A key ingredient to improving the efficiency of elliptic curve primality proving (and many other algorithms) is the ability to directly *construct* an elliptic curve $E/\mathbb{F}_q$ with a specified number of rational points, rather than generating curves at random until a suitable curve is found. To do this we need to develop the theory of *complex multiplication*.

Recall from Lecture 7 that for any elliptic curve E/k, the multiplication-by-n maps $[n]$ form a subring of the endomorphism ring $\mathrm{End}(E)$. This subring is isomorphic to $\mathbb{Z}$, and it is notationally convenient to simply identify it with $\mathbb{Z}$.[1] Thus the inclusion $\mathbb{Z} \subseteq \mathrm{End}(E)$ always holds. For curves with complex multiplication, this inclusion is strict.

Definition 14.1. An elliptic curve E/k has *complex multiplication (CM)* if $\mathrm{End}(E) \neq \mathbb{Z}$.

As we shall see in later lectures, the term arises from the fact that endomorphisms of elliptic curves over $\mathbb{C}$ can be viewed as "multiplication-by-α" maps, for some complex number α. If $\mathrm{End}(E) = \mathbb{Z}$ then α is an integer, and in general, α is an algebraic integer.

14.1 Endomorphism rings of elliptic curves

Our first objective is to classify the different endomorphism rings that are possible. We will consider this problem in its full generality, for an elliptic curve E over a field k of characteristic p (possibly $p = 0$). We begin by summarizing some of the basic facts about $\mathrm{End}(E)$ that we will need, several of which we saw previously in Lecture 7.

Lemma 14.2. *$\mathbb{Z}$ lies in the center of $\mathrm{End}(E)$.*

Proof. $(n\phi)(P) = n\phi(P) = \phi(nP) = (\phi n)(P)$ for all $n \in \mathbb{Z}, \phi \in \mathrm{End}(E)$, and $P \in E(\bar{k})$. □

Lemma 14.3. *$\mathrm{End}(E)$ has no zero divisors.*

Proof. Recall that every nonzero isogeny α has a finite kernel, since $|\ker \alpha| \leq \deg \alpha$. If $\alpha, \beta \in \mathrm{End}(E)$ are both nonzero, then both have finite kernels, and therefore $\alpha\beta$ has a finite kernel, since the preimage of $\ker \beta$ under α must be finite. Therefore $\alpha\beta \neq 0$. □

Recall that every nonzero isogeny $\alpha\colon E_1 \to E_2$ has a unique *dual isogeny* $\hat{\alpha}\colon E_2 \to E_1$ for which $\hat{\alpha}\alpha = [\deg \alpha]$. The dual of an endomorphism is clearly an endomorphism, and for every nonzero $n \in \mathbb{Z}$ we have $\hat{n} = n$. We analogously define $\hat{0} = 0$, and note that $\hat{0}0 = \deg 0$. The *trace* of an endomorphism is defined as $\mathrm{tr}\,\phi = \phi + \hat{\phi}$, and for all $\phi \in \mathrm{End}(E)$ and all positive integers n prime to p we have

$$\deg \phi \equiv \det \phi_n \bmod n \qquad \text{and} \qquad \mathrm{tr}\,\phi \equiv \mathrm{tr}\,\phi_n \bmod n,$$

where ϕ_n denotes the restriction of ϕ to $E[n] \simeq \mathbb{Z}/n\mathbb{Z} \oplus \mathbb{Z}/n\mathbb{Z}$; see Theorem 7.14.

Lemma 14.4. *For all $\phi, \lambda \in \mathrm{End}(E)$, we have $\deg(\phi\lambda) = \deg \phi \deg \lambda$.*

[1] With this identification in mind, we often write n instead of $[n]$. Note that $n\phi = \phi + \cdots + \phi$ is the same endomorphism as the composition $[n] \circ \phi$, so there is no risk of confusion.

Proof. For any ϕ and λ we may pick an integer $n \perp p$ such that n is strictly greater than both $\deg(\phi\lambda)$ and $\deg\phi\deg\lambda$. We then have

$$\deg(\phi\lambda) \equiv \det(\phi_n\lambda_n) \equiv \det\phi_n \det\lambda_n \equiv \deg\phi\deg\lambda \bmod n,$$

and therefore the nonnegative integers $\deg(\phi\lambda)$ and $\deg\phi\deg\lambda$ must be equal. □

We now now show that, as an operator on $\mathrm{End}(E)$, the dual map is an anti-commutative linear involution, also called an *anti-involution*.

Theorem 14.5. *Let ϕ and λ be elements of $\mathrm{End}(E)$ and let a and b be integers. The following properties hold:*

$$\text{(i) } \hat{\hat{\phi}} = \phi, \qquad \text{(ii) } \widehat{\phi\lambda} = \hat{\lambda}\hat{\phi}, \qquad \text{(iii) } \widehat{a\phi + b\lambda} = a\hat{\phi} + b\hat{\lambda}.$$

Proof. Property (i) was proved in Lecture 7 for nonzero isogenies, and note that $\hat{\hat{0}} = \hat{0} = 0$. Property (ii) is immediate if either endomorphism is zero, and otherwise we have

$$(\hat{\lambda}\hat{\phi})(\phi\lambda) = \hat{\lambda}(\deg\phi)\lambda = (\deg\phi)\hat{\lambda}\lambda = \deg\phi\deg\lambda = \deg(\phi\lambda),$$

which implies $\widehat{\phi\lambda} = \hat{\lambda}\hat{\phi}$, by definition. For property (iii) we use Lemma 7.9 to obtain

$$\widehat{a\phi + b\lambda} = \widehat{a\phi} + \widehat{b\lambda} = \hat{\phi}a + \hat{\lambda}b = a\hat{\phi} + b\hat{\lambda},$$

which completes the proof. □

Finally, we recall Theorem 7.13, which states that every endomorphism ϕ satisfies the characteristic equation

$$\phi^2 - \mathrm{tr}(\phi)\phi + \deg\phi = 0. \tag{1}$$

14.2 The endomorphism algebra of an elliptic curve

The additive group of $\mathrm{End}(E)$, like all abelian groups, is a $\mathbb{Z}$-module. Thus we can think of the ring $\mathrm{End}(E)$ as a $\mathbb{Z}$-module with a multiplication operation that is distributive and commutes with scalar multiplication by elements of $\mathbb{Z}$. We now want to "upgrade" our $\mathbb{Z}$-module with multiplication to a $\mathbb{Q}$-vector space with multiplication, that is, a $\mathbb{Q}$-algebra, where the multiplication must be compatible with the vector field operations, but need not be commutative. To do this we take the tensor product of $\mathrm{End}(E)$ with $\mathbb{Q}$.

Definition 14.6. The *endomorphism algebra* of E is $\mathrm{End}^0(E) = \mathrm{End}(E) \otimes_{\mathbb{Z}} \mathbb{Q}$.

General tensor product constructions can be rather abstract (see [1, p. 22] for a quick review of tensor products), but tensoring a $\mathbb{Z}$-module with $\mathbb{Q}$ is the simplest possible case; all we are really doing is extending our ring of scalars $\mathbb{Z}$ to the field $\mathbb{Q}$. With this in mind, we write the tensor $\phi\otimes s$ as $s\phi$. In general, not every element of a tensor product $R \otimes S$ is of the form $r\otimes s$ (an elementary tensor), but in the case of $\mathrm{End}^0(E)$ this is true.

Lemma 14.7. *Every element of $\mathrm{End}^0(E)$ can be written as $s\phi$, with $s \in \mathbb{Q}$ and $\phi \in \mathrm{End}(E)$.*

Proof. It suffices to show that $s_1\phi_1 + s_t\phi_2$ can be written as $s_3\phi_3$, where $s_1, s_2, s_3 \in \mathbb{Q}$ and $\phi_1, \phi_2, \phi_3 \in \mathrm{End}(E)$. Let $s_1 = a/b$ and $s_2 = c/d$ with $a, b, c, d \in \mathbb{Z}$. Then

$$s_1\phi_1 + s_2\phi_2 = \frac{a}{b}\phi_1 + \frac{c}{d}\phi_2 = \frac{ad}{bd}\phi_2 + \frac{bc}{bd}\phi_2 = \frac{1}{bd}\big(ad\phi_1 + bc\phi_2\big),$$

so we may take $s_3 = \frac{1}{bd}$ and $\phi_3 = ad\phi_1 + bc\phi_2$. □

We now extend the dual map to $\mathrm{End}^0(E)$ by scalars, defining $\widehat{s\phi} = s\hat{\phi}$ for all $s \in \mathbb{Q}$. This implies that $\hat{s} = s$ for all $s \in \mathbb{Q}$ (take $\phi = 1$), thus $\hat{\hat{\alpha}} = \alpha$ holds for all $\alpha \in \mathrm{End}^0(E)$. We also have $\widehat{\alpha\beta} = \hat{\beta}\hat{\alpha}$ for all $\alpha, \beta \in \mathrm{End}^0(E)$, since this holds for elements of $\mathrm{End}(E)$ and scalars commute. The fact that the dual map is $\mathbb{Z}$-linear on $\mathrm{End}(E)$ implies that it is $\mathbb{Q}$-linear on $\mathrm{End}^0(E)$. Thus all three properties of Theorem 14.5 hold for the dual map on End^0, and it is an anti-involution, also known as the *Rosati involution*.

The Rosati involution allows us to extend the notions of degree and trace on $\mathrm{End}(E)$ to a norm N and a trace T defined on all of $\mathrm{End}^0(E)$.

Definition 14.8. Let $\alpha \in \mathrm{End}^0(E)$. The (reduced) *norm* of α is $N\alpha = \alpha\hat{\alpha}$ and the *trace* of α is $T\alpha = \alpha + \hat{\alpha}$.

With these definitions the characteristic equation (1) also holds in $\mathrm{End}^0(E)$, since for any $\alpha \in \mathrm{End}^0(E)$ we have

$$\begin{aligned} \alpha^2 - T(\alpha)\alpha + N\alpha &= \alpha^2 - (\alpha + \hat{\alpha})\alpha + \alpha\hat{\alpha} \\ &= \alpha^2 - \alpha^2 - \hat{\alpha}\alpha + \alpha\hat{\alpha} \\ &= 0. \end{aligned}$$

Here we have used the fact that α commutes with its dual $\hat{\alpha}$ (this is true in $\mathrm{End}(E)$, and scalars commute with every element of $\mathrm{End}^0(E)$).

We now show that both $N\alpha$ and $T\alpha$ lie in $\mathbb{Q}$, and derive some other useful properties of the norm and the trace.

Lemma 14.9. *For all $\alpha \in \mathrm{End}^0(E)$ we have $N\alpha \in \mathbb{Q}_{\geq 0}$, with $N\alpha = 0$ if and only if $\alpha = 0$.*

Proof. Write $\alpha = c\phi$, with $c \in \mathbb{Q}$ and $\phi \in \mathrm{End}(E)$. Then $N\alpha = \alpha\hat{\alpha} = c^2 \deg\phi \geq 0$. If either c or ϕ is zero then $\alpha = 0$ and $N\alpha = 0$, and otherwise $N\alpha > 0$. □

Corollary 14.10. *Every nonzero $\alpha \in \mathrm{End}^0(E)$ has a multiplicative inverse α^{-1}.*

Proof. Let $\beta = \hat{\alpha}/N\alpha$. Then $\alpha\beta = \alpha\hat{\alpha}/N\alpha = N\alpha/N\alpha = 1$ (and we similarly have $\beta\alpha = (\hat{\alpha}/N\alpha)\alpha = \hat{\alpha}\alpha/N\alpha = \alpha\hat{\alpha}/N\alpha = N\alpha/N\alpha = 1$), so $\beta = \alpha^{-1}$. □

The corollary implies that $\mathrm{End}^0(E)$ is a *division ring* (also known as a skew field). Thus $\mathrm{End}^0(E)$ is a field if and only if it is commutative. As we saw in Problem Set 4, $\mathrm{End}(E)$, and therefore $\mathrm{End}^0(E)$, need not be commutative, so $\mathrm{End}^0(E)$ is not necessarily a field.

Lemma 14.11. *Let $\alpha, \beta \in \mathrm{End}^0(E)$ and $c, d \in \mathbb{Q}$. The following hold:*

(i) $T\alpha = 1 + N\alpha - N(1 - \alpha) \in \mathbb{Q}$;

(ii) $T(c\alpha + d\beta) = cT\alpha + dT\beta$;

(iii) *If $T\alpha = 0$ then $\alpha^2 = -N\alpha \in \mathbb{Q}_{\leq 0}$.*

Proof. For (i) we have $1 + \alpha\hat{\alpha} - (1 - \alpha)(1 - \hat{\alpha}) = \alpha + \hat{\alpha} = T\alpha$, which must lie in $\mathbb{Q}$ since $N\alpha$ and $N(1 - \alpha)$ lie in $\mathbb{Q}$. For (ii) we note that the trace map on $\mathrm{End}(E)$ is $\mathbb{Z}$-linear and the Rosati involution fixes $\mathbb{Q}$. For (iii) we apply $\alpha^2 - (T\alpha)\alpha + N\alpha = 0$. □

We are now ready to prove our main result, which classifies the possible endomorphism algebras of an elliptic curve.

Theorem 14.12. $\mathrm{End}^0(E)$ *is isomorphic to one of the following:*

(i) *The field of rational numbers* $\mathbb{Q}$*;*

(ii) *An imaginary quadratic number field* $\mathbb{Q}(\alpha)$*, with* $\alpha^2 < 0$*;*

(iii) *A quaterion algebra of the form*[2]

$$\mathbb{Q} + \alpha\mathbb{Q} + \beta\mathbb{Q} + \alpha\beta\mathbb{Q},$$

where $\alpha^2 < 0$*,* $\beta^2 < 0$*, and* $\alpha\beta = -\beta\alpha$*.*

Note that $\mathrm{End}^0(E)$ is commutative if and only if we are in one of the first two cases.

Proof. The $\mathbb{Q}$-algebra $\mathrm{End}^0(E)$ obviously contains $\mathbb{Q}$. If it equals $\mathbb{Q}$, then we are in case (i). Otherwise, choose $\alpha \in \mathrm{End}^0(E) \setminus \mathbb{Q}$. By replacing α with $\alpha - \frac{1}{2}T\alpha$, we may assume without loss of generality that $T\alpha = 0$. Then, by Lemma 14.11, $\alpha^2 < 0$, so $\mathbb{Q}(\alpha)$ is an imaginary quadratic number field. If $\mathrm{End}^0(E) = \mathbb{Q}(\alpha)$, then we are in case (ii).

Otherwise, choose $\beta \in \mathrm{End}^0(E) \setminus \mathbb{Q}(\alpha)$. As above, we assume without loss of generaility that $T\beta = 0$ (so $\beta^2 < 0$). Furthermore, by replacing β with

$$\beta - \frac{T(\alpha\beta)}{2\alpha^2}\alpha \tag{2}$$

we can assume that $T(\alpha\beta) = 0$ (one can check this by multiplying (2) by α and taking the trace). Thus $T\alpha = T\beta = T(\alpha\beta) = 0$. This means that $\alpha = -\hat{\alpha}$, $\beta = -\hat{\beta}$, and $\alpha\beta = -\widehat{\alpha\beta} = -\hat{\beta}\hat{\alpha}$. Substituting the first two equalities into the third, $\alpha\beta = -\beta\alpha$.

To prove that $\mathbb{Q}(\alpha, \beta)$ is a quaternion algebra, it only remains to show that 1, α, β, and $\alpha\beta$ are linearly independent over $\mathbb{Q}$. By construction, 1, α, and β are linearly independent. Now suppose for the sake of contradiction that

$$\alpha\beta = a + b\alpha + c\beta,$$

for some $a, b, c \in \mathbb{Q}$. We then have

$$(\alpha\beta)^2 = (a^2 + b^2\alpha^2 + c^2\beta^2) + 2a(b\alpha + c\beta).$$

The LHS lies in $\mathbb{Q}$, since $T(\alpha\beta) = 0$, as does the first term on the RHS, since $T\alpha = T\beta = 0$. Thus $b\alpha + c\beta$ must lie in $\mathbb{Q}$, and it follows that both b and c are nonzero, since $\alpha, \beta \notin \mathbb{Q}$. But if we let $d = b\alpha + c\beta$, then $\beta = (d - b\alpha)/c$ lies $\in \mathbb{Q}(\alpha)$, which is our desired contradiction.

We now claim that $\mathrm{End}^0(E) = \mathbb{Q}(\alpha, \beta)$. Suppose not. Let $\gamma \in \mathrm{End}^0(E) \setminus \mathbb{Q}(\alpha, \beta)$. As with β, we may assume without loss of generality that $T\gamma = 0$ and $T(\alpha\gamma) = 0$, which implies $\alpha\gamma = -\gamma\alpha$, as above. Then $\alpha\beta\gamma = -\beta\alpha\gamma = \beta\gamma\alpha$, so α commutes with $\beta\gamma$. By Lemma 14.13 below, $\beta\gamma \in \mathbb{Q}(\alpha)$. But then $\gamma \in \mathbb{Q}(\alpha, \beta)$, which is a contradiction. □

Lemma 14.13. *Suppose that* $\alpha, \beta \in \mathrm{End}^0(E)$ *commute and that* $\alpha \notin \mathbb{Q}$*. Then* $\beta \in \mathbb{Q}(\alpha)$*.*

Proof. As in the proof of the Theorem 14.12, we can linearly transform α and β to some $\alpha' = \alpha + a$ and $\beta' = \beta + b\alpha + c$, where $a, b, c \in \mathbb{Q}$, so that $T\alpha' = T\beta' = T(\alpha'\beta') = 0$, and therefore $\alpha'\beta' = -\beta'\alpha'$ (set $a = \frac{1}{2}T\alpha$ and use (2) to determine b and c). We also have $\alpha'\beta' = \beta'\alpha'$, since if α and β commute then so do α' and β', since they are polynomials in α and β. But then $2\alpha'\beta' = 0$, which means $\alpha' = 0$ or $\beta' = 0$, since $\mathrm{End}^0(E)$ has no zero divisors. We cannot have $\alpha' = 0$, since $\alpha \notin \mathbb{Q}$, so $\beta' = 0$, which implies $\beta \in \mathbb{Q}(\alpha)$. □

[2] A general quaternion algebra over $\mathbb{Q}$ has $\alpha^2, \beta^2 \in \mathbb{Q}$ and $\alpha\beta = -\beta\alpha$. The constraint $\alpha^2, \beta^2 < 0$ make this a *definite* quaternion algebra, which is the only kind of quaternion algebra we shall consider.

14.3 Orders

Having classified the possible endomorphism algebras $\mathrm{End}^0(E)$, our next task is to classify the possible endomorphism rings $\mathrm{End}(E)$. We begin with the following corollary to Theorem 14.12.

Corollary 14.14. *The additive group of* $\mathrm{End}(E)$ *is isomorphic to* $\mathbb{Z}^r$*, where* r *is* $1, 2,$ *or* 4*, depending on whether* $\mathrm{End}^0(E)$ *is isomorphic to* $\mathbb{Q}$*, and imaginary quadratic field, or a definite quaternion algebra, respectively.*

Proof. It follows from Lemma 14.3 that the additive group of $\mathrm{End}(E)$ is torsion-free. The fact that every element of $\mathrm{End}(E)$ satisfies a monic quadratic equation with integer coefficients implies that $\mathrm{End}(E)$ is finitely generated (the proof is essentially the same as the proof that the ring of integers of a number field is finitely generated, see either [1, Ch. 2] or [3, Ch. 2]). Thus the additive group of $\mathrm{End}(E)$ is isomorphic to $\mathbb{Z}^r$ for some r, and r must equal to the dimension of $\mathrm{End}^0(E)$ as a $\mathbb{Q}$-vector space, since $\mathrm{End}^0(E) = \mathrm{End}(E) \otimes \mathbb{Q}$. The corollary follows. □

Definition 14.15. Let $\mathcal{K}$ be a $\mathbb{Q}$-algebra of finite dimension r as a vector space over $\mathbb{Q}$. An *order* $\mathcal{O}$ in $\mathcal{K}$ is a subring whose additive group is isomorphic to $\mathbb{Z}^r$. Equivalently, $\mathcal{O}$ is a subring that is finitely generated as a $\mathbb{Z}$-module and for which $\mathcal{K} = \mathcal{O} \otimes \mathbb{Q}$.

It follows from Corollary 14.14 that the endomorphism ring $\mathrm{End}(E)$ is an order in the $\mathbb{Q}$-algebra $\mathrm{End}^0(E) = \mathrm{End}(E) \otimes \mathbb{Q}$. Note that if $\mathrm{End}^0(E) = \mathbb{Q}$, then we must have $\mathrm{End}(E) = \mathbb{Z}$, since $\mathbb{Z}$ is the only order in $\mathbb{Q}$.

Corollary 14.16. *If* E *is an elliptic curve with complex multiplication then* $\mathrm{End}(E)$ *is either an order in an imaginary quadratic field, or an order in a quaternion algebra.*

Every order lies in some *maximal order* (an order that is not contained in any other); this follows from Zorn's lemma. In general, maximal orders need not be unique, but when the $\mathbb{Q}$-algebra $\mathcal{K}$ is a number field[3] (a finite extension of $\mathbb{Q}$), this is the case. In view of Corollary 14.16, we are primarily interested in the case where $\mathcal{K}$ is an imaginary quadratic field, but it is just as easy to prove this for all number fields. We first need to recall a few standard results from algebraic number theory.[4]

Definition 14.17. An *algebraic number* α is a complex number that is the root of a polynomial with coefficients in $\mathbb{Q}$. An *algebraic integer* is a complex number that is the root of a monic polynomial with coefficients in $\mathbb{Z}$.

Two fundamental results of algebraic number theory are (1) the set of algebraic integers in a number field form a ring, and (2) every number field has an *integral basis* (a basis whose elements are algebraic integers). The following theorem gives a more precise statement.

Theorem 14.18. *The set of algebraic integers* $\mathcal{O}_K$ *in a number field* K *forms a finitely generated ring whose additive group is isomorphic to* $\mathbb{Z}^r$*, where* $r = [K : \mathbb{Q}]$ *is the dimension of* K *as a* $\mathbb{Q}$*-vector space.*

[3] Some authors define a number field as any subfield of $\mathbb{C}$, distinguishing finite extensions of $\mathbb{Q}$ as *algebraic* number fields. We adopt the more common convention that all number fields are algebraic number fields.

[4] Algebraic number theory is *not* a prerequisite for this course. We do presume some familiarity with imaginary quadratic fields; these are covered in most algebra courses.

Proof. See Theorems 2.9 and 2.16 in [3] (or see Theorem 2.1 and Corollary 2.30 in [1]), and then apply the definition of an order. □

Theorem 14.19. *The ring of integers $\mathcal{O}_K$ of a number field K is its unique maximal order.*

Proof. The previous theorem implies that $\mathcal{O}_K$ is an order. To show that it is the unique maximal order, we need to show that every order $\mathcal{O}$ in K is contained in $\mathcal{O}_K$. It suffices to show that every $\alpha \in \mathcal{O}$ is an algebraic integer. Viewing $\mathcal{O}$ as a lattice of rank $r = [K : \mathbb{Q}]$, consider the sublattice generated by all powers of α. Let $[\beta_1, \dots, \beta_r]$ be a basis for this sublattice, where each β_i is a $\mathbb{Z}$-linear combination of powers of α. Let n be an integer larger than any of the exponents in any of the powers of α that appear in any β_i. Then $\alpha^n = c_1\beta_1 + \cdots + c_r\beta_r$, for some $c_1, \dots, c_n \in \mathbb{Z}$, and this determines a monic polynomial of degree n with α as a root. Therefore α is an algebraic integer. □

Finally, we characterize the orders in imaginary quadratic fields, which are the number fields we are most interested in.

Theorem 14.20. *Let K be an imaginary quadratic field with ring of integers $\mathcal{O}_K$. The orders in K are precisely the lattices $\mathbb{Z} + f\mathcal{O}_K$, where f is any positive integer.*

Proof. We first show that $\mathcal{O} = \mathbb{Z} + f\mathcal{O}_K$ is a ring. The lattice $\mathcal{O}$ is contained in the ring $\mathcal{O}_K$ and contains 1. It suffices to show that $\mathcal{O}$ is closed under multiplication. So let $a + f\alpha$ and $b + f\beta$ be arbitrary elements of $\mathcal{O}$, with $a, b \in \mathbb{Z}$ and $\alpha, \beta \in \mathcal{O}_K$. Then

$$(a + f\alpha)(b + f\beta) = ab + af\beta + bf\alpha + abf^2\alpha\beta = ab + f(a\beta + b\alpha + abf\alpha\beta) \in \mathcal{O},$$

since $ab \in \mathbb{Z}$ and $(a\beta + b\alpha + abf\alpha\beta) \in \mathcal{O}_K$. So $\mathcal{O}$ is a subring of K. To see that $\mathcal{O}$ is an order, note that $\mathcal{O} \otimes \mathbb{Q} = \mathcal{O}_K \otimes \mathbb{Q} = K$.

Now let $\mathcal{O}$ be any order in K. The maximal order $\mathcal{O}_K$ is a rank 2 lattice containing 1, so we may write $\mathcal{O}_K$ as $[1, \tau]$ for some $\tau \notin \mathbb{Z}$ for which $\mathcal{O}_K = \mathbb{Z}[\tau]$. Let f be the least positive integer for which $f\tau \in \mathcal{O}$. The lattice $[1, f\tau]$ lies in $\mathcal{O}$, and we claim that in fact $\mathcal{O} = [1, f\tau]$. Any element α of $\mathcal{O}$ must lie in $\mathcal{O}_K$ and is therefore of the form $\alpha = a + b\tau$ for some $a, b \in \mathbb{Z}$. The element $b\tau = \alpha - a$ than lies in $\mathcal{O}$, and the minimality of f implies that f divides b. Thus $\mathcal{O} = [1, f\tau] = \mathbb{Z} + f\mathcal{O}_K$. □

The integer f in Theorem 14.20 is called the *conductor* of the order $\mathcal{O} = \mathbb{Z} + f\mathcal{O}_K$.[5] It is equal to the index of $\mathcal{O}$ in $\mathcal{O}_K$.

References

[1] J. S. Milne, *Algebraic number theory*, online course cnotes http://www.jmilne.org/math/CourseNotes/ant.html, 2013.

[2] Joseph H. Silverman, *The arithmetic of elliptic curves*, Graduate Texts in Mathematics **106**, second edition, Springer 2009.

[3] Ian Stewart and David Tall, *Algebraic number theory and Fermat's last theorem*, third edition, A.K. Peters, 2002.

[5] The conductor f should not be confused with the conductor of an elliptic curve, which we will see later.

18.783 Elliptic Curves
Spring 2013