Elliptic curves with complex multiplication

§ Elliptic curves

Let k be a field

Definition: 1) An abelian variety is a connected smooth proper group scheme over k

2) An elliptic curve is an abelian variety of dimension 1.

Theorem 1: Let E be a scheme over k. The following are equivalent:

1) E is an elliptic curve;
2) E is a connected smooth projective curve of genus 1 with a fixed k-rational point;
3) E is a smooth projective plane cubic curve given by a Weierstraß equation $y^2 + axy + by = x^3 + cx^2 + dx + e$ with $a,b,c,d,e \in k$ (in affine coordinates)
($y^2 = x^3 + Ax + B$ with $A, B \in k$ if $\operatorname{char} k \neq 2,3$)

We cannot go through the details of the proof, but it is worth making some remarks.

Remark: a) In (2), the genus of E is $g = \dim H^1(E, \mathcal{O}_E)$. Since E is smooth, this is both the arithmetic and the geometric genus.

b) A surprising feature of Theorem 1 is that point (2) and (3) do not mention the group structure at all. This rests on the following fact: if X is an abelian variety and $x \in X(k)$, there is a unique group scheme structure on the underlying scheme of X which has x as the identity element.
In point (2), this result allows one to give a unique group scheme structure to a connected smooth proper scheme of genus 1.

c) Let us see how the group structure works in (2) and (3). For simplicity, we assume that k is algebraically closed.

⇝ Let E be a connected smooth projective curve of genus one with a fixed k-rational point $P_0 \in E(k)$. We denote by $\operatorname{Pic}(E)$ the Picard group of E (line bundles of E up to isomorphism, multiplication given by tensor product of line bundles) and by $Cl(E)$ the class group of E (free abelian group generated by the set of k-points of E, modulo linear equivalence). Since E is smooth, we have

an isomorphism $Cl(E) \xrightarrow{\sim} Pic(E)$, $D \mapsto \mathcal{O}(D)$. Let $Pic^0 X$ be the subgroup of $Pic X$ corresponding to divisors of degree zero under this isomorphism. Then we have a bijection $E(k) \to Pic^0(E)$, $[P] \mapsto \mathcal{O}([P]-[P_0])$. This allows to give a group structure to $E(k)$. For k algebraically closed, this is enough to turn E into a group scheme.

ms Let E be a smooth projective cubic curve given by a Weierstraß equation. Once we have fixed coordinates so that E is defined by the equation $y^2 + axy + by = x^3 + cx^2 + dx + e$, E intersects the hyperplane at infinity in a unique point P_0, which will be the identity of the group structure. Given two points $P, Q \in E(k)$, let L be the projective line in $\mathbb{P}^2$ passing through P and Q (if $P=Q$, we take the line tangent to E at P). By Bezout's theorem, L intersects E at precisely one point, say R. We repeat the same procedure with R and P_0 to obtain another point, which we call $P+Q$. The assignement $E(k) \times E(k) \to E(k)$, $(P, Q) \mapsto P+Q$ gives a group structure to $E(k)$.

d) The group scheme structure on E is automatically abelian. This is true for all abelian varieties.

e) The implication 1) ⇒ 2) shows that an elliptic curve is always projective. This is also a feature of all abelian varieties.

Let us assume that k is algebraically closed. It is then possible to classify elliptic curves via the so-called "j-invariant".

For an effective Weil divisor D over E we define the "complete linear system" attached to D to be the set of Weil divisors over E which are linearly equivalent to D. This set is denoted by $|D|$ and it is in bijection with $\left(H^0(E, \mathcal{O}(D)) \setminus \{0\}\right) / k^\times$.

Fix a point $P_0 \in E(k)$ and consider the divisor $D = 2 \cdot [P_0]$. Since $\deg D = 2 > 0 = 2g-2$, by Riemann-Roch it follows that $|D|$ has dimension 1. Since $\deg D = 2 \geq 2 = 2g$, $|D|$ has no base point (which means that $\mathcal{O}(D)$ is generated by global sections). Putting this together, $\dim H^0(E, \mathcal{O}(D)) = 2$ and two linearly

independent global sections, say σ_1, σ_2, yield a well-defined map $f: E \to \mathbb{P}^1_k$, $x \mapsto [\sigma_1(x), \sigma_2(x)]$ of degree 2.

By Hurwitz's theorem, f is ramified at exactly four points, P_0 being one of them. Since the automorphisms of $\mathbb{P}^1$ act triply transitively on $\mathbb{P}^1$, we can assume that $f(P_0) = \infty$ and that two of the other branch points are sent to 0 and 1 via f. Let $\lambda \in \mathbb{P}^1(k)$ be the fourth branch point of f after applying this automorphism. We define the j-invariant of E by

$$j(E) := 2^8 \frac{(\lambda^2 - \lambda + 1)^3}{\lambda^2 (\lambda - 1)^2}$$

Remark: If we start with E defined as a plane cubic curve given by the equation $y^2 = x^3 + Ax + B$ (for $\operatorname{char} k \neq 2, 3$), then we may as well define $j(E) = 2^8 \cdot 3^3 \frac{A^3}{4A^3 + 27B^2}$. The fact that $4A^3 + 27B^2 \neq 0$ follows from smoothness.

Theorem 2: Let k be algebraically closed, $\operatorname{char} k \neq 2$.

1) $j(E)$ only depends on E;
2) two elliptic curves E and E' are isomorphic if and only if $j(E) = j(E')$;
3) every element of k occurs as the j-invariant of an elliptic curve.

In other words, the affine line $\mathbb{A}^1_k$ is a "moduli space for elliptic curves" via the assignement $E \mapsto j(E)$.

If $k = \mathbb{C}$, we can further describe the complex points of an elliptic curve as a 1-dimensional complex torus. Let us briefly recall how this works.

~~~ Via the exponential map.

Let G be any connected commutative algebraic group over $\mathbb{C}$ (which is automatically smooth). Its complex points can be given the structure of a complex manifold, which can be further enhanced to a complex Lie group exploiting the group scheme structure on G.

Let $\mathfrak{g}_{\mathbb{C}}$ be the tangent space of $G(\mathbb{C})$ at the identity $0 \in G(\mathbb{C})$. This has the structure of a Lie algebra, but, since G is commutative, its Lie brackets are trivial. This means that for our purposes, we can regard
~~~

$\mathfrak{g}_{\mathbb{C}}$ simply as a $\mathbb{C}$-vector space. We can then consider $\mathfrak{g}_{\mathbb{C}}$ as a complex Lie group via the natural Lie group structure on $\mathbb{C}^n$.

There exists a homomorphism of complex Lie groups $\exp_G : \mathfrak{g}_{\mathbb{C}} \longrightarrow G(\mathbb{C})$, called "exponential map". Roughly speaking, given a vector $v \in \mathfrak{g}_{\mathbb{C}}$, one can construct a unique analytic homomorphism $\varphi_v : \mathbb{C} \to G(\mathbb{C})$ such that $(d\varphi_v)_0 \left(\frac{d}{dz}\right) = v$, and then one sets $\exp_G(v) = \varphi_v(1)$.

The exponential map has the property to fit into a short exact sequence $0 \to \Lambda \to \mathfrak{g}_{\mathbb{C}} \to G(\mathbb{C}) \to 0$ of abelian groups, where Λ is discrete and $\Lambda \cong H_1^{\text{sing}}(G(\mathbb{C}), \mathbb{Z})$.

If we specialize this to the case of $G = E$ an elliptic curve, then $\dim_{\mathbb{C}} \mathfrak{g}_{\mathbb{C}} = 1$ and Λ is a free abelian group of rank 2. Thus, Λ is a lattice in $\mathbb{C}$ and $E(\mathbb{C}) \cong \mathbb{C}/\Lambda$. It can be shown that for any lattice Λ in $\mathbb{C}$, the torus $\mathbb{C}/\Lambda$ arises as the complex points of an elliptic curve.

If $G = X$ is an abelian variety, one similarly gets $X(\mathbb{C}) \cong \mathbb{C}^n/\Lambda$ where $n = \dim X$ and $\Lambda \subseteq \mathbb{C}^n$ is a lattice. However, for $n > 1$ not all lattices arise in this way.

⇝ Via elliptic functions.

Let $\Lambda \subseteq \mathbb{C}$ be a lattice, say $\Lambda = \mathbb{Z}\omega_1 \oplus \mathbb{Z}\omega_2$. An "elliptic function" with respect to Λ is a meromorphic function f on $\mathbb{C}$ such that $f(z+\omega) = f(z)$ for all $\omega \in \Lambda$. Thus, an elliptic function defines a meromorphic function $f : \mathbb{C}/\Lambda \to \mathbb{C}$.

Weierstraß $\wp$-function: $\wp(z) = \frac{1}{z^2} + \sum_{\omega \in \Lambda \setminus \{0\}} \left(\frac{1}{(z-\omega)^2} - \frac{1}{\omega^2} \right)$ (double poles at $\omega \in \Lambda$)

$\wp$ satisfies $(\wp')^2 = 4\wp^3 - g_2\wp_3 - g_3$ with $g_2 = 60 \sum_{\omega \in \Lambda \setminus \{0\}} \frac{1}{\omega^4}$ and $g_3 = 140 \sum_{\omega \in \Lambda \setminus \{0\}} \frac{1}{\omega^6}$.

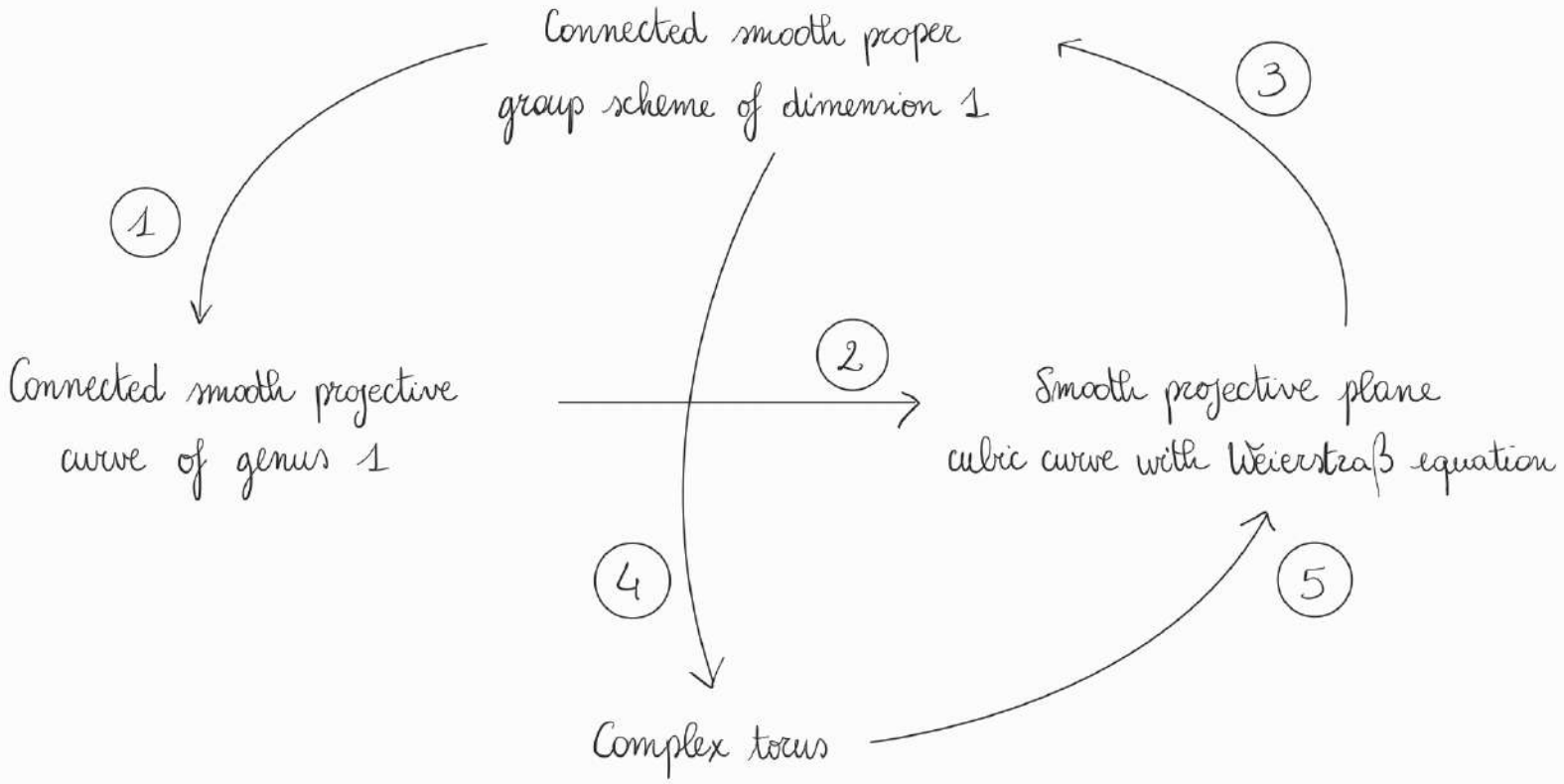
The $\mathbb{C}$-algebra of elliptic functions for Λ is $\mathbb{C}(\wp, \wp')$.

The map $\mathbb{C} \longrightarrow \mathbb{P}^2_{\mathbb{C}}$, $z \mapsto [\wp(z) : \wp'(z) : 1]$ has image lying in the (smooth) curve with equation $y^2 = 4x^3 - g_2 x - g_3$, which makes up the complex points of an elliptic curve E. This map factors through Λ, and it induces an isomorphism $\mathbb{C}/\Lambda \cong E(\mathbb{C})$, which also respects the group structure.

If we start from an arbitrary elliptic curve E, we can recover Λ by taking the periods $\omega_1 = \int_{\gamma_1} \frac{dx}{y}$, $\omega_2 = \int_{\gamma_2} \frac{dx}{y}$, where γ_1, γ_2 are two loops generating $H_1^{\text{sing}}(E(\mathbb{C}), \mathbb{Z})$.

In particular, if E is an elliptic curve over $\mathbb{C}$, the abstract group $E(\mathbb{C})$ is isomorphic to $\mathbb{R}/\mathbb{Z} \times \mathbb{R}/\mathbb{Z}$. In particular, the torsion points of $E(\mathbb{C})$ are $E[n] = \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$.

We can give an overview of the several characterizations of elliptic curves.



(1) For the genus: ones shows that $\Omega^1_{E/k} \cong \mathcal{O}_E$ (which implies that the canonical divisor is 0, so the genus is 1 by Riemann-Roch). To prove this, the group structure gives translation maps, which are automorphisms of E. An element φ of the stalk of $\Omega_{E/k}$ at a point $x \in X$ can be used to define a global section ω of Ω_E using translations and one shows that $\Omega^1_{E/k} \cong \mathcal{O}_E \cdot \omega$.
For projectivity: fix $P_0 \in E(k)$ and consider the divisor $D = 3[P_0]$. Then by Riemann-Roch $\dim H^0(E, \mathcal{O}(D)) = \deg D = 3$ and D is base-point free. This allows one to write a map $E \longrightarrow \mathbb{P}^2_k$, which then is proved to be an embedding

(2) One constructs the embedding of the previous point and then considers $D' = 6[P_0]$. Writing $H^0(E, \mathcal{O}(2[P_0])) = \mathrm{Span}_k \langle 1, x \rangle$ and $H^0(E, \mathcal{O}(3[P_0])) = \mathrm{Span}_k \langle 1, x, y \rangle$, one sees that $1, x, x^3, y, y^2, xy, x^2y \in H^0(E, \mathcal{O}(6[P_0]))$, which has dimension 6. There must be a relation among these sections, and the rest of the computations are classical

(3) One writes down the group law explicitly as we have already seen.
(4) Via the exponential map.
(5) Via elliptic functions.

Let us now have a look at the endomorphism ring of an elliptic curve. We allow k to be any field. If E is an elliptic curve over k, we define its endomorphism ring to be $\mathrm{End}(E) = \{ f : E \to E \mid f \text{ is a morphism of group schemes} \}$.
Equivalently, $\mathrm{End}(E)$ consists of the morphisms $f : E \to E$ of k-schemes such that $f(0) = 0$ (and the multiplication is automatically preserved).
For every $n \in \mathbb{Z}$, there is a multiplication-by-n map $[n] : E \to E$. In this way, we get a morphism $\mathbb{Z} \to \mathrm{End}(E)$.

Proposition 3: 1) $\mathrm{End}(E)$ has characteristic 0, it is an integral domain and has rank at most four as a $\mathbb{Z}$-module;
2) $\mathrm{End}(E)$ has an involution $\varphi \mapsto \hat{\varphi}$;
3) For all $\varphi \in \mathrm{End}(E)$, $\varphi\hat{\varphi} \in \mathbb{Z}$ and $\varphi\hat{\varphi} = 0$ if and only if $\varphi = 0$.

Proposition 4: Any ring R with properties (1), (2) and (3) above satisfies one and only one of the following:
1) $R = \mathbb{Z}$;
2) R is an order in an imaginary quadratic field
3) R is an order in a quaternion algebra over $\mathbb{Q}$.

In order to better understand Proposition 4, let us recall a few definitions.

Definition: Let A be a (not necessarily commutative) $\mathbb{Q}$-algebra which is finitely generated over $\mathbb{Q}$. A subring R of A is an "order" if R is finitely generated as a $\mathbb{Z}$-module and $R \otimes_{\mathbb{Z}} \mathbb{Q} = A$.

Definition: A quaternion algebra over $\mathbb{Q}$ is a $\mathbb{Q}$-algebra A of dimension 4 as a $\mathbb{Q}$-vector space having a $\mathbb{Q}$-basis of the form $\{1, \alpha, \beta, \alpha\beta\}$ for $\alpha, \beta \in A$ such that $\alpha^2, \beta^2 \in \mathbb{Q}$, $\alpha^2 < 0$, $\beta^2 < 0$ and $\alpha\beta = -\beta\alpha$.

Let us now go through some consequences of Proposition 4. We divide the study of $\mathrm{End}(E)$ according to the characteristic of k. Let $\bar{k}$ be a fixed algebraic closure of k.

↝ If $\mathrm{char}\, k = 0$, it is not difficult to prove that $\mathrm{End}(E)$ is a commutative ring. To give an idea of how this goes, let $\omega \in \Omega^1_{E\otimes_k \bar{k}/\bar{k}}$ be a non-zero invariant differential form. Since $\Omega^1_{E\otimes_k \bar{k}/\bar{k}} = \bar{k}(E\otimes_k \bar{k})\cdot\omega$ for every $\varphi \in \mathrm{End}(E)$ there is $a_\varphi \in \bar{k}(E\otimes_k \bar{k})$ such that $\varphi^*\omega = a_\varphi \cdot \omega$. But $\mathrm{div}(a_\varphi) = \mathrm{div}(\varphi^*\omega) - \mathrm{div}(\omega) = 0$, since $\mathrm{div}(\omega) = 0$. It follows that $a_\varphi \in \bar{k}$. The assignement $\varphi \mapsto a_\varphi$ can then be checked to induce an embedding $\mathrm{End}(E) \hookrightarrow \bar{k}$.

Together with Proposition 4, this fact implies that $\mathrm{End}(E)$ cannot be an order in a quaternion algebra over $\mathbb{Q}$, but it can only be $\mathbb{Z}$ or an order in an imaginary quadratic field.

If $\mathrm{End}(E) \neq \mathbb{Z}$, we say that E has "complex multiplication"

↝ If $\mathrm{char}\, k = p > 0$, the isomorphism type of $\mathrm{End}(E)$ is strictly connected to the p-torsion points of E. If $m \in \mathbb{Z}$ and $p \nmid m$, then $E[m] \cong \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$. Otherwise, $E[p^n]$ can be either 0 or $\mathbb{Z}/p^n\mathbb{Z}$. For $\mathrm{End}(E)$ we have the following possibilities:

- $\mathrm{End}(E)$ is an order in a quaternion algebra over $\mathbb{Q}$ if and only if $E[p^n] = 0$ for some (equivalently, for all) $n \geq 1$. In this case, $j(E) \in \mathbb{F}_{p^2}$.
- $\mathrm{End}(E)$ is a quadratic imaginary field if and only if $E[p^n] \cong \mathbb{Z}/p^n\mathbb{Z}$ for all $n \geq 1$ and $j(E)$ is algebraic over $\mathbb{F}_p$.
- $\mathrm{End}(E) = \mathbb{Z}$ if and only if $E[p^n] \cong \mathbb{Z}/p^n\mathbb{Z}$ for all $n \geq 1$ and $j(E)$ is transcendental over $\mathbb{F}_p$.

§ Complex multiplication

Let E be an elliptic curve over $\mathbb{C}$. As we have seen, there is a lattice $\Lambda = \mathbb{Z}\omega_1 \oplus \mathbb{Z}\omega_2 \subseteq \mathbb{C}$ such that $E(\mathbb{C}) \cong \mathbb{C}/\Lambda$ as Lie groups.

Remark: Suppose we are given two lattices $\Lambda_1, \Lambda_2 \subseteq \mathbb{C}$. Of course there is an $\mathbb{R}$-linear map $\varphi: \mathbb{C} \to \mathbb{C}$ such that $\varphi(\Lambda_1) = \Lambda_2$. This gives a bijection $\varphi: \mathbb{C}/\Lambda_1 \to \mathbb{C}/\Lambda_2$. Notice that this bijection is a diffeomorphism of 2-dimensional real manifolds, but it is not a holomorphic map. Thus, φ is not an isomorphism of Lie groups.

It can be checked that every $\varphi \in \mathrm{End}(E)$ acts on $\mathbb{C}/\Lambda$ (under the isomorphism $E(\mathbb{C}) \cong \mathbb{C}/\Lambda$) as multiplication by some complex number $\alpha_\varphi \in \mathbb{C}$ satisfying $\alpha_\varphi \cdot \Lambda \subseteq \Lambda$. Conversely, every such number gives an endomorphism of E.
Hence, we have a bijection $\mathrm{End}(E) \cong \{\alpha \in \mathbb{C} \mid \alpha \cdot \Lambda \subseteq \Lambda\}$.
This gives an embedding $\mathrm{End}(E) \hookrightarrow \mathbb{C}$, i.e. we can $\mathrm{End}(E)$ is a discrete subring of $\mathbb{C}$. Any discrete subring of $\mathbb{C}$ is either $\mathbb{Z}$ or an order in a quadratic imaginary extension of $\mathbb{Q}$.
We have already seen this characterization, but this is a faster way to reach it when E is defined over $\mathbb{C}$ using the isomorphism $E(\mathbb{C}) \cong \mathbb{C}/\Lambda$.

Assume now that E has complex multiplication, i.e. $\mathrm{End}(E) \cong \mathcal{O}$ where $\mathcal{O}$ is an order in a quadratic imaginary field K.
Recall that the ring of integers $\mathcal{O}_K$ of K is of the form $\mathcal{O}_K = \mathbb{Z} \oplus \mathbb{Z}\alpha$ where $\alpha = \frac{1+\sqrt{D}}{2}$ or $\alpha = \frac{\sqrt{D}}{2}$ where D is the discriminant of K. Thus, there is $f \in \mathbb{Z}$ such that $\mathcal{O} = \mathbb{Z} \oplus \mathbb{Z} f\alpha$, and f is called "conductor" of $\mathcal{O}$. For convenience, we fix an embedding of K into $\mathbb{C}$.

Lemma 5: $\mathcal{O}$ is a Noetherian ring of dimension 1. However, $\mathcal{O}$ is not normal, as its integral closure in $K = \mathrm{Frac}(\mathcal{O})$ is $\mathcal{O}_K$.

We focus on the study of fractional ideals of $\mathcal{O}$ (see Cox, "Primes of the form $x^2 + ny^2$")

Lemma 6: Let Λ be an $\mathcal{O}$-module. The following are equivalent:

1) Λ is projective;

2) Λ is isomorphic to a fractional ideal of $\mathcal{O}$ (i.e., an invertible $\mathcal{O}$-submodule of K)

Moreover, if (1) or (2) holds, then Λ has rank 1 if and only if it is isomorphic to a proper fractional ideal of $\mathcal{O}$ (i.e. $\{z \in \Lambda \mid z\Lambda \subseteq \Lambda\} = \mathcal{O}$).

Definition: The Picard group of $\mathcal{O}$ is

$$\mathrm{Pic}(\mathcal{O}) = \{\text{Projective } \mathcal{O}\text{-modules of rank } 1\}/\text{iso}.$$

This is a group with product given by tensor product of modules.
We have $\mathrm{Pic}(\mathcal{O}) \cong \{\text{proper fractional ideals of } \mathcal{O}\}/\{\text{principal ideals of } \mathcal{O}\}$
For $\mathcal{O} = \mathcal{O}_K$, $\mathrm{Pic}(\mathcal{O}_K)$ recovers the notion of class group of K.

Definition: Let $\mathfrak{a}$ be an ideal of $\mathcal{O}$. We define its norm to be $N(\mathfrak{a}) = |\mathcal{O} : \mathfrak{a}|$ (the index of $\mathfrak{a}$ as an additive subgroup of $\mathcal{O}$).

It can be seen that the norm is always finite and multiplicative.

Lemma 7: Let $\mathfrak{a}$ be an ideal of $\mathcal{O}$. The following are equivalent:

1) $\mathfrak{a} + f\mathcal{O} = \mathcal{O}$;

2) $N(\mathfrak{a})$ is coprime to the conductor f of $\mathcal{O}$.

If an ideal $\mathfrak{a}$ of $\mathcal{O}$ satisfies one of the two equivalent conditions in the last lemma, we say that $\mathfrak{a}$ is "prime to f". It is not difficult to check that ideals prime to f are proper, so they determine an element of $\mathrm{Pic}(\mathcal{O})$.

Lemma 8: Let $I(\mathcal{O}) = \{\text{proper fractional ideals of } \mathcal{O}\}$, $P(\mathcal{O}) = \{\text{proper principal ideals of } \mathcal{O}\}$. Let $I_f(\mathcal{O})$ be the subgroup of $I(\mathcal{O})$ generated by ideals of $\mathcal{O}$ prime to f and $P_f(\mathcal{O}) = I_f(\mathcal{O}) \cap P(\mathcal{O})$.

Then the natural inclusion $I_f(\mathcal{O}) \hookrightarrow I(\mathcal{O})$ induces an isomorphism $\mathrm{Pic}(\mathcal{O}) = I(\mathcal{O})/P(\mathcal{O}) \cong I_f(\mathcal{O})/P_f(\mathcal{O})$.

Thus, $\mathrm{Pic}(\mathcal{O})$ is generated by the classes of ideals of $\mathcal{O}$ prime to f. These ideals can be related to ideals of the maximal order $\mathcal{O}_K$ with the same property.

Lemma 9: There is an isomorphism $I_f(\mathcal{O}_K) \xrightarrow{\sim} I_f(\mathcal{O})$, $\mathfrak{b} \mapsto \mathfrak{b} \cap \mathcal{O}$ with inverse given by $\mathfrak{a}\mathcal{O}_K \longleftarrow \mathfrak{a}$.

Let now $P_f(\mathcal{O}_K)$ be the subgroup of $P(\mathcal{O}_K)$ generated by principal ideals of the form $z\mathcal{O}_K$ where $z \equiv a \pmod{f\mathcal{O}_K}$ for some $a \in \mathbb{Z}$ with $\gcd(a, f) = 1$.

Corollary 10: $\mathrm{Pic}(\mathcal{O}) \cong I_f(\mathcal{O}_K) / P_f(\mathcal{O}_K)$.

By working out some more details, it is possible to deduce from the finiteness of $\mathrm{Pic}(\mathcal{O}_K)$ that $\mathrm{Pic}(\mathcal{O})$ is finite as well. Moreover, Corollary 10 implies that ideals of $\mathcal{O}$ prime to f factor uniquely as products of prime ideals of $\mathcal{O}$ prime to f.

Let Λ_E be the period lattice of E, which defines an isomorphism $E(\mathbb{C}) \cong \mathbb{C}/\Lambda_E$. Λ_E is a projective $\mathcal{O} = \mathrm{End}(E)$-module of rank 1, whose isomorphism class only depends on the isomorphism class of E. Indeed, if we write $\Lambda_E = \mathbb{Z}\omega_1 \oplus \mathbb{Z}\omega_2$ for $\omega_1, \omega_2 \in \mathbb{C}$, then $\Lambda_E \cong \Lambda$ where $\Lambda = \mathbb{Z} \oplus \mathbb{Z}\frac{\omega_2}{\omega_1}$. Since $\mathcal{O}\Lambda \subseteq \Lambda$, $\alpha \cdot 1 = n_1 + n_2\frac{\omega_2}{\omega_1}$ for $n_1, n_2 \in \mathbb{Z}$, which shows that $\frac{\omega_2}{\omega_1} \in K$. It follows that Λ is a proper fractional ideal of $\mathcal{O}$.

Conversely, given a projective $\mathcal{O}$-module $\Lambda \subseteq \mathbb{C}$ of rank 1, the torus $\mathbb{C}/\Lambda$ has complex multiplication in $\mathcal{O}$.

This proves the following:

Proposition 11: The assignement $E \mapsto \Lambda_E$ yields a bijection

$$\left\{ \begin{array}{l} \text{Elliptic curves with} \\ \text{CM by } \mathcal{O} \end{array} \right\} / \text{iso} \xrightarrow{\sim} \left\{ \begin{array}{l} \text{Projective } \mathcal{O}\text{-modules} \\ \text{of rank 1} \end{array} \right\} / \text{iso} = \mathrm{Pic}(\mathcal{O})$$

Since $\mathrm{Pic}(\mathcal{O})$ is finite, it follows that there are only finitely many complex elliptic curves with complex multiplication by $\mathcal{O}$.

Corollary 12: If E is a complex elliptic curve with complex multiplication by $\mathcal{O}$, its j-invariant $j(E)$ is an algebraic number.

Proof: Using the classical definition via a Weierstraß equation, E is isomorphic to the curve with equation $y^2 + xy = x^3 + \frac{36}{j(E)-1728}x - \frac{1}{j(E)-1728}$ in affine coordinates. Suppose that $j(E)$ is transcendental. Then we have infinitely many morphisms $\varphi: \mathbb{Q}(j(E)) \hookrightarrow \mathbb{C}$. The curve E_φ given by the equation $y^2+xy = x^3 + \frac{1}{\varphi(j(E))-1728}x - \frac{1}{\varphi(j(E))-1728}$ still has complex multiplication by $\mathcal{O}$, but if $\varphi(j(E)) \neq j(E)$ then E_φ is not isomorphic to E. This contradicts the finiteness of $\mathrm{Pic}(\mathcal{O})$. □

Let $\mathrm{Ell}(\mathcal{O})$ denote the set of elliptic curves with complex multiplication by $\mathcal{O}$. We have just seen that $\mathrm{Ell}(\mathcal{O})$ is in bijection with $\mathrm{Pic}(\mathcal{O})$.

There is a natural simply transitive action of $\mathrm{Pic}(\mathcal{O})$ on $\mathrm{Ell}(\mathcal{O})$, which we now describe.

Let $E \in \mathrm{Ell}(\mathcal{O})$ and $\Lambda \in \mathrm{Pic}\mathcal{O}$. Consider a free resolution $\mathcal{O}^m \xrightarrow{Z} \mathcal{O}^n \longrightarrow \Lambda \longrightarrow 0$.

If $\Lambda = \mathcal{O}$, we define $\mathrm{Hom}(\Lambda, E)$ to be E. Otherwise, Z yields an $m \times n$ matrix with coefficients in $\mathcal{O} = \mathrm{End}(E)$. Its transpose therefore defines a map ${}^tZ: E^n \to E^m$. More precisely, by applying $\mathrm{Hom}_{\mathcal{O}}(-, E(\mathbb{C}))$ we obtain a map ${}^tZ: E(\mathbb{C})^n \to E(\mathbb{C})^m$ which can be upgraded to a map ${}^tZ: E^n \to E^m$ of group schemes since ${}^tZ$ has entries in $\mathcal{O} \cong \mathrm{End}(E)$. We then define $\mathrm{Hom}(\Lambda, E)$ to be the identity component of the kernel of ${}^tZ$. It can be checked that $\mathrm{Hom}(\Lambda, E)$ is a complex elliptic curve with complex multiplication by $\mathcal{O}$, so $\mathrm{Hom}(\Lambda, E) \in \mathrm{Ell}(\mathcal{O})$

The map $\mathrm{Pic}(\mathcal{O}) \times \mathrm{Ell}(\mathcal{O}) \to \mathrm{Ell}(\mathcal{O})$, $(\Lambda, E) \mapsto \mathrm{Hom}(\Lambda, E)$ defines a simply transitive action of $\mathrm{Pic}(\mathcal{O})$ on $\mathrm{Ell}(\mathcal{O})$.

We can give a more explicit description of this action

Claim: Under the identification $\mathrm{Ell}(\mathcal{O}) \cong \mathrm{Pic}(\mathcal{O})$, the action of $\mathrm{Pic}(\mathcal{O})$ on $\mathrm{Ell}(\mathcal{O})$ coincides with the inverse left multiplication on $\mathrm{Pic}(\mathcal{O})$ (i.e. $\mathrm{Ell}(\mathcal{O}) \to \mathrm{Pic}(\mathcal{O})$ maps $\mathrm{Hom}(\Lambda, E)$ to $\Lambda^{-1}\Lambda_E$).

In order to show that these two actions coincide, it is enough to check this for the classes of prime ideals $\mathfrak{p}$ of $\mathcal{O}$ coprime to f, as these generate $\mathrm{Pic}(\mathcal{O})$.

We have an exact sequence of $\mathcal{O}$-modules $0 \to \Lambda_E \to \mathbb{C} \to E(\mathbb{C}) \to 0$.

By applying $\mathrm{Hom}_{\mathcal{O}\text{-mod}}(-,-)$ to the sequences $\mathcal{O}^m \xrightarrow{\phi} \mathcal{O}^n \to \mathfrak{p} \to 0$ and $0 \to \Lambda_E \to \mathbb{C} \to E(\mathbb{C}) \to 0$ we obtain a diagram

$$\begin{array}{ccccc}
 & & 0 & 0 & 0 \\
 & & \downarrow & \downarrow & \downarrow \\
0 & \to & \mathrm{Hom}(\mathfrak{p}, \Lambda_E) & \to \mathrm{Hom}(\mathfrak{p}, \mathbb{C}) & \to \mathrm{Hom}(\mathfrak{p}, E(\mathbb{C})) \\
 & & \downarrow & \downarrow & \downarrow \\
0 & \to & \mathrm{Hom}(\mathcal{O}^m, \Lambda_E) & \to \mathrm{Hom}(\mathcal{O}^m, \mathbb{C}) & \to \mathrm{Hom}(\mathcal{O}^m, E(\mathbb{C})) \\
 & & \downarrow & \downarrow & \downarrow \\
0 & \to & \mathrm{Hom}(\mathcal{O}^m, \Lambda_E) & \to \mathrm{Hom}(\mathcal{O}^m, \mathbb{C}) & \to \mathrm{Hom}(\mathcal{O}^m, E(\mathbb{C}))
\end{array}$$

Now observe that:

- $\mathrm{Hom}(\mathcal{O}^r, M) \cong M^r$ for every $\mathcal{O}$-module M and $r \geq 1$.
- for every torsion-free $\mathcal{O}$-module M, the map $\mathfrak{p}^{-1}M \to \mathrm{Hom}(\mathfrak{p}, M)$, $m \mapsto (x \mapsto x \cdot m)$ is an isomorphism. This is a standard check with commutative algebra.

The above diagram becomes:

$$\begin{array}{ccccccc}
 & & 0 & 0 & 0 & & \\
 & & \downarrow & \downarrow & \downarrow & & \\
0 & \to & \mathfrak{p}^{-1}\Lambda_E & \to \mathbb{C} & \to \mathrm{Hom}(\mathfrak{p}, E(\mathbb{C})) & & \\
 & & \downarrow & \downarrow & \downarrow & & \\
0 & \to & \Lambda_E^m & \to \mathbb{C}^m & \to E(\mathbb{C})^n & \to & 0 \\
 & & \downarrow {}^t\phi & \downarrow {}^t\phi & \downarrow {}^t\phi & & \\
0 & \to & \Lambda_E^m & \to \mathbb{C}^m & \to E(\mathbb{C})^m & \to & 0
\end{array}$$

By applying the snake lemma to the bottom rows, we obtain an exact sequence

$$0 \to \mathfrak{p}^{-1}\Lambda_E \to \mathbb{C} \to \mathrm{Hom}(\mathfrak{p}, E(\mathbb{C})) \to \Lambda_E^n / {}^t\phi(\Lambda_E^m),$$

which hence gives an exact sequence $0 \to \mathbb{C}/\mathfrak{p}^{-1}\Lambda_E \to \mathrm{Hom}(\mathfrak{p}, E(\mathbb{C})) \to \Lambda_E^n / {}^t\phi(\Lambda_E^m)$.

Now, $\mathrm{Hom}(\mathfrak{p}, E(\mathbb{C})) = \ker({}^t\mathcal{Z} : E(\mathbb{C})^n \to E(\mathbb{C})^m)$. Since ${}^t\mathcal{Z} \in M_{m\times n}(\mathcal{O})$ has entries in $\mathcal{O} \cong \mathrm{End}(E)$, we can realize ${}^t\mathcal{Z}$ as a map of group schemes ${}^t\mathcal{Z} : E^n \to E^m$. Hence, $\mathrm{Hom}(\mathfrak{p}, E(\mathbb{C}))$ can be thought of as the complex points of the group scheme $\ker({}^t\mathcal{Z} : E^n \to E^m)$. Let $\mathrm{Hom}(\mathfrak{p}, E)$ denote the identity component of this group scheme (which is the definition of the action of $\mathfrak{p}$ on E).
Using the fact that $\mathbb{C}/\mathfrak{p}^{-1}\Lambda_E$ is connected, while $\Lambda_E^n / {}^t\mathcal{Z}(\Lambda_E^m)$ is discrete, one sees that $\mathbb{C}/\mathfrak{p}^{-1}\Lambda_E = \mathrm{Hom}(\mathfrak{p}, E)(\mathbb{C})$ (i.e., the complex points of the identity component of $\mathrm{Hom}(\mathfrak{p}, E)$). This implies that the two actions agree.

If E is any elliptic curve over $\mathbb{C}$ and $\sigma : \mathbb{C} \to \mathbb{C}$ is any field automorphism, we define the elliptic curve E^σ to be $E \to \mathrm{Spec}\,\mathbb{C} \xrightarrow{\sigma} \mathrm{Spec}\,\mathbb{C}$. It is clear that $\mathrm{End}(E^\sigma) \cong \mathrm{End}(E)$. If $E \in \mathrm{Ell}(\mathcal{O})$, then we obtain an action of $\mathrm{Gal}(\bar{K}/K)$ on $\mathrm{Ell}(\mathcal{O})$.

Lemma 13: The actions of $\mathrm{Gal}(\bar{K}/K)$ and $\mathrm{Pic}(\mathcal{O})$ on $\mathrm{Ell}(\mathcal{O})$ commute.

Proof: For $\Lambda \in \mathrm{Pic}(\mathcal{O})$ and $\sigma \in \mathrm{Gal}(\bar{K}/K)$
$\mathrm{Hom}(\Lambda, E)^\sigma = (\ker(\mathcal{Z}^t : E^n \to E^m)^\circ)^\sigma = \ker({}^t\mathcal{Z}^\sigma : (E^\sigma)^n \to (E^\sigma)^m)^\circ = \mathrm{Hom}(\Lambda^\sigma, E^\sigma)$.
Since $\sigma \in \mathrm{Gal}(\bar{K}/K)$, $\Lambda^\sigma = \Lambda$, hence $\mathrm{Hom}(\Lambda, E)^\sigma = \mathrm{Hom}(\Lambda, E^\sigma)$. □

Remark: Since any field automorphism of $\bar{K}$ acts on $\mathrm{Ell}(\mathcal{O})$, we actually obtain an action of $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ on $\mathrm{Ell}(\mathcal{O})$. However, this action does not commute with the one of $\mathrm{Pic}(\mathcal{O})$, since we need that $\Lambda^\sigma = \Lambda$.

The reason why we care about commutativity is the following.
If we fix $E \in \mathrm{Ell}(\mathcal{O})$, then for every $\sigma \in \mathrm{Gal}(\bar{K}/K)$ there is some $\eta_E(\sigma) \in \mathrm{Pic}(\mathcal{O})$ such that $E^\sigma = \mathrm{Hom}(\eta_E(\sigma), E)$.

Lemma 14: $\eta_E(\sigma)$ does not depend on E.

Proof: Let $F \in \mathrm{Ell}(\mathcal{O})$ and take $\tau \in \mathrm{Gal}(\bar{K}/K)$ so that $F = E^\tau$. Then

$$F^\sigma = (E^\tau)^\sigma = (\eta_E(\tau)\cdot E)^\sigma \overset{\text{commutativity of the two actions}}{=} \eta_E(\tau)\cdot E^\sigma = \eta_E(\tau)\,\eta_E(\sigma)\cdot E \overset{\mathrm{Pic}(\mathcal{O}) \text{ is abelian}}{=} \eta_E(\sigma)\,\eta_E(\tau)\cdot E = \eta_E(\sigma)\cdot E^\tau = \eta_E(\sigma)\cdot F$$

□

It follows that we have a group homomorphism
$\eta: \mathrm{Gal}(\bar{K}/K) \longrightarrow \mathrm{Pic}(\mathcal{O})$ such that $E^\sigma = \mathrm{Hom}(\eta(\sigma), E)$ for all $E \in \mathrm{Ell}(\mathcal{O})$.
Since η is surjective, we have realized $\mathrm{Pic}(\mathcal{O})$ as a finite quotient of $\mathrm{Gal}(\bar{K}/K)$, hence there is a finite extension H of K such that $\mathrm{Gal}(H/K) \cong \mathrm{Pic}(\mathcal{O})$.
This extension is a finite abelian extension of K, and the j-invariants $j(E)$ of any $E \in \mathrm{Ell}(\mathcal{O})$ lie in H.

Next, we want to apply some results of class field theory in order to better describe H.
Recall: The ring of finite adèles of K is $\mathbb{A}_{K,f} = \prod'_{\mathfrak{p} \text{ finite place}} K_\mathfrak{p}$, where $K_\mathfrak{p}$ is the completion of K with respect to the $\mathfrak{p}$-adic valuation and $\prod'$ denotes the restricted product with respect to $\{\mathcal{O}_{K_\mathfrak{p}}\}_\mathfrak{p}$ (i.e. $(x_\mathfrak{p})_\mathfrak{p} \in \mathbb{A}_{K,f}$ if and only if $x_\mathfrak{p} \in \mathcal{O}_{K_\mathfrak{p}}$ for all but finitely many primes $\mathfrak{p}$ of $\mathcal{O}$). $\mathbb{A}_{K,f}$ can be turned into a topological ring with the restricted product topology.
Finite idèles of K: $\mathbb{I}_{K,f} = \mathbb{A}_{K,f}^\times$ with the restricted product topology.
We have diagonal embeddings $K \hookrightarrow \mathbb{A}_{K,f}$, $K^\times \hookrightarrow \mathbb{I}_{K,f}$.
Given an order $\mathcal{O}$ in K, we denote by $\hat{\mathcal{O}}$ its closure in $\mathbb{A}_{K,f}$.
Lemma 15: The map $\mathbb{I}_{K,f} / K^\times \hat{\mathcal{O}}^\times \longrightarrow \mathrm{Pic}(\mathcal{O})$ is an isomorphism.
$\alpha \longmapsto (\alpha^{-1}\hat{\mathcal{O}}) \cap K \ (\subseteq \mathbb{C})$

An application of the fundamental theorem of class field theory yields:
Theorem 16: There exists an abelian extension H_f of K with the following properties:
1) H_f is unramified outside of the primes of K above f;
2) Let $\mathfrak{p}$ be a prime of K coprime to f, $\pi_\mathfrak{p} \in K_\mathfrak{p}$ a uniformizer and $\sigma_\mathfrak{p}$ the Frobenius element of $\mathrm{Gal}(H_f/K)$ at $\mathfrak{p}$. Then the map
$\mathrm{rec}: \mathrm{Pic}(\mathcal{O}) \cong \mathbb{I}_{K,f}/K^\times\hat{\mathcal{O}}^\times \longrightarrow \mathrm{Gal}(H_f/K)$, $[\mathfrak{p}] := (\ldots, 1, \pi_\mathfrak{p}, 1, \ldots) \mapsto \sigma_\mathfrak{p}^{-1}$
is an isomorphism.
The field H_f in Theorem 16 is called the "ring class field of K of conductor f".
The morphism $\mathrm{rec}: \mathrm{Pic}(\mathcal{O}) \xrightarrow{\sim} \mathrm{Gal}(H_f/K)$ is the "Artin reciprocity map".

Proposition 17: The abelian extension H equals $H_{\mathfrak{f}}$.

In particular, for all primes $\mathfrak{p}$ of K coprime to $\mathfrak{f}$ we have $\eta(\sigma_{\mathfrak{p}}) = [\mathfrak{p}] \in \mathrm{Pic}(\mathcal{O})$

Proof: Let $E \in \mathrm{Ell}(\mathcal{O})$. Let Σ be the set of primes $\mathfrak{p}$ of $\mathcal{O}_K$ which satisfy the following conditions:

1) $\mathfrak{p}$ is unramified in H/K;
2) E has good reduction at all the primes of H above $\mathfrak{p}$;
3) the prime $\mathfrak{p}$ does not divide $N_K^H(j(E_1) - j(E_2))$ for all $E_1, E_2 \in \mathrm{Ell}(\mathcal{O})$, $E_1 \neq E_2$;
4) the norm of $\mathfrak{p}$ is a rational prime $p \in \mathbb{Z}$, i.e. p is not inert in $K/\mathbb{Q}$.

The set of these primes has density one, hence the Chebotarev density theorem implies that the Frobenii $\sigma_{\mathfrak{p}}$ of the primes $\mathfrak{p} \in \Sigma$ generate $\mathrm{Gal}(H/K)$.

Let $\mathfrak{p} \in \Sigma$ and $\mathfrak{p}'$ be a prime of H lying above $\mathfrak{p}$. Let $\overline{E}$ be the reduction of E at $\mathfrak{p}'$, which, by property (2), is an elliptic curve defined over a finite field F of characteristic p.

It is then possible to prove that:

a) $\overline{E}$ is ordinary (which means that $\overline{E}[p^r] = \mathbb{Z}/p^r\mathbb{Z}$ for all $r \geq 1$ or, equivalently, $\mathrm{End}(\overline{E})$ is an order in a quadratic imaginary field).
In particular, the Frobenius morphism $\mathrm{Frob}: \overline{E} \to \overline{E}^{(p)}$ is the unique inseparable isogeny of degree p from $\overline{E}$.
(Here, if $\varphi \in \mathrm{Gal}(F/\mathbb{F}_p)$ is the Frobenius, $\overline{E}^{(p)}$ is the curve $\overline{E} \to \mathrm{Spec}\, F \xrightarrow{\varphi} \mathrm{Spec}\, F$, and $\mathrm{Frob}: \overline{E} \to \overline{E}^{(p)}$ is the absolute Frobenius. This means that we consider the map $\overline{E} \to \overline{E}$ which is the identity on the topological spaces and $\mathcal{O}_{\overline{E}}(U) \to \mathcal{O}_{\overline{E}}(U)$, $x \mapsto x^p$. This map is a morphism of $\mathbb{F}_p$-schemes, not of F-schemes. It induces a map of F schemes $\mathrm{Frob}: \overline{E} \to \overline{E}^{(p)}$).

b) the elliptic curve $E/E[\mathfrak{p}] = \mathrm{Hom}([\mathfrak{p}], E)$ is defined over $\mathbb{Q}(j(E)) \subseteq H$ and the natural projection $E \to E/E[\mathfrak{p}]$ (i.e. $\mathrm{Hom}(\mathcal{O}, E) \to \mathrm{Hom}([\mathfrak{p}], E)$) becomes a purely inseparable morphism when reduced modulo $\mathfrak{p}'$.

By combining (a) and (b), it follows that $E \to \mathrm{Hom}([\mathfrak{p}], E)$, when reduced modulo $\mathfrak{p}'$, coincides with $\mathrm{Frob}: \overline{E} \to \overline{E}^{(p)}$. This means that $\overline{\mathrm{Hom}(\mathfrak{p}, E)} = \overline{E}^{(p)}$. Notice that $\overline{E}^{(p)}$ coincides with $\overline{(E^{\sigma_{\mathfrak{p}}})}$.

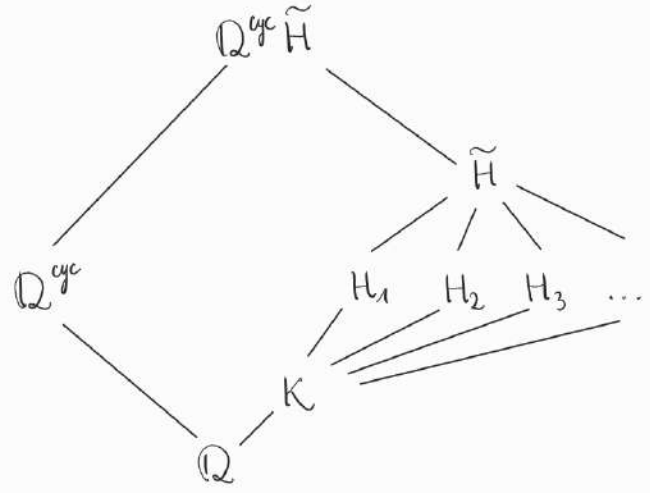
By the property (3), $j(E_1) \not\equiv j(E_2) \pmod{\mathfrak{p}}$ for all distinct $E_1, E_2 \in \mathrm{Ell}(\mathcal{O})$.

This means that the elliptic curves with complex multiplication by $\mathcal{O}$ remain distinct when reduced modulo $\mathfrak{p}'$. Two of these curves, namely $E^{\sigma_{\mathfrak{p}}}$ and $\mathrm{Hom}([\mathfrak{p}], E)$, become equal when reduced modulo $\mathfrak{p}'$, hence $E^{\sigma_{\mathfrak{p}}} = \mathrm{Hom}([\mathfrak{p}], E)$ already. As a result, $\eta(\sigma_{\mathfrak{p}}) = [\mathfrak{p}]$.
This holds for a set of primes whose Frobenii generate the whole $\mathrm{Gal}(H/K)$ by the Chebotarev density theorem, so we may conclude that $H = H_{\mathfrak{f}}$ □

Let us summarize what we have seen so far.
Given a quadratic imaginary field K, one can construct the Hilbert class field H_1 of K (the maximal abelian unramified extension of K). The previous result tells us that $H_1 = K(j(E))$ where E is any elliptic curve with complex multiplication by $\mathcal{O}_K$. Next, we can allow some ramification by considering the Hilbert class field $H_{\mathfrak{f}}$ of conductor $\mathfrak{f}$, which we have seen that it is generated by the j-invariant of an elliptic curve with complex multiplication by $\mathcal{O}$ with $[\mathcal{O}_K : \mathcal{O}] = \mathfrak{f}$.
These are all abelian extensions of K, so their compositum $\tilde{H}$ is an abelian extension of K as well. Let $\mathbb{Q}^{cyc}$ be the cyclotomic extension of $\mathbb{Q}$.
Question: is it true that $\tilde{H} \cdot \mathbb{Q}^{cyc}$ is the maximal abelian extension of K?

Theorem 18: $\mathrm{Gal}(K^{ab} / \tilde{H}\mathbb{Q}^{cyc})$ is a product of groups of order 2.
This follows from class field theory. Thus, adjoining roots of unity and all the j-invariants above is not enough to construct K^{ab}.

The picture at the moment is the following:



Now, let E be an elliptic curve with complex multiplication by $\mathcal{O}_K$. We have seen that $j(E) \in H_1$, so we may assume that E is defined over H_1. Let L_E be the extension of H_1 generated by the coordinates of the torsion points of E.

- $\mathrm{Gal}(L_E / H_1) \hookrightarrow U(K) = \prod_{\mathfrak{p} \text{ finite}} \mathcal{O}_{K_\mathfrak{p}}^\times$.
- By class field theory, L_E corresponds to a group homomorphism $\vartheta_E : I_{H_1,\mathfrak{f}} \longrightarrow U(K)$
- Let U be the group of integral units of K (i.e. $U = \mathcal{O}_K^\times$, which corresponds to $\mathrm{Aut}(E)$ under $\mathrm{End}(E) \cong \mathcal{O}_K$). Notice that $U = \{\pm 1\}$ if $K \neq \mathbb{Q}(i), \mathbb{Q}(\sqrt{-3})$, otherwise $U = \{\pm 1, \pm i\}$ and $U = \{6^{\text{th}} \text{ roots of unity}\}$.
- $U(H_1) \hookrightarrow I_{H_1,\mathfrak{f}}$, and the restriction of ϑ_E to $U(H_1)$ takes the form $\vartheta_E(x) = N_K^{H_1}(x^{-1})\, \rho_E(x)$ for $x \in U(H_1)$, where $\rho_E : U(H_1) \to U$.
- L_E and ρ_E depend on E; to get rid of this, let $X = E/U \cong \mathbb{P}^1$ and let L be the extension of H_1 generated by the coordinates of the images in X of the torsion points of E under $E \to E/U \cong \mathbb{P}^1$. Then L does not depend on E in $\mathrm{Ell}(\mathcal{O}_K)$

Theorem 19: L is the maximal abelian extension of K.

Remark: Explicitly in coordinates, if $K \neq \mathbb{Q}(i), \mathbb{Q}(\sqrt{-3})$, then $U = \{\pm 1\}$ and the map $h : E(\mathbb{C}) \to E/U(\mathbb{C})$ is given by $(x,y) \mapsto x$.

Suppose K has class number 1. Then:

- $H_1 = K$, and $j(E) \in \mathbb{Q}$.
- $\#\mathrm{Ell}(\mathcal{O}_K) = 1$, hence $L_E = L$.
- $K(h(E_{\mathrm{tors}})) = K(E_{\mathrm{tors}})$.