17 Complex multiplication

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

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

together with an explicit isomorphism

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

where $\wp(z)$ is the Weierstrass $\wp$-function for the lattice L. The map Φ is a group isomorphism that is also an isomorphism of complex manifolds (we did not actually prove the latter fact, but it is clear that Φ is a holomorphic map away from L and this is the only analytic property of Φ that we will use).

17.1 Endomorphism rings of complesx tori and elliptic curves over $\mathbb{C}$

Having established the correspondence between $\mathbb{C}/L$ and $E/\mathbb{C}$, we now wish to make explicit the relationship between endomorphisms of $\mathbb{C}/L$ and endomorphisms of $E/\mathbb{C}$. We know that every endomorphism ϕ of an elliptic curve $y^2 = x^3 + Ax + B$ can be expressed in terms of rational functions in x and y, and it is natural to expect that we should be able to express the corresponding endomorphism of the torus $\mathbb{C}/L$ in terms of rational functions of $\wp(z)$ and $\wp'(z)$, since $x = \wp(z)$ and $y = \wp'(z)$ under the isomorphism Φ. In order to prove this we need the following lemma.

Recall that the set of all elliptic functions for a lattice L forms a field $\mathbb{C}(L)$. We now want to show that $\mathbb{C}(L)$ is generated by the Weierstrass $\wp$-function and its derivative, and moreover, that the subfield of even elliptic functions in $\mathbb{C}(L)$ is generated by the the Weirestrass $\wp$-function alone.

Lemma 17.1. *Let $f(z)$ be an elliptic function with respect to a lattice L. Then $f(z)$ can be written as a rational function of $\wp(z) = \wp(z;L)$ and $\wp'(z)$. Moreover, if $f(z)$ is an even function, then it can be written as a rational function of $\wp(z)$ alone, and if $f(z)$is an even function with no poles outside L it can be written as a polynomial in $\wp(z)$.*

Proof. Every $f \in \mathbb{C}(L)$ can be written as the sum

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

of an even function and an odd function, and every odd function $g \in \mathbb{C}(L)$ is of the form

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

where $g(z)/\wp'(z)$ is an even function. It is thus enough to show that if $f \in \mathbb{C}(L)$ is an even function then it can be written as a rational function of $\wp(z)$.

So let $f \in \mathbb{C}(L)$ be an even function and let $L = [\omega_1, \omega_2]$. We may assume without loss of generality that f does not have poles at $\omega_1/2, \omega_2/2, (\omega_1+\omega_2)/2$: we can always replace f by $g = (af+b)/(cf+d)$ for some $a, b, c, d \in \mathbb{C}$ chosen so that g does not have poles at these points, and provided that $ad - bc \neq 0$ (which we can easily arrange), we have $\mathbb{C}(f) = \mathbb{C}(g)$.

Now suppose that $f(z)$ has a pole of order n at a point w with $2w \notin L$, and consider the even elliptic function

$$(\wp(z) - \wp(w)^n.$$

which has poles only at points in L and a zero of order n at w; here we use the fact that $\wp'(w) \neq 0$ (by Lemma 15.30), so w is a simple zero of $\wp(z) - \wp(w)$. The function

$$(\wp(z) - \wp(w))^n f(z)$$

is then holomorphic at w, and it does not have any poles at points where $f(z)$ is holomorphic except possibly for points in L. The function $f(z)$ has only finitely many poles in any fundamental region, so we can repeat this process until we obtain a polynomial $Q \in \mathbb{C}[x]$ such that $Q(\wp(z))f(z)$ is holomorphic at all points $w \notin L$.

It thus suffices to consider the case where f is holomorphic outside L, which we now assume. The Laurent series for $f(z)$ about 0 can be written in the form

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

with $a_{2n} \neq 0$. If $n \geq 0$, then f is holomorphic on $\mathbb{C}$, and f bounded (since it is periodic), so by Liouville's theorem it is a constant function, hence an element of $\mathbb{C}(\wp)$. If $n > 0$ then

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

is an even elliptic function of order at most $2(n-1)$ that is holomorphic outside L. Repeating the process until $n = 0$, we obtain a function of the form $f(z) - P\big(\wp(z)\big)$, with $P \in \mathbb{C}[x]$, that is holomorphic and bounded on $\mathbb{C}$ and therefore constant. It follows that $f \in \mathbb{C}[\wp]$. $\square$

Theorem 17.2. *Let $L \subseteq \mathbb{C}$ be a lattice, let $E = E_L$ be the corresponding elliptic curve, and let $\Phi\colon \mathbb{C}/L \to E(\mathbb{C})$ be the isomorphism that sends $z \notin L$ to $\big(\wp(z), \wp'(z)\big)$. For any $\alpha \in \mathbb{C}$, the following are equivalent:*

(1) $\alpha L \subseteq L$;

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

(3) *There is a unique* $\phi = \phi_\alpha \in \mathrm{End}(E)$ *such that the following diagram commutes:*

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

where α denotes the endomorphism of $\mathbb{C}/L$ induced by $z \mapsto \alpha z$.

Moreover, for every $\phi \in \mathrm{End}(E)$ there is a unique $\alpha = \alpha_\phi$ such that (1)–(3) hold. The maps $\alpha \mapsto \phi_\alpha$ and $\phi \to \alpha_\phi$ are inverse ring isomorphisms between $\mathrm{End}(E)$ and $\{\alpha \in \mathbb{C} : \alpha L \subseteq L\}$, and we have $\mathrm{N}(\alpha) = \deg \phi = \deg u = \deg v + 1$, where $\phi = \phi_\alpha$ and $u, v \in \mathbb{C}[x]$ are as in (2).

Before beginning the proof, let us be clarify the two ways we may view $\{\alpha \in \mathbb{C} : \alpha L \subseteq L\}$ as a ring. First, it is a subring of $\mathbb{C}$, since it clearly contains 0 and 1 and it closed under addition and multiplication. Second, for any $\alpha \in \mathbb{C}$ the map $z \mapsto \alpha z$ is an endomorphism of the additive group of $\mathbb{C}$, and if $\alpha L \subseteq L$ then this map induces an endomorphism of $\mathbb{C}/L$; note that we can view the product $\alpha\beta$ either as multiplication of complex numbers or as a composition of endomorphisms. It is not necessarily obvious that every endomorphism of $\mathbb{C}/L$ is induced by a map of the form $z \mapsto \alpha z$, but it will follow from the theorem.

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

(1) $\Rightarrow$ (2): Let $\omega \in L$. Then $\wp(\alpha(z+\omega)) = \wp(\alpha z + \alpha\omega) = \wp(\alpha z)$. Thus $\wp(\alpha z)$ is periodic, and $\wp(\alpha z)$ is clearly meromorphic, so it is an elliptic function (with respect to L). It is an even function, so it can be written as a rational function of $\wp(z)$, by Lemma 17.1.

(2) $\Rightarrow$ (1): The function $\wp(\alpha z)$ has a pole at 0, and if it is a rational function of $\wp(z)$ then it is periodic and has a pole at every $\omega \in L$. This implies that $\wp(z)$ has a pole at $\alpha\omega$ for all $\omega \in L$, but $\wp(z)$ is holomorphic outside L so $\alpha\omega \in L$ for a all $\omega \in L$.

(2) $\Rightarrow$ (3): Assume $\wp(\alpha z) = u(\wp(z))/v(\wp(z))$ and let $\phi = \phi_\alpha$ be the rational map

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

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

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

We then have

$$\phi(\Phi(z)) = (\phi(\wp(z), \wp'(z)) = \left(\frac{u(\wp(z))}{v(\wp(z))}, \frac{s(\wp(z))}{t(\wp(z))}\wp'(z)\right) = (\wp(\alpha z), \wp'(\alpha z)) = \Phi(\alpha z).$$

If $\phi' \in \mathrm{End}(E)$ also satisfies $\phi'(\Phi(z)) = \Phi(\alpha z)$ then

$$(\phi - \phi')(\Phi(z)) = \phi(\Phi(z)) - \phi'(\Phi(z)) = \Phi(\alpha z) - \Phi(\alpha(z)) = 0,$$

which implies $\phi' = \phi$, so $\phi = \phi_\alpha$ is unique.

(3) $\Rightarrow$ (1): Let $\phi = \phi_\alpha$. For all $\omega \in L$ we have $\Phi(\alpha\omega) = \phi(\Phi(\omega)) = \phi(0) = 0$, which implies $\alpha\omega \in L$, thus $\alpha L \subseteq L$.

We now prove the "moreover" part of the theorem. For any $\phi \in \mathrm{End}(E)$, the map

$$\Phi^{-1} \circ \phi \circ \Phi$$

is an endomorphism of $\mathbb{C}/L$, since Φ and Φ^{-1} are isomorphisms, and we can lift it to a map $\phi^* \colon \mathbb{C} \to \mathbb{C}$ that is periodic with respect to L. On any sufficiently small open neighborhood U of $0 \in \mathbb{C}$ the map ϕ^* is holomorphic[1] away from 0. We have $\phi^*(0) \in L$ and

$$\phi^*(z_1 + z_2) \equiv \phi^*(z_1) + \phi^*(z_2) \bmod L,$$

[1] An analog of the inverse function theorem holds for holomorphic functions.

and by replacing ϕ^* with $\phi^* - \phi^*(0)$ if necessary, we may assume $\phi^*(0) = 0$. By continuity, $\phi^*(z) \to 0$ as $z \to 0$, so on very sufficiently small U we have

$$\phi^*(z_1 + z_2) = \phi^*(z_1) + \phi^*(z_2)$$

for all $z_1, z_2 \in U$. We now use the definition of the derivative to compute, for any $z \in U$,

$$\begin{aligned}(\phi^*)'(z) &= \lim_{h\to 0} \frac{\phi^*(z+h) - \phi^*(z)}{h} \\ &= \lim_{h\to 0} \frac{\phi^*(z) + \phi^*(h) - \phi^*(z)}{h} \\ &= \lim_{h\to 0} \frac{\phi^*(0+h) - \phi^*(0)}{h} = (\phi^*)'(0).\end{aligned}$$

Thus the derivative of ϕ^* is equal to a constant $\alpha := \alpha_\phi := (\phi^*)'(0)$ at all $z \in U$, and $\phi^*(z) = \alpha z$ for all $z \in U$. For any $z \in \mathbb{C}$, we may choose $n \in \mathbb{Z}$ such that $\frac{z}{n} \in U$. Thus

$$\phi^*(z) = n\phi^*\left(\frac{z}{n}\right) = n\alpha\frac{z}{n} = \alpha z$$

for all $z \in \mathbb{C}$, so ϕ^* is the multiplication-by-α map $z \mapsto \alpha z$ on $\mathbb{C}/L$. For all $\omega \in L$ we must have $\phi^*(\omega) = \alpha\omega \in L$, since ϕ^* induces an endomorphism of $\mathbb{C}/L$, thus $\alpha L \subseteq L$, and α satisfies the equivalent conditions (1)–(3). By construction we have $\phi(\Phi(z)) = \Phi(\alpha_\phi z)$, so $\phi = \phi_\alpha$, since ϕ_α is unique. Conversely, if $\phi(\Phi(z)) = \Phi(\alpha' z)$ for some α' then $\alpha' = \phi^*$, so $\alpha = \alpha_\phi$ is unique and the maps $\alpha \mapsto \phi_\alpha$ and $\phi \mapsto \alpha_\phi$ are inverse bijections.

We now show that the map $\Psi\colon \mathrm{End}(E) \to \{\alpha \in \mathbb{C} : \alpha L \subseteq L\}$ that sends ϕ to α_ϕ is a ring homomorphism. Clearly, $\Psi(0) = 0$ and $\Psi(1) = 1$. Let $\phi_1, \phi_2 \in \mathrm{End}(E)$. Then

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

since Φ is an isomorphism, and

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

Thus Ψ is a ring homomorphism and therefore an isomorphism, since it is a bijection.

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

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

which has integer coefficients and discriminant $\operatorname{tr}(\phi)^2 - 4\deg(\phi) \le 0$. Thus either $\alpha \in \mathbb{Z}$ or α is an algebraic integer in an imaginary quadratic field, and in either case we can compute its trace $\mathrm{T}(\alpha) = \alpha + \bar{\alpha} = \operatorname{tr}(\phi)$ and norm $\mathrm{N}(\alpha) = \alpha\bar{\alpha} = \deg\phi$.

Finally, we note that by (2) we can write $v(\wp(z))\wp(\alpha z) = u(\wp(z))$. The functions $u(\wp(z))$ and $v(\wp(z))$ have poles of order $2\deg u$ and $2\deg v$ at zero, respectively, while $\wp(\alpha z)$ has a pole of order 2 at zero, so we must have $\deg u = \deg v + 1$ and therefore

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

where $\phi = \phi_\alpha = \left(\frac{u(x)}{v(x)}, \frac{s(x)}{t(x)}y\right)$ as above. □

Corollary 17.3. *Let E be an elliptic curve defined over $\mathbb{C}$. Then $\mathrm{End}(E)$ is commutative and therefore isomorphic to either $\mathbb{Z}$ or an order in an imaginary quadratic field.*

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

Remark 17.4. Corollary 17.3 applies to elliptic curves over $\mathbb{Q}$, and over number fields, since these are subfields of $\mathbb{C}$, and it can be extended to arbitrary fields of characteristic 0 via the Lefschetz principle; see [1, Thm. VI.6.1].

Remark 17.5. Theorem 17.2 explains the origin of the term *complex multiplication* (CM). When $\mathrm{End}(E_L)$ is bigger than $\mathbb{Z}$ the extra endomorphisms in $\mathrm{End}(E_K)$ all correspond to multiplication-by-α maps in $\mathrm{End}(\mathbb{C}/L)$ for some (non-real) $\alpha \in \mathbb{C}$.

17.2 Elliptic curves with a given endomorphism ring

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

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

In order to simplify the discussion, it will be convenient to view these isomorphism as equalities. This is clear for the isomorphism on the right, since every endomorphism $\alpha\colon \mathbb{C}/L \to \mathbb{C}/L$ is induced by a map $z \mapsto \alpha z$. For the isomorphism on the left, note that $\mathrm{End}^0(E_L)$ is isomorphic to either $\mathbb{Q}$ or an imaginary quadratic field, so we can always embed $\mathrm{End}^0(E_L)$ in $\mathbb{C}$. Once we have done this, provided that we regard $\mathrm{End}(E_L)$ as a subring of $\mathrm{End}^0(E_L)$ (via the canonical injection $\phi \mapsto \phi \otimes 1$), we actually have an equality $\mathrm{End}(E_L) = \{\alpha \in \mathbb{C} : \alpha L \subseteq L\}$; moreover, when $\mathrm{End}(\mathbb{C}/L)$ is an imaginary quadratic order $\mathcal{O}$, we can choose the embedding of $\mathrm{End}^0(E_L)$ into $\mathbb{C}$ so that each multiplication-by-α endomorphism of $\mathbb{C}/L$ corresponds to $\alpha \in \mathrm{End}(E_L)$ (as opposed to $\hat{\alpha}$). This is known as the *normalized identification* of $\mathrm{End}(E_L)$ with $\mathrm{End}(\mathbb{C}/L) = \mathcal{O}$, which we henceforth assume.

We now want to focus on the CM case, where $\mathrm{End}(E_L)$ is an order $\mathcal{O}$ in an imaginary quadratic field K. The order $\mathcal{O}$ is itself a lattice, and we would like to understand how the lattices L and $\mathcal{O}$ are related. In particular, for which lattices L do we have $\mathrm{End}(E_L) = \mathcal{O}$? An obvious candidate is $L = \mathcal{O}$. If $\alpha \in \mathrm{End}(E_{\mathcal{O}})$, then $\alpha\mathcal{O} \subseteq \mathcal{O}$, by (1), and therefore $\alpha \in \mathcal{O}$, since the ring $\mathcal{O}$ contains 1. Conversely, if $\alpha \in \mathcal{O}$, then $\alpha\mathcal{O} \subseteq \mathcal{O}$, since $\mathcal{O}$ is closed under multiplication, and therefore $\alpha \in \mathrm{End}(E_{\mathcal{O}})$, by (1); thus $\mathrm{End}(E_{\mathcal{O}}) = \mathcal{O}$.

The same holds for any lattice that is homothetic to $\mathcal{O}$. Indeed, the set $\{\alpha \in \mathbb{C}\colon \mathfrak{a}L \subseteq L\}$ does not change if we replace L with $L' = \lambda L$ for any $\lambda \in \mathbb{C}^\times$, so we are really only interested in lattices up to homethety (and elliptic curves up to isomorphism). So the question now before us is whether there are any lattices L not homothetic to $\mathcal{O}$ for which we have $\mathrm{End}(E_L) = \mathcal{O}$.

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

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

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

so $[m,i] = \frac{2m}{1+i}[1,i]$ is homothetic to $\mathcal{O}$, as is $[n,i] = \frac{2n}{1+i}[1,i]$. This is a direct consequence of the fact that $\mathbb{Z}[i]$ is a principal ideal domain (PID), which implies that every ideal in $\mathbb{Z}[i]$ is homothetic to $\mathbb{Z}[i]$ as a lattice. Of course most imaginary quadratic orders are not PIDs (including all but two of the orders[2] in $\mathbb{Q}(i)$), but even when this is not the case there are only finitely many non-homothetic ideals in $\mathcal{O}$ (as discussed below), even though there are infinitely many distinct $\mathcal{O}$-ideals.

The second complication is that while every lattice L for which $\mathrm{End}(E_L) = \mathcal{O}$ is an $\mathcal{O}$-ideal, the converse does not hold (unless $\mathcal{O}$ is the maximal order $\mathcal{O}_K$). If we start with an arbitrary $\mathcal{O}$-ideal L, it is clear that the set

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

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

Definition 17.6. Let $\mathcal{O}$ be an order in an imaginary quadratic field K, and let L be an $\mathcal{O}$-ideal. We say that L is a *proper* $\mathcal{O}$-ideal if $\mathcal{O}(L) = \mathcal{O}$.

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

Definition 17.7. Let $\mathcal{O}$ be an order in an imaginary quadratic field. Two $\mathcal{O}$-ideals $\mathfrak{a}$ and $\mathfrak{b}$ are said to be *equivalent* if $\gamma\mathfrak{a} = \delta\mathfrak{b}$ for some $\gamma, \delta \in \mathcal{O}$; we can also write this as $(\gamma)\mathfrak{a} = (\delta)\mathfrak{b}$, where (γ) and (δ) denote principal ideals and $(\gamma)\mathfrak{a}$ and $(\gamma)\delta$ are ideal products.

Recall that the product of two $\mathcal{O}$-ideals $\mathfrak{a}$ and $\mathfrak{b}$ is the ideal generated by all products ab with $a \in \mathfrak{a}$ and $b \in \mathfrak{b}$, and that ideal multiplication is commutative and associative. It is enough to consider products of generators, so if $\mathfrak{a} = [a_1, a_2]$ and $\mathfrak{b} = [b_1, b_2]$, then $\mathfrak{ab}$ is the ideal generated by the four elements $a_1b_1, a_1b_2, a_2b_1, a_2b_2$. Since $\mathfrak{ab}$ is an $\mathcal{O}$-ideal, it is a free $\mathbb{Z}$-module of rank 2 and be written as a lattice $[c_1, c_2]$, where c_1 and c_2 are $\mathcal{O}$-linear combinations of $a_1b_1, a_1b_2, a_2b_1, a_2b_2$. Note that ideal multiplication respects equivalence:

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

Definition 17.8. Let $\mathcal{O}$ be an order in an imaginary quadratic field. The *ideal class group* $\mathrm{cl}(\mathcal{O})$ is the multiplicative group of equivalence classes of proper $\mathcal{O}$-ideals.

Remark 17.9. One can also define $\mathrm{cl}(\mathcal{O})$ using *fractional* $\mathcal{O}$-ideals, which are the lattices in K that are homothetic to $\mathcal{O}$-ideals (so of the form $\frac{1}{a}\mathfrak{a}$ for some nonzero $a \in \mathcal{O}$ and $\mathcal{O}$-ideal $\mathfrak{a}$), equivalently, finitely generated $\mathcal{O}$-modules that lie in K. One then defines $\mathrm{cl}(\mathcal{O})$ as the quotient of the group of invertible fractional $\mathcal{O}$-ideals modulo principal fractional $\mathcal{O}$-ideals.

[2]This is an important point to remember: not all orders are maximal orders. Even fields of class number one contain infinitely many orders that are not principle ideal domains.

This approach is used in most number theory textbooks, but the definition in terms of equivalence classes of proper $\mathcal{O}$-ideals is better motivated in our setting and follows the historical development of the subject. For practical computations (and many theoretical applications), it is most efficient to represent $\mathrm{cl}(\mathcal{O})$ using binary quadratic forms that correspond to proper $\mathcal{O}$-ideals, modulo an equivalence relation that corresponds to equivalence of $\mathcal{O}$-ideals; this correspondence is explored in Problem Set 9.

It is not *a priori* clear that the set $\mathrm{cl}(\mathcal{O})$ is actually a group. It is clearly closed under an associative multiplication and contains an identity element (the class of principal ideals), hence an abelian monoid, but it s not immediately obvious that every element has an inverse. We will give an explicit proof of this in the next lecture (an alternative proof is given in Problem Set 9, where it is also shown that $\mathrm{cl}(\mathcal{O})$ is finite).

Even without necessarily knowing that $\mathrm{cl}(\mathcal{O})$ is a group, our discussion above makes the following proposition clear.

Theorem 17.10. *Let $\mathcal{O}$ be an order in an imaginary quadratic field. There is a one-to-one correspondence between elements of the ideal class group $\mathrm{cl}(\mathcal{O})$ and homethety classes of lattices $L \subseteq \mathbb{C}$ for which $\mathrm{End}(E_L) \simeq \mathcal{O}$.*

17.3 Discriminants

To streamline our work with imaginary quadratic orders, we define the *discriminant* of $\mathcal{O}$, which is a negative integer that is a square modulo 4 that uniquely determines $\mathcal{O}$.

Definition 17.11. The *discriminant* of an imaginary quadratic order $\mathcal{O} = [\alpha, \beta]$ is

$$\mathrm{disc}(\mathcal{O}) = \det \begin{pmatrix} \alpha & \beta \\ \bar{\alpha} & \bar{\beta} \end{pmatrix}^2.$$

Lemma 17.12. *Let $\mathcal{O} = [\alpha, \beta]$ be an order in an imaginary quadratic field. The discriminant $\mathrm{disc}(\mathcal{O})$ does not depend on the choice of basis $[\alpha, \beta]$ and it is a negative integer that is a square modulo 4.*

Proof. We may regard $\mathbb{C}$ as an $\mathbb{R}$-vector space embedded in $\mathbb{R}^3$ via maps $1 \mapsto (1,0,0)$ and $i \mapsto (0,1,0)$. Under this embedding α and β, correspond to the vectors $\vec{\alpha} = (\mathrm{re}\,\alpha, \mathrm{im}\,\alpha, 0)$ and $\vec{\beta} = (\mathrm{re}\,\beta, \mathrm{im}\,\beta, 0)$, and the magnitude of their cross product is

$$|\vec{\alpha} \times \vec{\beta}| = |(0, 0, \mathrm{re}\,\alpha\,\mathrm{im}\,\beta - \mathrm{re}\,\beta\,\mathrm{im}\,\alpha)| = |\,\mathrm{im}(\alpha\bar{\beta} - \beta\bar{\alpha})/2|,$$

which we note is the area of the the parallelogram spanned by α and β. We also have

$$|\mathrm{disc}(\mathcal{O})| = |(\alpha\bar{\beta} - \beta\bar{\alpha})^2| = |\,\mathrm{im}(\alpha\bar{\beta} - \beta\bar{\alpha})|^2,$$

thus

$$|\mathrm{disc}(\mathcal{O})| = 4|\vec{\alpha} \times \vec{\beta}|^2.$$

The RHS is 4 times the square of the area of a fundamental parallelogram of the lattice $\mathcal{O}$, which is independent of the choice of basis, and the sign of $\mathrm{disc}(\mathcal{O})$ is always negative, since $\alpha\bar{\beta} - \beta\bar{\alpha}$ is purely imaginary. Thus $\mathrm{disc}(\mathcal{O})$ is independent of the choice of basis.

Let us now write $\mathcal{O} = [1, \tau]$, where τ is an algebraic integer satisfying an integer quadratic equation $x^2 + bx + c$ with $b^2 - 4c < 0$ not a perfect square. We then have

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

which shows that $\operatorname{disc}(\mathcal{O})$ is a negative integer that is a square modulo 4. □

Definition 17.13. A negative integer D that is a square modulo 4 is an (imaginary quadratic) *discriminant*. Discriminants that are not the product of a square and a discriminant are said to be *fundamental*; every discriminant can be written uniquely as the product of a square and a fundamental discriminant.

For $D \equiv 1 \bmod 4$ the property of being a fundamental discriminant is equivalent to being square-free. For $D \equiv 0 \bmod 4$, if $D/4$ is square-free and not a discriminant, then D is 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 17.14. *Let D be an imaginary quadratic discriminant. There is a unique imaginary quadratic order $\mathcal{O}$ with $\operatorname{disc}(\mathcal{O}) = u^2 D_K$, where D_K is the fundamental discriminant of the maximal order $\mathcal{O}_K$ in $K = \mathbb{Q}(\sqrt{\operatorname{disc}(\mathcal{O})})$, and $u = [\mathcal{O}_K : \mathcal{O}]$ is the conductor of $\mathcal{O}$.*

Proof. Write $D = \operatorname{disc}(\mathcal{O})$ as $D = u^2 D_K$, with $u \in \mathbb{Z}_{>0}$ and D_K a fundamental discriminant. Let $K = \mathbb{Q}(\sqrt{D})$, and let $\mathcal{O}_K$ be its maximal order. Choose a shortest non-integer vector $\omega \in \mathcal{O}_K$, with minimal polynomial $x^2 + bx + c$, so that $\mathcal{O}_K = [1, \omega]$. Then $b^2 - 4c$ must equal D_K: if not, we could make ω shorter by replacing it with ω/v, where $b^2 - 4c = v^2 D_K$, since then $v|b$, $v|c$ and ω/v is a root of $x^2 + (b/v)x + c/b \in \mathbb{Z}[x]$ hence an element of $\mathcal{O}_K$. From (2) we see that $\operatorname{disc}(\mathcal{O}_K) = D_K$. The order $\mathcal{O} = [1, u\omega]$ then has discriminant $(u\bar{\omega} - u\omega)^2 = u^2 D_K = D$.

Conversely, if $\mathcal{O} = [1, \tau]$ is any order with discriminant D, than τ must be the root of a quadratic equation with discriminant D, by (2); therefore $\tau \in K$ and $\mathcal{O} \subseteq \mathcal{O}_K$. We must have $[\mathcal{O}_K : \mathcal{O}] = u$, since $\operatorname{disc}(\mathcal{O}) = u^2 \operatorname{disc}(\mathcal{O}_K)$ and the discriminant is proportional to the square of the area of a fundamental parallelogram. Lemma 17.15 implies $u\mathcal{O}_k \subseteq \mathcal{O}$, so $u\omega \in \mathcal{O}$, and therefore $[1, u\omega] \subseteq [1, \tau]$. Equality must hold, since both orders have index u in $\mathcal{O}_K$. Thus $[1, \tau] = [1, u\omega]$, so $[1, u\omega]$ is the unique order of discriminant D. □

Lemma 17.15. *If L' is an index n sublattice of L then nL is an index n sublattice of L'.*

Proof. Without loss of generality, we may assume $L = [1, \tau]$ and $L' = [a + b\tau, c + d\tau]$. As shown in the proof of Theorem 17.14, for any complex lattice $[\omega_1, \omega_2]$ the area of its fundamental parallelogram is given by $|\operatorname{im}(\omega_1\bar{\omega}_2 - \omega_2\bar{\omega}_1)|/2$. Comparing areas of the fundamental parallelograms of L and L', we have

$$\begin{aligned} n|\operatorname{im}(\tau - \bar{\tau})|/2 &= |\operatorname{im}((a + b\tau)(c + d\bar{\tau}) - (c + d\tau)(a + b\bar{\tau}))|/2 \\ n|\operatorname{im}\tau| &= |(a + b\operatorname{re}\tau)d\operatorname{im}\tau - (c + d\operatorname{re}\tau)b\operatorname{im}\tau| \\ n &= |ad - bc|, \end{aligned}$$

Thus $d(a + b\tau) - b(c + d\tau) = \pm n$ and $a(c + d\tau) - c(a + b\tau) = \pm n\tau$, therefore $nL \subseteq L'$. We then have $[L : L'] = n$ and $[L : L'][L' : nL] = [nL : L] = n^2$, so $[L' : nL] = n$. □

References

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

18.783 Elliptic Curves

Spring 2015