18 The CM action

Let $L \subseteq \mathbb{C}$ be a lattice and $E_L/\mathbb{C}$ the corresponding elliptic curve $y^2 = 4x^3 - g_2(L)x - g_3(L)$. In the previous lecture we proved that the endomorphism rings $\mathrm{End}(E_L)$ and $\mathrm{End}(\mathbb{C}/L)$ are both isomorphic to the ring

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

which is either equal to $\mathbb{Z}$, or an order $\mathcal{O}$ in an imaginary quadratic field. We then considered the following question: given an order $\mathcal{O}$ in an imaginary quadratic field, for which lattices L do we have $\mathcal{O}(L) = \mathcal{O}$. By the Uniformization Theorem (Corollary 16.12), this is equivalent to asking which elliptic curves $E/\mathbb{C}$ have *complex multiplication* (CM) by $\mathcal{O}$; recall that this means $\mathrm{End}(E) = \mathcal{O}$.

We established the necessary condition that L must be homothetic to an $\mathcal{O}$-ideal, and defined *proper* $\mathcal{O}$-ideals to be the $\mathcal{O}$-ideals L for which $\mathcal{O}(L) = \mathcal{O}$.[1] So, by construction, $\mathcal{O}(L) = \mathcal{O}$ if and only if L is homothetic to a proper $\mathcal{O}$-ideal; in this lecture we will give a more intrinsic condition for an $\mathcal{O}$-ideal to be proper. We defined the ideal class group $\mathrm{cl}(\mathcal{O})$ as the set of proper $\mathcal{O}$-ideals modulo the equivalence relation

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

which holds precisely when $\mathfrak{a}$ and $\mathfrak{b}$ are homothetic as lattices. It follows that there is a one-to-one relationship between $\mathrm{cl}(\mathcal{O})$ and the set of homethety classes of lattices L for which $\mathcal{O}(L) = \mathcal{O}$, equivalently, the set of isomorphism classes of elliptic curves $E/\mathbb{C}$ for which $\mathrm{End}(E) = \mathcal{O}$.

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

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

It follows from our discussion above that there is a bijection from $\mathrm{cl}(\mathcal{O})$ to $\mathrm{Ell}_{\mathcal{O}}(\mathbb{C})$ that sends the equivalence class $[\mathfrak{a}]$ of a proper $\mathcal{O}$-ideal $\mathfrak{a}$ to the isomorphism class $j(E_{\mathfrak{a}}) = j(\mathfrak{a})$; the reverse map is given by the Uniformization theorem, which tells us that we can construct a lattice L for which $j(L) = j(E)$, and this lattice L is then homothetic to a proper $\mathcal{O}$-ideal $\mathfrak{a}$ that has the same j-invariant $j(\mathfrak{a}) = j(E)$ when viewed as a lattice.

As you will prove in Problem Set 9, $\mathrm{cl}(\mathcal{O})$ is a finite group; thus the set $\mathrm{Ell}_{\mathcal{O}}(\mathbb{C})$ is finite. Its cardinality is the *class number* $h(\mathcal{O}) = |\mathrm{cl}(\mathcal{O})|$, which we may also write as $h(D)$, where $D = \mathrm{disc}(\mathcal{O})$. Remarkably, not only are the sets $\mathrm{cl}(\mathcal{O})$ and $\mathrm{Ell}_{\mathcal{O}}(\mathbb{C})$ in bijection, the set $\mathrm{Ell}_{\mathcal{O}}(\mathbb{C})$ admits a group action by $\mathrm{cl}(\mathcal{O})$. 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.

[1] The term "proper $\mathcal{O}$-ideal" is an unfortunate historical choice, since this terminology can also refer to $\mathcal{O}$-ideals that are properly contained in $\mathcal{O}$. In this lecture we will prove that $\mathcal{O}$-ideals are proper if and only if they are invertible and henceforth use the term "invertible $\mathcal{O}$-ideal" instead.

Andrew V. Sutherland

18.1 Fractional ideals

Definition 18.1. Let $\mathcal{O}$ be an integral domain with fraction field K. Any set of the form $\mathfrak{b} = \lambda\mathfrak{a}$ with $\lambda \in K^\times$ and $\mathfrak{a}$ an $\mathcal{O}$-ideal is called a *fractional $\mathcal{O}$-ideal*. 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]

Like $\mathcal{O}$-ideals, fractional $\mathcal{O}$-ideals are $\mathcal{O}$-modules (additive groups that admit a scalar multiplication by $\mathcal{O}$).[3] Fractional $\mathcal{O}$-ideals that happen to lie in $\mathcal{O}$ are thus $\mathcal{O}$-ideals (such fractional $\mathcal{O}$-ideal are sometimes called *integral* $\mathcal{O}$-ideals to emphasize this); conversely, every $\mathcal{O}$-ideal is a fractional $\mathcal{O}$-ideal. If $\mathfrak{b} = \lambda\mathfrak{a}$ is a fractional $\mathcal{O}$-ideal we can always write $\lambda = \frac{a}{b}$ for some $a, b \in \mathcal{O}$ with $b \neq 0$, and after replacing $\mathfrak{a}$ with $a\mathfrak{a}$ we can write $\mathfrak{b} = \frac{1}{b}\mathfrak{a}$ with $b \in \mathcal{O}$ nonzero and $\mathfrak{a}$ an $\mathcal{O}$-ideal. In our setting, where $\mathcal{O}$ is an order in an imaginary quadratic field K (which must be its fraction field since it is the smallest field containing $\mathcal{O}$), we can even make b a positive integer by rationalizing the denominator and noting that $\mathfrak{a} = -1 \cdot \mathfrak{a}$ for any $\mathcal{O}$-ideal $\mathfrak{a}$.

18.2 Norms

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

Definition 18.2. Let $K/\mathbb{Q}$ be a number field and let $\alpha \in K^\times$. Let $\alpha_1, \ldots, \alpha_m$ be the roots of the minimal polynomial $f \in \mathbb{Q}[x]$ of α over $\mathbb{Q}$ (which may lie in an extension of K), and let $n = [K : \mathbb{Q}(\alpha)]$. The (field) *norm* and *trace* of α are defined by

$$\mathrm{N}\alpha := \prod_{i=1}^{m} \alpha_i^n \in \mathbb{Q}^\times \qquad \text{and} \qquad \mathrm{T}\alpha := \sum_{i=1}^{m} n\alpha_i \in \mathbb{Q}.$$

Note that $\mathrm{N}\alpha$ is a power of the constant term of the monic polynomial f, and $\mathrm{T}\alpha$ is a multiple of the negation of the degree $m-1$ coefficient of f; this makes it clear that both $\mathrm{N}\alpha$ and $\mathrm{T}\alpha$ lie in $\mathbb{Q}$ (and in $\mathbb{Z}$ if α is an algebraic integer). Note that $\mathrm{N}\alpha$ is nonzero because the constant term of f cannot be nonzero (otherwise f would not be minimal).

When $K/\mathbb{Q}$ is a Galois extension we can simply take the product and sum over all mn *Galois conjugates* $\sigma(\alpha)$ for $\sigma \in \mathrm{Gal}(K/\mathbb{Q})$. This makes it clear that in this case the norm map is multiplicative. In fact this holds for any number field K; this follows from the proof of Lemma 18.4 below, which relates $\mathrm{N}\alpha$ to the determinant of the multiplication-by-α map, which can be viewed as a linear transformation of the $\mathbb{Q}$-vector space K.

Note that $\mathrm{N}\alpha$ depends on K, not just α; for example, if $\alpha \in \mathbb{Q}^\times$ then $\mathrm{N}\alpha = \alpha^{[K:\mathbb{Q}]}$, which will vary if we fix α and change K. It should really be viewed as a homomorphism

$$\mathrm{N}\colon K^\times \to \mathbb{Q}^\times$$

[2] One 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.

[3] Some authors define fractional $\mathcal{O}$-ideals to be finitely generated $\mathcal{O}$-modules that are contained in 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 only case we care about), the definitions are equivalent.

and is often written as $\mathrm{N}_{K/\mathbb{Q}}$ to emphasis this. Definition 18.2 generalizes to any finite extension K/k (just replace $\mathbb{Q}$ with k), and is then denoted $\mathrm{N}_{K/k}$ and defines a homomorphism $K^\times \to k^\times$.

When $K \simeq \mathrm{End}^0(E)$ is an imaginary quadratic field, Definition 18.2 coincides with our definition of the (reduced) norm and trace of α as an element of $\mathrm{End}^0(E)$ (see Definition 13.6). If K is an imaginary quadratic field embedded in $\mathbb{C}$, this is equivalent to taking $\mathrm{N}\alpha = \alpha\bar{\alpha}$ and $\mathrm{T}\alpha = \alpha + \bar{\alpha}$, where $\bar{\alpha}$ denotes complex conjugation (equivalently, conjugation by the non-trivial element of $\mathrm{Gal}(K/\mathbb{Q})$. Thus in this setting the complex conjugate

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

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

Definition 18.3. Let $\mathcal{O}$ be an order in a number field K and let $\mathfrak{a}$ be a nonzero $\mathcal{O}$-ideal. The (ideal) *norm* of $\mathfrak{a}$ is

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

Alternatively, if we fix $\mathbb{Z}$-bases for $\mathcal{O}$ and $\mathfrak{a}$ we have

$$\mathrm{N}\mathfrak{a} = |\det M_{\mathfrak{a}}|$$

where $M_{\mathfrak{a}}$ is an integer matrix whose rows express the basis elements of $\mathfrak{a}$ as $\mathbb{Z}$-linear combinations of basis elements of $\mathcal{O}$. Note that $|\det M_{\mathfrak{a}}|$ is independent of the choice of basis, and it is nonzero because $\mathfrak{a}$ and $\mathcal{O}$ are both free $\mathbb{Z}$-modules of rank $r = \dim K$ (which also makes it clear why $[\mathcal{O} : \mathfrak{a}]$ is actually finite).[4] That these two definitions are equivalent follows from the fact that we can diagonalize $M_{\mathfrak{a}}$ using row and column operations that do not change $|\det M_{\mathfrak{a}}|$ (each corresponding to a change of basis for $\mathcal{O}$ or $\mathfrak{a}$).[5] It is then clear that we have $\mathcal{O}/\mathfrak{a} \simeq \mathbb{Z}/d_1\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/d_r\mathbb{Z}$, where $d_1, \ldots, d_r$ are the diagonal entries of this matrix, and we then have $|d_1 \cdots d_r| = |\det M_{\mathfrak{a}}|$. We can also interpret $\mathrm{N}\mathfrak{a}$ as the ratio of the volumes of fundamental parallelograms for $\mathfrak{a}$ and $\mathcal{O}$, which we may view as $\mathbb{Z}$-lattices embedded in the $\mathbb{Q}$-vector space $K \simeq \mathbb{Q}^r$ (with the Euclidean metric).

We now relate the norm of a nonzero element of $\mathcal{O}$ to the norm of the principal ideal it generates.

Lemma 18.4. *Let α be a nonzero element of an order $\mathcal{O}$ in a number field K. Then*

$$\mathrm{N}(\alpha) = |\mathrm{N}\alpha|,$$

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

Proof. Let $\mathcal{O}_K$ be the maximal order in K. Note that $\mathrm{N}(\alpha) = [\mathcal{O} : \alpha\mathcal{O}] = [\mathcal{O}_K : \alpha\mathcal{O}_K]$ is the same as the norm of the principal $\mathcal{O}_K$-ideal generated by α, so without loss of generality we assume $\mathcal{O} = \mathcal{O}_K$. Let $L = \mathbb{Q}(\alpha) \subseteq K$, and let us fix a $\mathbb{Z}$-basis for $\mathcal{O}_K$ that contains a $\mathbb{Z}$-basis for $\mathcal{O}_L$; this is possible because $\mathcal{O}_L$ is a free $\mathbb{Z}$-module of rank $m = [L : \mathbb{Q}]$ that is contained in the free $\mathbb{Z}$-module $\mathcal{O}_K$ of rank $r = [K : \mathbb{Q}]$. Note that $m|r$, since K is an L-vector space of dimension $n = [K : L]$. Moreover, we may order our basis into n blocks

[4] That $\mathfrak{a}$ is a free $\mathbb{Z}$-module follows from the fact that it is a submodule of the free $\mathbb{Z}$-module $\mathcal{O}$ and $\mathbb{Z}$ is a principal ideal domain (submodules of free module over PIDs are always free, but this is *not true* of more general rings). That $\mathfrak{a}$ has the same rank as $\mathcal{O}$ follows from the fact that it contains a nonzero integer (for example, the norm of any of its elements) and therefore an integer multiple of $\mathcal{O}$.

[5] This amounts to putting $M_{\mathfrak{a}}$ in *Smith normal form.*

of size m, each of which is a $\mathbb{Q}$-basis for an m-dimensional subspace of K isomorphic to L. Let us now consider the $r \times r$ matrix $M_{(\alpha)}$ of the $\mathbb{Z}$-linear transformation given by the multiplication-by-α map $\mathcal{O} \to \mathcal{O}$ with respect to this basis. Assuming we order our basis appropriately, the matrix $M_{(\alpha)}$ is then a block diagonal matrix consisting of n square $m \times m$ matrices along the diagonal, all of which are conjugate. We then have

$$\mathrm{N}(\alpha) = |\det M_{(\alpha)}|.$$

On the other hand, the characteristic polynomial $g \in \mathbb{Z}[x]$ of $M_{(\alpha)}$ is the nth power of the minimal polynomial f of α over $\mathbb{Q}$ (which lies in $\mathbb{Z}[x]$ because α is an algebraic integer), and $\mathrm{N}\alpha$ is the constant coefficient of g, which has the same absolute value as $\det M_{(\alpha)}$.

To see this, note that if B is the first block diagonal matrix of M, representing the multiplication by α map on $\mathcal{O}_L$, then f is the minimal polynomial of B, since it is the minimal polynomial of α, and it has degree m so it is the characteristic polynomial of B. The n block diagonal matrices of M are all conjugate, hence they all have the same characteristic polynomial, and therefore $g = f^n$. ☐

Warning 18.5. 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 true**. As an example, consider the ideal $\mathfrak{a} = [2, 2i]$ in the order $\mathcal{O} = [1, 2i]$, which has norm $\mathrm{N}\mathfrak{a} = [\mathcal{O} : \mathfrak{a}] = 2$. Then $\mathfrak{a}^2 = [4, 4i]$ and

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

However, as we shall see (at least when $\mathcal{O}$ is an order in an imaginary quadratic field), the ideal norm is multiplicative when $\mathfrak{a}$ and $\mathfrak{b}$ are both proper/invertible $\mathcal{O}$-ideals, hence in all cases when $\mathcal{O} = \mathcal{O}_K$ is the maximal order. In any case we always have the following corollary of Lemma 18.4.

Corollary 18.6. *Let $\mathcal{O}$ be an order in a number field, let $\alpha \in \mathcal{O}$ be nonzero, and let $\mathfrak{a}$ be an $\mathcal{O}$-ideal. Then*

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

Proof. We have

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

The corollary implies that $\mathrm{N}(\mathfrak{a}\mathfrak{b}) = \mathrm{N}\mathfrak{a}\mathrm{N}\mathfrak{b}$ whenever one of $\mathfrak{a}$ and $\mathfrak{b}$ is principal. This allows us to make the following definition.

Definition 18.7. Let $\mathfrak{b} = \lambda\mathfrak{a}$ be a nonzero fractional ideal in an order $\mathcal{O}$ of a number field. The *norm* of $\mathfrak{b}$ is

$$\mathrm{N}\mathfrak{b} := \mathrm{N}\lambda\mathrm{N}\mathfrak{a} \in \mathbb{Q}^\times.$$

Corollary 18.6 ensures that this is well defined: if $\lambda\mathfrak{a} = \lambda'\mathfrak{a}'$, after writing $\lambda = a/b$ and $\lambda' = a'/b'$ we have $ab'\mathfrak{a} = a'b\mathfrak{a}'$ and therefore

$$\mathrm{N}\mathfrak{a}' = \frac{\mathrm{N}a\mathrm{N}b'}{\mathrm{N}a'\mathrm{N}b}\mathrm{N}\mathfrak{a} = \frac{\mathrm{N}\lambda}{\mathrm{N}\lambda'}\mathrm{N}\mathfrak{a},$$

so $\mathrm{N}\lambda'\mathrm{N}\mathfrak{a}' = \mathrm{N}\lambda\mathrm{N}\mathfrak{a}$.

Taking $\lambda = 1$ or $\mathfrak{a} = \mathcal{O}$, we can view this as a generalization of Definitions 18.2 and 18.3.

18.3 Invertible 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 $\mathcal{O}(\mathfrak{b}) = \mathcal{O}$. We say that a fractional $\mathcal{O}$-ideal $\mathfrak{b}$ is *invertible* if there exists a fractional $\mathcal{O}$-ideal $\mathfrak{b}^{-1}$ for which $\mathfrak{b}\mathfrak{b}^{-1} = \mathcal{O}$. Notice that this definition applies in the case that $\mathfrak{b}$ is an $\mathcal{O}$-ideal, but then $\mathfrak{b}^{-1}$ will not be an $\mathcal{O}$-ideal (unless $\mathfrak{b} = \mathcal{O}$). As we shall see, the notions of properness and invertibility coincide, but 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 18.8. *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 we have $\mathfrak{a}\mathfrak{a}^{-1} = \mathfrak{a}\lambda\mathfrak{b}^{-1} = \mathfrak{b}\mathfrak{b}^{-1} = \mathcal{O}$. □

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 18.9. *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 $\mathfrak{a}\bar{\mathfrak{a}} = (\mathrm{N}\mathfrak{a})$, where $\bar{\mathfrak{a}} = [\bar{\alpha}, \bar{\beta}]$ and $(\mathrm{N}\mathfrak{a})$ is the principal $\mathcal{O}$-ideal generated by the integer $\mathrm{N}\mathfrak{a}$; the inverse of $\mathfrak{a}$ is then the fractional $\mathcal{O}$-ideal $\mathfrak{a}^{-1} = \frac{1}{\mathrm{N}\mathfrak{a}}\bar{\mathfrak{a}}$.*

Proof. We first assume that $\mathfrak{a} = [\alpha, \beta]$ is a proper $\mathcal{O}$-ideal and show that $\mathfrak{a}\bar{\mathfrak{a}} = (\mathrm{N}\mathfrak{a})$, which implies $\mathfrak{a}^{-1} = \frac{1}{\mathrm{N}\mathfrak{a}}\bar{\mathfrak{a}}$. Let $\tau = \beta/\alpha$, so that $\mathfrak{a} = \alpha[1, \tau]$, and let $ax^2 + bx + c$ be the least multiple of the minimal polynomial of τ that lies in $\mathbb{Z}[x]$, so $\gcd(a, b, c) = 1$. The fractional ideal $[1, \tau]$ is homothetic to $\mathfrak{a}$, and we have $\mathcal{O}([1, \tau]) = \mathcal{O}(\mathfrak{a}) = \mathcal{O}$, 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 $\omega\tau \in [1, \tau]$, so $n\tau^2 \in [1, \tau]$, which implies that $a|n$, since otherwise the polynomial ax^2+bx+c would have a leading coefficient smaller than a in absolute value. And $a\tau[1, \tau] \subseteq [1, \tau]$, so $\alpha\tau \in \mathcal{O}([1, \tau]) = \mathcal{O}$, therefore $n = a$ and $\mathcal{O} = [1, a\tau]$. Thus

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

We also have

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

Since $a\tau^2 + b\tau + c = 0$, we have $\tau + \bar{\tau} = -b/a$, and $\tau\bar{\tau} = c/a$, with $\gcd(a, b, c) = 1$. So

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

as claimed. Conversely, 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 $\mathcal{O} \subseteq \mathcal{O}(\mathfrak{a})$. □

Corollary 18.10. *Let $\mathcal{O}$ be an order in an imaginary quadratic field and let $\mathfrak{a}$ and $\mathfrak{b}$ be invertible fractional $\mathcal{O}$-ideals. Then* $\mathrm{N}(\mathfrak{a}\mathfrak{b}) = \mathrm{N}\mathfrak{a}\mathrm{N}\mathfrak{b}$.

Proof. If $\mathfrak{a} = \alpha\mathfrak{a}'$ and $\mathfrak{b} = \beta\mathfrak{b}'$ for some $\alpha, \beta \in K^\times$ and $\mathcal{O}$-ideals $\mathfrak{a}'$ and $\mathfrak{b}'$, then $\mathfrak{a}'$ and $\mathfrak{b}'$ are invertible, by Lemma 18.8. By definition, $\mathrm{N}\mathfrak{a} = \mathrm{N}\alpha\mathrm{N}\mathfrak{a}'$ and $\mathrm{N}\mathfrak{b} = \mathrm{N}\beta\mathrm{N}\mathfrak{b}'$, and the field norm is multiplicative, so $\mathrm{N}(\alpha\beta) = \mathrm{N}\alpha\mathrm{N}\beta$. Thus it suffices to consider the case where $\mathfrak{a} = \mathfrak{a}'$ and $\mathfrak{b} = \mathfrak{b}'$ are invertible $\mathcal{O}$-ideals. We then have

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

and it follows that $\mathrm{N}(\mathfrak{a}\mathfrak{b}) = \mathrm{N}\mathfrak{a}\mathrm{N}\mathfrak{b}$. □

18.4 The CM action

Now let $E/\mathbb{C}$ be an elliptic curve with $\mathrm{End}(E) = \mathcal{O}$. Then E 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

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

(the reason for using $E_{\mathfrak{a}^{-1}\mathfrak{b}}$ rather than $E_{\mathfrak{a}\mathfrak{b}}$ will become clear later). The action of the equivalence class $[\mathfrak{a}]$ on the isomorphism class $j(E_\mathfrak{b})$, is then defined by

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

which we can also write as

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

and it is clear that this does not depend on the choice of representatives $\mathfrak{a}$ 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 $\mathrm{cl}(\mathcal{O})$ acts trivially on $\mathrm{Ell}_\mathcal{O}(\mathbb{C})$. 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 $\mathrm{cl}(\mathcal{O})$ on $\mathrm{Ell}_\mathcal{O}(\mathbb{C})$.

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 16.5, and in this case we have $a\mathfrak{b} = \lambda\mathfrak{b}$ for some nonzero $\lambda \in \mathcal{O}$, and then $\mathfrak{a} = \lambda\mathcal{O} = (\lambda)$ is principal. Thus the only element of $\mathrm{cl}(\mathcal{O})$ that fixes *any* element of $\mathrm{Ell}_\mathcal{O}(\mathbb{C})$ is the identity. This implies that the action of $\mathrm{cl}(\mathcal{O})$ is not only faithful, it is *free*: only the identity has a fixed point. The fact that the sets $\mathrm{cl}(\mathcal{O})$ and $\mathrm{Ell}_\mathcal{O}(\mathbb{C})$ have the same cardinality implies that the action must be transitive: if we fix any $j_0 \in \mathrm{Ell}_\mathcal{O}(\mathbb{C})$ the images $[\mathfrak{a}]j_0$ of j_0 under the action of each $[\mathfrak{a}] \in \mathrm{cl}(\mathcal{O})$ must all be distinct, otherwise the action would not be free); there are only $\#\mathrm{Ell}_\mathcal{O}(\mathbb{C}) = \#\mathrm{cl}(\mathcal{O})$ possibilities, so the $\mathrm{cl}(\mathcal{O})$-orbit of j_0 is $\mathrm{Ell}_\mathcal{O}(\mathbb{C})$.

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 *principal homogeneous space* for G, or simply a *G-torsor*. With this terminology, the set $\mathrm{Ell}_\mathcal{O}(\mathbb{C})$ is a $\mathrm{cl}(\mathcal{O})$-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 "difference" or "ratios" of elements of X as group elements. In the case of the $\mathrm{cl}(\mathcal{O})$-torsor $\mathrm{Ell}_{\mathcal{O}}(\mathbb{C})$ 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 $\mathrm{cl}(\mathcal{O})$-torsor $\mathrm{Ell}_{\mathcal{O}}(\mathbb{F}_q)$, as we shall soon do, we cannot readily distinguish the element of $\mathrm{Ell}_{\mathcal{O}}(\mathbb{F}_q)$ that corresponds to $j(E_{\mathcal{O}})$.

18.5 Isogenies over the complex numbers

To better understand the $\mathrm{cl}(\mathcal{O})$-action on $\mathrm{Ell}_{\mathcal{O}}(\mathbb{C})$ we need to look at isogenies between elliptic curves over the complex numbers. Let $L \subseteq L'$ be lattices, and let E and E' be the elliptic curves corresponding to $\mathbb{C}/L$ and $\mathbb{C}/L'$, respectively. The map $\iota\colon \mathbb{C}/L \to \mathbb{C}/L'$ that lifts $z \in \mathbb{C}/L$ to $\mathbb{C}$ and then reduces it modulo L' induces an isogeny $\phi\colon E \to E'$ that makes the following diagram commute:

$$\begin{array}{ccc} \mathbb{C}/L & \xrightarrow{\ \iota\ } & \mathbb{C}/L' \\ \Big\downarrow{\scriptstyle \Phi} & & \Big\downarrow{\scriptstyle \Phi'} \\ E(\mathbb{C}) & \xrightarrow{\ \phi\ } & E'(\mathbb{C}) \end{array}$$

Note that L' contains L as a sublattice, so this is well-defined: equivalence modulo L' implies equivalence modulo L (but not vice versa). The isomorphism Φ sends $z \in \mathbb{C}/L$ to the point $\big(\wp(z;L), \wp'(z;L)\big)$ on E, and the isomorphism Φ' sends $z \in \mathbb{C}/L'$ to the point $\big(\wp(z;L'), \wp'(z;L')\big)$ on E'.

It is clear that the induced map $\phi := \Phi' \circ \iota \circ \Phi^{-1}$ is a group homomorphism; to show that it is an isogeny we need to check that it is also a rational map. To see this, notice that the meromorphic function $\wp(z;L')$ is periodic with respect to L', and therefore also periodic with respect to the sublattice L. It is thus an elliptic function for L, and since it is an even function, it may be expressed as a rational function of $\wp(z;L)$, by Lemma 17.1. Thus

$$\wp(z;L') = \frac{u\big(\wp(z;L)\big)}{v\big(\wp(z;L)\big)}$$

for some polynomials $u, v \in \mathbb{C}[x]$. Similarly, $\wp'(z;L')$ is an odd elliptic function for L, so $\wp'(z:L')/\wp'(z:L)$ is an even elliptic function for L, and we therefore have

$$\wp'(z,L') = \frac{s\big(\wp(z;L)\big)}{t\big(\wp(z;L)\big)}\wp'(z;L),$$

for some $s, t \in \mathbb{C}[x]$. Thus

$$\phi(x,y) = \left(\frac{u(x)}{v(x)}, \frac{s(x)}{t(x)}y\right).$$

The points in the kernel of ϕ are precisely the points $\big(\wp(z;L), \wp'(z;L)\big)$ for which $z \in L'$ (modulo L). It follows that the kernel of ϕ has cardinality $[L' : L]$, and we are in characteristic zero, so the isogeny ϕ is separable and therefore $\deg\phi = |\ker\phi| = [L' : L]$.

We now note that the homothetic lattice $L'' = nL'$ has index n in L, by Lemma 17.15. If we let $E''/\mathbb{C}$ be the elliptic curve corresponding to $\mathbb{C}/L''$ (which is isomorphic to E'), then the inclusion map $\iota\colon \mathbb{C}/L'' \to \mathbb{C}/L$ induces an isogeny $\tilde{\phi}\colon E'' \to E$ of degree n. Composing

$\tilde{\phi}$ with the isomorphism from E' to E'', we obtain the dual isogeny $\hat{\phi}\colon E' \to E$, since the composition $\phi \circ \hat{\phi}$ is precisely the multiplication-by-n map on E'.

If $\mathfrak{a}$ and $\mathfrak{b}$ are invertible $\mathcal{O}$-ideals then we have an isogeny from $E_{\mathfrak{b}}$ to $\mathfrak{a}E_{\mathfrak{b}} = E_{\mathfrak{a}^{-1}\mathfrak{b}}$ induced by the lattice inclusion $\mathfrak{b} \subseteq \mathfrak{a}^{-1}\mathfrak{b}$ (to see that this is an inclusion, note that $\mathfrak{a}\mathfrak{b} \subseteq \mathfrak{b}$). Thus there is an isogeny $\phi_{\mathfrak{a}}$ associated to the action of $\mathfrak{a}$ on $E_{\mathfrak{b}}$ defined in (1). Given any elliptic curve $E/\mathbb{C}$ with endomorphism ring $\mathcal{O}$ and an invertible $\mathcal{O}$-ideal $\mathfrak{a}$, we define the $\mathfrak{a}$-*torsion subgroup*

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

where we view $\alpha \in \mathfrak{a} \subset \mathcal{O} \simeq \operatorname{End}(E)$ as the multiplication-by-α endomorphism.

Theorem 18.11. *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 may assume without loss of generality we assume $E = E_{\mathfrak{b}}$ for some proper $\mathcal{O}$-ideal $\mathfrak{b}$. Let Φ be the isomorphism from $\mathbb{C}/\mathfrak{b} \to E_{\mathfrak{b}}$ that sends z to $(\wp(z), \wp'(z))$. We have

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

This proves (i). We then note that

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

which proves (ii). □

18.6 The Hilbert class polynomial

Let $\mathcal{O}$ be an order of discriminant D in an imaginary quadratic field K. The first main theorem of complex multiplication states that the elements of $\operatorname{Ell}_{\mathcal{O}}(\mathbb{C})$ are algebraic integers that all have the same minimal polynomial over K:

$$H_D(X) = \prod_{j(E) \in \operatorname{Ell}_{\mathcal{O}}(\mathbb{C})} (X - j(E))$$

known as the *Hilbert class polynomial* (of discriminant D).[6] Remarkably, not only do the coefficients of $H_D(X)$ lie in K, they actually lie in $\mathbb{Z}$. Moreover, the theorem states that

[6] Some authors reserve the term Hilbert class polynomial for the case $\mathcal{O} = \mathcal{O}_K$ and call $H_D(X)$ a *ring class polynomial* in general.

the splitting field L of $H_D(X)$ over K has Galois group isomorphic to $\mathrm{cl}(\mathcal{O})$. The roots of $H_D(X)$ are precisely the elements of $\mathrm{Ell}_{\mathcal{O}}(\mathbb{C})$, and the action of the Galois group $\mathrm{Gal}(L/K)$ is precisely the $\mathrm{cl}(\mathcal{O})$-action on $\mathrm{Ell}_{\mathcal{O}}(\mathbb{C})$ defined above.

The first main theorem of complex multiplication is one of the central results of what is known as *class field theory*. We will prove it over the course of the next two lectures.

References

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

18.783 Elliptic Curves
Spring 2015