be the isomorphism from $\mathbb{C}/\mathfrak{b} \rightarrow E_{\mathfrak{b}}$

that sends z to $(\wp(z), \wp'(z))$. We have

$$\begin{aligned}
\Phi^{-1}(E[\mathfrak{a}]) &= \{z \in \mathbb{C}/\mathfrak{b} : \alpha z = 0 \text{ for all } \alpha \in \mathfrak{a}\} \\
&= \{z \in \mathbb{C} : \alpha z \in \mathfrak{b} \text{ for all } \alpha \in \mathfrak{a}\}/\mathfrak{b} \\
&= \{z \in \mathbb{C} : z\mathfrak{a} \subseteq \mathfrak{b}\}/\mathfrak{b} \\
&= \{z \in \mathbb{C} : z\mathcal{O} \subseteq \mathfrak{a}^{-1}\mathfrak{b}\}/\mathfrak{b} \\
&= (\mathfrak{a}^{-1}\mathfrak{b})/\mathfrak{b} \\
&= \ker\left(\mathbb{C}/\mathfrak{b} \xrightarrow{z \mapsto z} \mathbb{C}/\mathfrak{a}^{-1}\mathfrak{b}\right) \\
&= \Phi^{-1}(\ker \phi_{\mathfrak{a}}),
\end{aligned}$$

which proves (i). We then note that

$$\#E[\mathfrak{a}] = [\mathfrak{a}^{-1}\mathfrak{b} : \mathfrak{b}] = [\mathfrak{b} : \mathfrak{a}\mathfrak{b}] = [\mathcal{O} : \mathfrak{a}\mathcal{O}] = [\mathcal{O} : \mathfrak{a}] = N\mathfrak{a},$$

which proves (ii). □

Corollary 17.15. *Let \mathcal{O} be an imaginary quadratic order and let \mathfrak{a} be an invertible \mathcal{O} -ideal. For every elliptic curve E/\mathbb{C} with CM by \mathcal{O} the elliptic curves E and $\mathfrak{a}E$ are related by an isogeny $\phi_{\mathfrak{a}}: E \rightarrow \mathfrak{a}E$ of degree $N\mathfrak{a}$.*

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

17.6 Discriminants

To streamline our work with imaginary quadratic orders, we define the *discriminant* of \mathcal{O} , a negative integer that uniquely determines \mathcal{O} . Since \mathcal{O} is a subring of an imaginary quadratic field that has rank 2 as a \mathbb{Z} -module, we can always write \mathcal{O} as $[1, \tau]$, where τ 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 17.16. 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

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

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

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

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

Since the discriminant $\text{disc}(\mathcal{O})$ 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 17.17. 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 17.18. *Let D be an imaginary quadratic discriminant. There is a unique imaginary quadratic order \mathcal{O} with $\text{disc}(\mathcal{O}) = D = u^2 D_K$, 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. Write $D = \text{disc}(\mathcal{O})$ as $D = u^2 D_K$, with $u \in \mathbb{Z}_{>0}$ and D_K a fundamental discriminant. Let $K = \mathbb{Q}(\sqrt{D_K})$, and let \mathcal{O}_K be its ring of integers, the maximal order of K , by Theorem 12.26. Now define

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

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 $(u\tau - \bar{u}\bar{\tau})^2 = u^2 D_K = D$.

Conversely, if $\mathcal{O} = [1, \omega]$ is any imaginary quadratic order of discriminant D , then ω 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 τ defined as above. By Lemma 17.19 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 . \square

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

Lemma 17.19. *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

$$\begin{aligned} n|\text{im } \tau| &= |a \text{ im } c\tau| = |ac| |\text{im } \tau| \\ n &= |ac|, \end{aligned}$$

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

- [1] David A. Cox, [*Primes of the form \$x^2 + ny^2\$: Fermat, class field theory, and complex multiplication*](#), second edition, Wiley, 2013.

MIT OpenCourseWare
<https://ocw.mit.edu>

18.783 / 18.7831 Elliptic Curves
Spring 2021

For information about citing these materials or our Terms of Use, visit: <https://ocw.mit.edu/terms>.