ELLIPTIC CURVES WITH COMPLEX MULTIPLICATION

PEDRO HENRIQUE PONTES

Let $E/\mathbb{C}$ be an elliptic curve. From the study of the endomorphism rings of elliptic curves over $\mathbb{C}$, we know that the endomorphism ring $\text{End}(E)$ of $E$ must be either isomorphic to $\mathbb{Z}$, or to an order in a quadratic imaginary extension of $\mathbb{Q}$ (see Theorem VI.5.5 of [Sil09]). In the second case, when $E$ has endomorphisms other than the multiplication-by-$m$ maps, we say that $E$ has complex multiplication. These curves will be the object of our study in this text, and we will closely follow the exposition of Chapter II of [Sil94]. All the definitions, results, and proofs presented here were in either [Sil94] or [Sil09].

We will start with remembering a few facts about elliptic curves over $\mathbb{C}$ in general that will be used in this text, and then proceed to develop the basic facts in the study of elliptic curves with complex multiplication. As an application, we will show how to construct some abelian field extensions, and show how this theory of elliptic curves with CM gives us an explicit construction of the Hilbert class field of quadratic imaginary extensions of $\mathbb{Q}$.

This text was written as a project for the course Math 574 Selected Topics in Number Theory: Elliptic Curves and Number Theory, taught by Prof. Dr. Jerrold Tunnell, Fall 2013.

1. Elliptic curves over $\mathbb{C}$

Here we will state some results of Chapter VI of [Sil09] that will be used in the text concerning the equivalence of elliptic curves over $\mathbb{C}$ and the lattices in $\mathbb{C}$. Note that we will also follow the notation of [Sil09].

Given a lattice $\Lambda$ in $\mathbb{C}$, we can define in $\mathbb{P}^2(\mathbb{C})$ the following

\[
E_\Lambda : y^2 = 4x^3 - g_2(\Lambda)x - g_3(\Lambda)
\]

which is an elliptic curve over $\mathbb{C}$ by Proposition VI.3.6 of [Sil09]. The same result also states that the map

\[
f : \mathbb{C}/\Lambda \to E_\Lambda
\]

\[
z \mapsto [\wp(z, \Lambda), \wp'(z, \Lambda), 1].
\]

is a complex analytic isomorphism of Lie groups (an isomorphism of Riemann surfaces that is also a group homomorphism).

Given an elliptic curve $E/\mathbb{C}$, by Theorem VI.5.1 of [Sil09] we see that there exists a lattice $\Lambda$ in $\mathbb{C}$ such that $E$ is isomorphic to $E_\Lambda$. This, with the isomorphism (2), shows us that every elliptic curve over $\mathbb{C}$ is given by a lattice $\Lambda$ as in (1), up to isomorphism.
In fact, we have an equivalence of categories (see Theorem VI.5.3 of [Sil09]), and by
Theorem VI.5.5 we have the isomorphism
\[ \text{End}(E_\Lambda) \simeq R = \{ \alpha \in \mathbb{C} : \alpha \Lambda \subseteq \Lambda \} . \]
Also given two lattices \( \Lambda, \Lambda' \) in \( \mathbb{C} \), the elliptic curves \( E_\Lambda \) and \( E_{\Lambda'} \) are isomorphic if, and only if \( \mathbb{C}/\Lambda \) and \( \mathbb{C}/\Lambda' \) are isomorphic, which happens if, and only if \( \Lambda \) and \( \Lambda' \) are homothetic.

We will soon restrict ourselves to the case when \( R \) is the ring of integers of a quadratic imaginary field \( K \), but for completeness we give the following definition:

**Definition.** Let \( K \) be a number field. An *order* \( R \) in \( K \) is a subring of \( K \) that is finitely generated as a \( \mathbb{Z} \)-module, and that \( R \otimes \mathbb{Q} = K \).

### 2. Complex multiplication basics

Let \( E/\mathbb{C} \) be an elliptic curve. If \( \text{End}(E) \simeq R \), where \( R \) is an order of the imaginary quadratic field \( K/\mathbb{Q} \), then we say that \( E \) has *complex multiplication* by \( R \). We will restrict ourselves to the case when \( R \) is the ring of integers of the field \( K \), which we denote by \( R_K \). Hence we may also say that \( E \) has *complex multiplication* by \( K \). So let us fix a field \( K \) and say that, from now on, \( K \) represents a quadratic imaginary extension of \( \mathbb{Q} \), and \( R_K \) is its ring of integers.

We start by fixing an isomorphism between \( \text{End}(E) \) and \( R \) that has nice properties:

**Proposition 1.** Let \( E/\mathbb{C} \) be an elliptic curve with complex multiplication by the ring \( R \subseteq \mathbb{C} \). Then there is a unique isomorphism \([\cdot] : R \to \text{End}(E)\) such that for any invariant differential \( \omega \) on \( E \), we have
\[ [\alpha] \ast \omega = \alpha \omega, \quad \text{for all } \alpha \in R. \]

In this case we say that the pair \((E, [\cdot])\) is *normalized*.

Note that this Proposition is basically an extension to the larger ring \( R \supseteq \mathbb{Z} \) of the property that, if \( \omega \) is an invariant differential on \( E \), then
\[ [m] \ast \omega = m \omega, \quad \text{for all } m \in \mathbb{Z} \]
(see Corollary III.5.3 in [Sil09]).

**Proof of Proposition 1** Let \( \Lambda \) be a lattice in \( \mathbb{C} \) such that \( E \) is isomorphic to \( E_\Lambda \). Now, two invariant differentials on \( E \) are scalar multiples of each other, since their quotient would be a translation-invariant function, hence, a constant. Also (by Section I of [Sil09]), the change from a Weierstrass equation to another changes an invariant differential only by a multiplicative constant, so it is enough to prove the result for an invariant differential of \( E_\Lambda \).
So let \( R = \{ \alpha \in \mathbb{C} : \alpha \Lambda \subseteq \Lambda \} \) and let \( f \) be the isomorphism. Then given \( \alpha \in R \), we need to define \([\alpha] \in \text{End}(E_\Lambda)\). Let
\[
\phi_\alpha : \mathbb{C}/\Lambda \to \mathbb{C}/\Lambda
\]
\[
z \mapsto \alpha z.
\]
Then \( \phi_\alpha \) is a holomorphic map on \( \mathbb{C}/\Lambda \), using \( \phi_\alpha \) and we can define \([\alpha]\) to be
\[
[\alpha] = f^{-1} \circ \phi_\alpha \circ f : E_\Lambda \to E_\Lambda,
\]
and this way \([\alpha]\) is an endomorphism of \( E_\Lambda \). Then the map \( \alpha \mapsto [\alpha] \) is a ring homomorphism, it is injective, and it is surjective since any map in \( \psi \in \text{End}(E_\Lambda) \) can be translated to a holomorphic map on \( \mathbb{C}/\Lambda \) by taking \( f \circ \psi \circ f^{-1} \), but any such holomorphic map is given by \( \phi_\alpha \) for some \( \alpha \in R \) (see Theorem VI.4.1 of \([\text{Sil09}]\)). Therefore \( \alpha \mapsto [\alpha] \) is a ring isomorphism.

Now we need to verify (3). Let \( \omega \) be an invariant differential on \( E_\Lambda \). Then we see that \( f^*\omega \) is an invariant differential on \( \mathbb{C}/\Lambda \). Again, since any two invariant differentials differ only by a scalar multiple, there exists \( c \in \mathbb{C} \) such that \( f^*\omega = cdz \), where \( dz \) is the invariant differential on \( \mathbb{C}/\Lambda \).

This way
\[
[\alpha]^*\omega = (f^{-1})^* \circ \phi_\alpha^* f^* \omega = (f^{-1})^* \circ \phi_\alpha^* (cdz) = (f^{-1})^* (c\alpha dz) = \alpha \omega,
\]
as we wanted to verify. Uniqueness follows from the next Corollary by taking \( E_1 = E_2 \) and \( \phi = [1] \);

**Corollary 2.** Let \((E_1, [\cdot]_1)\), \((E_2, [\cdot]_2)\) be normalized elliptic curves with complex multiplication by \( R \), and let \( \phi : E_1 \to E_2 \) be an isogeny. Then we have
\[
\phi \circ [\alpha]_1 = [\alpha]_2 \circ \phi.
\]

**Proof.** Let \( \omega \neq 0 \) be an invariant differential on \( E_2 \). Then since \( \phi^*\omega \) is an invariant differential on \( E_1 \), we have
\[
(\phi \circ [\alpha]_1)^* \omega = [\alpha]_1^\phi^* \omega = \alpha \phi^* \omega = \phi^*(\alpha \omega) = \phi^* \circ [\alpha]_2^\omega = ([\alpha]_2 \circ \phi)^* \omega
\]
using the fact that both \((E_1, [\cdot]_1)\), \((E_2, [\cdot]_2)\) are normalized. Hence (Theorem III.5.2 of \([\text{Sil09}]\))
\[
([\phi \circ [\alpha]_1] - ([\alpha]_2 \circ \phi)]^* \omega = 0.
\]
But since we are working in characteristic zero, every morphism is separable. So for every nonconstant morphism \( \psi : E_1 \to E_2 \), the map
\[
\Omega_{E_2} \to \Omega_{E_1}
\]
\[
\theta \mapsto \psi^* \theta
\]
is injective (Proposition II.4.2 of \([\text{Sil09}]\)). This means that (4) implies that the isogeny \((\phi \circ [\alpha]_1) - ([\alpha]_2 \circ \phi)\) is constant and equal to \( O \). \(\square\)
where \( \bar{\mathfrak{a}} \) map the ideal class group of \( R \) same ideal class as \( \mathfrak{a} \) to \( \mathfrak{a} \) using the fact that \( \mathfrak{a} \subseteq K \). But since \( \mathfrak{a} \) is a fractional ideal of \( K \), it follows that \( R = R_K \). Therefore \( E_\mathfrak{a} \) is an elliptic curve with complex multiplication by \( R_K \).

Now if \( c \in K \), then \( c\mathfrak{a} \) is another fractional ideal of \( K \), and the lattice \( c\mathfrak{a} \) is homothetic to \( \mathfrak{a} \). Hence \( E_\mathfrak{a} \) is isomorphic to \( E_{c\mathfrak{a}} \). That is; if \( b = c\mathfrak{a} \) is a fractional ideal of \( K \) in the same ideal class as \( \mathfrak{a} \), then \( E_\mathfrak{a} \) is isomorphic to \( E_b \). This way, if we denote by \( \mathcal{C}L(R_K) \) the ideal class group of \( R_K \), and by \( \mathcal{E}\mathcal{L}(R_K) \) the set of elliptic curves over \( \mathbb{C} \) with complex multiplication by \( R_K \), modulo isomorphisms over \( \mathbb{C} \), then we have an injective map

\[
\mathcal{C}L(R_K) \to \mathcal{E}\mathcal{L}(R_K)
\]

\[
\bar{\mathfrak{a}} \mapsto E_\mathfrak{a},
\]

where \( \bar{\mathfrak{a}} \) denotes the ideal class of \( \mathfrak{a} \).

Given a lattice \( \Lambda \) in \( \mathbb{C} \), we can also define the product

\[\mathfrak{a}\Lambda = \{\alpha_1\lambda_1 + \cdots + \alpha_r\lambda_r : \alpha_i \in \mathfrak{a}, \lambda_i \in \Lambda\} \]

We will prove that \( \mathfrak{a}\Lambda \) is a lattice in \( \mathbb{C} \), and this will give an action of the ideal class group \( \mathcal{C}L(R_K) \) on the lattices in \( \mathbb{C} \), and on \( \mathcal{E}\mathcal{L}(R_K) \);

**Lemma 3.** Let \( \Lambda \) be a lattice in \( \mathbb{C} \) such that \( E_\Lambda \in \mathcal{E}\mathcal{L}(R_K) \), and let \( \mathfrak{a} \) and \( \mathfrak{b} \) be nonzero fractional ideals of \( K \). Then

(a) \( \mathfrak{a}\Lambda \) is a lattice in \( \mathbb{C} \);

(b) \( E_{\mathfrak{a}\Lambda} \) is also in \( \mathcal{E}\mathcal{L}(R_K) \); and

(c) \( E_{\mathfrak{a}\Lambda} \simeq E_{\mathfrak{b}\Lambda} \) if, and only if \( \bar{\mathfrak{a}} = \bar{\mathfrak{b}} \) in \( \mathcal{C}L(R_K) \).

**Proof.** (a) Since \( \text{End}(E_\Lambda) \simeq R_K \), by what we have seen in \([5]\) we have \( R_K\Lambda \subseteq \Lambda \). Since \( 1 \in R_K \) we also have \( R_K\Lambda = \Lambda \). Let \( d \in R_K \) be such that \( d\mathfrak{a} \subseteq R_K \). Then \( d\mathfrak{a}\Lambda \subseteq R_K\Lambda = \Lambda \), hence \( \mathfrak{a}\Lambda \subseteq \frac{1}{d}\Lambda \). In particular, \( \mathfrak{a}\Lambda \) is a discrete additive subgroup of \( \mathbb{C} \). Now let \( d' \in R_K \) be such that \( d'R_K \subseteq \mathfrak{a} \). Then \( d'\Lambda = d'R_K\Lambda \subseteq \mathfrak{a}\Lambda \), hence \( \mathfrak{a}\Lambda \) spans \( \mathbb{C} \). Therefore \( \mathfrak{a}\Lambda \) is a lattice in \( \mathbb{C} \).

(b) Let \( R = \{\alpha \in \mathbb{C} : \alpha\mathfrak{a}\Lambda \subseteq \mathfrak{a}\Lambda\} \). We need to prove that \( R = R_K \). Note that \( R_K \subseteq R \) since \( R_K = \{\alpha \in \mathbb{C} : \alpha\Lambda \subseteq \Lambda\} \). On the other hand, if \( \alpha \in R \), then \( \alpha\mathfrak{a}\Lambda \subseteq \mathfrak{a}\Lambda \). Hence

\[\alpha\Lambda = \alpha R_K\Lambda = a^{-1}\alpha\mathfrak{a}\Lambda \subseteq a^{-1}\mathfrak{a}\Lambda = R_K\mathfrak{a}\Lambda \subseteq \Lambda , \]

and \( \alpha \in R_K \).

(c) If \( \bar{\mathfrak{a}} = \bar{\mathfrak{b}} \) then there exists \( c \in K \) such that \( \mathfrak{b} = c\mathfrak{a} \). But then \( \mathfrak{a}\Lambda \) and \( \mathfrak{b}\Lambda \) are homothetic lattices, and so \( E_{\mathfrak{a}\Lambda} \simeq E_{\mathfrak{b}\Lambda} \).
On the other hand, if $E_{a\Lambda} \simeq E_{b\Lambda}$, then $a\Lambda$ and $b\Lambda$ are homothetic, so there exists $c \in \mathbb{C}$ such that $c a\Lambda = b\Lambda$. Multiplying by $b^{-1}$ we have $c b^{-1} a\Lambda = R_K \Lambda = \Lambda$, but this implies that $c b^{-1} a \subseteq \{ \alpha \in \mathbb{C} : \alpha \Lambda \subseteq \Lambda \} = R_K$. In particular, $c \in K$. Similarly we have $c^{-1} a^{-1} b \subseteq R_K$. Hence the ideal $c^{-1} a^{-1} b$ is an integral ideal, but so is its inverse $c b^{-1} a$. Therefore $c b^{-1} a = R_K$, and $\tilde{a} = \bar{b}$.

**Definition.** Let $G$ be a group acting on a set $X$. Then the action of $G$ on $X$ is called *simply transitive* if, and only if given $x, y \in X$ there exists one, and only one $g \in G$ such that $gx = y$.

**Proposition 4.** The following action of $\mathcal{CL}(R_K)$ on $\mathcal{ELL}(R_K)$

$$\mathcal{CL}(R_K) \times \mathcal{ELL}(R_K) \to \mathcal{ELL}(R_K)$$

$$(\tilde{a}, E_{\Lambda}) \mapsto \tilde{a} \ast E_{\Lambda} = E_{a^{-1} \Lambda}.$$

is simply transitive. In particular,

$$\# \mathcal{CL}(R_K) = \# \mathcal{ELL}(R_K).$$

**Proof.** Note that (6) indeed defines an action of $\mathcal{CL}(R_K)$ on $\mathcal{ELL}(R_K)$ by Lemma 3 and because if we are given a lattice $\Lambda$ and fractional ideals $a, b$ of $R_K$, then

$$\tilde{a} \ast (\bar{b} \ast E_{\Lambda}) = \tilde{a} \ast E_{b^{-1} \Lambda} = E_{a^{-1} b^{-1} \Lambda} = E_{(ab)^{-1} \Lambda} = (\overline{ab}) \ast E_{\Lambda}.$$ 

Now we prove that the action (6) is transitive. Let $\Lambda_1, \Lambda_2$ be lattices in $\mathbb{C}$ such that $E_{\Lambda_1}, E_{\Lambda_2} \in \mathcal{ELL}(R_K)$. Let $\lambda_1 \in \Lambda_1$, $\lambda_1 \neq 0$, and consider the lattice $a_1 = \frac{1}{\lambda_1} \Lambda_1$. By Theorem VI.5.5 of [Sil09], the lattice $a_1$ is contained in $K$. Now, $a_1$ is a rank 2 free $\mathbb{Z}$-module, and since $R_K \Lambda_1 = \Lambda_1$ by the fact that $\text{End}(\Lambda_1) \simeq R_K$, it follows that $a_1$ is a finitely generated $R_K$-module, and so $a_1$ is a fractional ideal of $K$. Similarly we let $\lambda_2 \in \Lambda_2$, $\lambda_2 \neq 0$, and define the fractional ideal $a_2 = \frac{1}{\lambda_2} \Lambda_2$.

This way,

$$\frac{\lambda_2}{\lambda_1} a_2 a_1^{-1} \Lambda_1 = \lambda_2 a_2 a_1^{-1} \frac{1}{\lambda_1} \Lambda_1 = \lambda_2 a_2 a_1^{-1} a_1 = \lambda_2 a_2 = \Lambda_2.$$ 

So if we let $a = a_2^{-1} a_1$, then we have

$$\tilde{a} \ast E_{\Lambda_1} = E_{a a_1^{-1} \Lambda_1} = E_{a_1 a_2 a_1^{-1} \Lambda_1} \simeq E_{\Lambda_2}.$$ 

Therefore the action (6) is transitive. The action is also simply transitive by (c) of Lemma 3.

Let $E/\mathbb{C}$ be an elliptic curve with complex multiplication by $K$, and assume that $(E, [\cdot])$ is a normalized pair. Given $m \in \mathbb{Z}$, we have $E[m]$, the set of points $P \in E$ such that $[m]P = O$. Now, note that $E[m]$ is the same as the set of points $P \in E$ such that $[mr]P = O$ for any $r \in R_K$, that is; $[\alpha]P = O$ for any $\alpha \in mR_K$. This suggests that given an integral ideal $a$ of $R_K$, we can define

$$E[a] = \{ P \in E : [\alpha]P = O, \text{ for all } \alpha \in a \},$$
the group of \( a \)-torsion points of \( E \).

Also, if \( a \) is an integral ideal of \( R_K \) and \( \Lambda \) is a lattice in \( \mathbb{C} \) such that \( E_{\Lambda} \in ELL(R_K) \), then \( a\Lambda \subseteq \Lambda \), so \( \Lambda \subseteq a^{-1}\Lambda \), and we can define the homomorphism

\[
\mathbb{C}/\Lambda \to \mathbb{C}/a^{-1}\Lambda \\
z \mapsto z.
\]

Using the isomorphisms \( \mathbb{C}/\Lambda \cong E_{\Lambda} \) and \( \mathbb{C}/a^{-1}\Lambda \cong E_{a^{-1}\Lambda} \) given by (2) we have an isogeny

\[
(7) \quad E_{\Lambda} \to \check{a} \ast E_{\Lambda}
\]

whose kernel is \( E[a] \);

**Proposition 5.** Let \( E \in ELL(R_K) \) and let \( a \) be an integral ideal of \( R_K \). Then

(a) \( E[a] \) is the kernel of the map (7); and
(b) \( E[a] \) is a free \( R_K/a \)-module of rank 1. In particular,

\[
\#E[a] = N_{K/\mathbb{Q}}(a).
\]

**Proof.** (a) Let \( \Lambda \) be a lattice such that \( E_{\Lambda} \cong E \). Note that \( E_{\Lambda}[a] \) maps to \( E[a] \) via this isomorphism (see Corollary [2]), so it is enough to prove the result for \( E = E_{\Lambda} \).

Fix the isomorphism \( f : \mathbb{C}/\Lambda \to E_{\Lambda} \) given by (2). Note that from the proof of Proposition [1] we have \( [\alpha] = f \circ \phi_{\alpha} \circ f^{-1} \), where \( \phi_{\alpha}(z) = \alpha z \) on \( \mathbb{C}/\Lambda \). This way we see that

\[
f^{-1}(E[a]) = \{ z \in \mathbb{C}/\Lambda : \alpha z = 0 \text{ for all } \alpha \in a \}
= \{ z \in \mathbb{C} : \alpha z \in \Lambda \text{ for all } \alpha \in a \}/\Lambda
= \{ z \in \mathbb{C} : za \in \Lambda \}/\Lambda = a^{-1}\Lambda/\Lambda.
\]

But \( a^{-1}\Lambda/\Lambda \) is the kernel of the map \( \mathbb{C}/\Lambda \to \mathbb{C}/a^{-1}\Lambda \), so the image of this set by \( f \) is the kernel of the map (7).

(b) Let \( \lambda \in \Lambda, \lambda \neq 0 \), and consider the lattice \( \frac{1}{\lambda}\Lambda \). Then by Theorem VI.5.5 of [Sil09], we have \( \frac{1}{\lambda}\Lambda \subseteq K \), and in fact \( \frac{1}{\lambda}\Lambda \) is a fractional ideal of \( K \). Since \( \Lambda \) and \( \frac{1}{\lambda}\Lambda \) are homothetic, we can assume that \( \Lambda \subseteq K \) is a fractional ideal of \( K \) in the first place.

Now, we have that \( E \) is an \( R_K \)-module by the action

\[
\alpha \cdot P = [\alpha]P, \quad \alpha \in R_K, \ P \in E.
\]

It is in this way that we see \( E[a] \) as an \( R_K/a \)-module.

Note that from part (a) we have \( E[a] \cong a^{-1}\Lambda/\Lambda \) as \( R_K/a \)-modules. Now if \( q \) is an integral ideal of \( R_K \) dividing \( a \), we have

\[
(8) \quad (a^{-1}\Lambda/\Lambda) \otimes_{R_K} (R_K/q) \cong a^{-1}\Lambda/(\Lambda + qa^{-1}\Lambda) = a^{-1}\Lambda/qa^{-1}\Lambda,
\]
where we used the fact that \( R_K\Lambda = \Lambda \), so \( \Lambda = R_K\Lambda \subseteq qa^{-1}\Lambda \) since \( q \mid a \). Now by the Chinese Remainder Theorem, we have

\[
R_K/a \simeq \prod_{p\mid a} R_K/p^{e(p)}
\]

for some \( e(p) > 0 \), where \( p \) always denotes prime ideals. So taking the direct product in (8) and letting \( b = a^{-1}\Lambda \) (fractional ideal of \( K \)) we have

\[
E[a] \simeq a^{-1}\Lambda/\Lambda \simeq \prod_{p\mid a} b/p^{e(p)} b.
\]

Hence it is enough to prove that \( b/p^eb \) is a rank 1 free \( R_K/p^e \)-module for any \( e \geq 1 \).

To see the idea, first we prove this in the case \( e = 1 \). Since two elements of \( b \) are \( R_K \)-linearly dependent, it follows that \( b/pb \) is an \( R_K/p \)-vector space of dimension at most 1. This space cannot have dimension zero, since this would imply \( b = pb \), a contradiction. Therefore \( b/pb \) is a dimension 1 free module (vector space) over \( R_K/p \).

In the general case \( e \geq 1 \), we quotient out by \( p^e \); let

\[
R' = R_K/p^e, \quad b' = b/p^eb, \quad p' = p/p^e.
\]

So \( b' \) is an \( R' \)-module. Note that \( b'/p'b' \simeq b/pb \) over \( R'/p' \simeq R_K/p \). So by the case \( e = 1 \) we know that \( b'/p'b' \) is a dimension 1 vector space over \( R'/p' \). Now, \( R' \) is a local ring with maximal ideal \( p' \) (any ideal of \( R' \) must be a projection to \( R' \) of an ideal of \( R_K \) containing \( p^e \)). We have \( b' \) finitely generated over \( R' \), and \( b'/p'b' \) generated by one element over \( R'/p' \). So by a form of Nakayama’s Lemma (see [Jac89], the Corollary after Nakayama’s Lemma) we have \( b' \) a free \( R' \)-module of rank one.

**Corollary 6.** Let \( E \in ELL(R_K) \), \( a \) an integral ideal of \( R_K \), and \( \alpha \in R_K \). Then

(a) the degree of the map \( E \rightarrow \alpha * E \) is \( N_{K/Q}(\alpha) \); and

(b) the degree of the endomorphism \( [\alpha] : E \rightarrow E \) is \( |N_{K/Q}(\alpha)| \).

**Proof.** (a) Follows directly from Proposition 5

(b) Follows from Proposition 5 and the fact that \( \ker[\alpha] = E[\alpha R_K] \), so \( \# \ker[\alpha] = N_{K/Q}(\alpha R_K) = |N_{K/Q}(\alpha)| \). □

3. Rationality

**Lemma 7.** Let \( E/\mathbb{C} \) be an elliptic curve and \( \sigma : \mathbb{C} \rightarrow \mathbb{C} \) a field automorphism of \( \mathbb{C} \). Then

\[ \text{End}(E) \simeq \text{End}(E^\sigma) \]

**Proof.** This follows directly from the fact that if \( \phi : E \rightarrow E \) is an isogeny, then \( \phi^\sigma : E^\sigma \rightarrow E^\sigma \) is also an isogeny, and if also \( \psi \in \text{End}(E) \), then

\[ (\phi + \psi)^\sigma = \phi^\sigma + \psi^\sigma \quad \text{and} \quad (\phi \circ \psi)^\sigma = \phi^\sigma \circ \psi^\sigma. \] □
Proposition 8. Let $E/C$ be an elliptic curve with complex multiplication by $K$. Then
\[ |Q(j(E)) : Q| \leq h_K. \]
In particular, $j(E)$ is an algebraic number.

Remark. Actually, more is known; we will prove later in this text that $[Q(j(E)) : Q] = h_K$, and it is also known that $j(E)$ is in fact an algebraic integer (see Theorem II.6.1 of [Sil94]).

Proof of Proposition 8. We can assume that $E$ is given by a Weierstrass equation with coefficients in $C$. Let $\sigma : C \to C$ be a field automorphism of $C$, then $E^\sigma$ is given by the same Weierstrass equation, but with every coefficient changed to its image by $\sigma$. This way we see that $j(E^\sigma) = \sigma(j(E))$.

Also, by Lemma [7] we know that $E^\sigma$ is also in $\mathcal{ELL}(R_K)$. Now, by Proposition 4 there are only $h_K$ isomorphism classes in $\mathcal{ELL}(R_K)$, and every isomorphism class is represented by its $j$-invariant (two elliptic curves over $C$ are isomorphic over $C$ if, and only if they have the same $j$-invariant). Therefore $\sigma(j(E)) = j(E^\sigma)$ takes at most $h_K$ different values as $\sigma$ ranges through the automorphisms of $C$. This implies (9). \hfill \Box

Corollary 9. We have $\mathcal{ELL}(R_K) \simeq \{\text{elliptic curves } E/Q \text{ with } \text{End}(E) \simeq R_K \text{ isomorphism over } Q\}$.

Proof. This follows from the fact that if $E \in \mathcal{ELL}(R_K)$, then by Proposition 8 we have $j_0 = j(E) \in \overline{Q}$, so there exists an elliptic curve $E'/Q(j_0)$ such that $E'$ is isomorphic to $E$ over $C$ (see Proposition III.1.4 of [Sil09]). Moreover, if $E''$ is another elliptic curve over $\overline{Q}$ such that $E'' \simeq E$ over $C$, then $j(E'') = j_0$, so $E'$ and $E''$ have the same $j$-invariant, and this implies that $E' \simeq E''$ over $Q$. \hfill \Box

Proposition 10. Let $E/L$ be an elliptic curve with complex multiplication by $K$, where $L \subseteq C$.

(a) We have
\[ [\alpha]_E^\sigma = [\sigma(\alpha)]_{E^\sigma}, \quad \text{for all } \alpha \in R_K, \sigma \in \text{Aut}(C), \]
where $(E, [\cdot]_E)$ and $(E^\sigma, [\cdot]_{E^\sigma})$ are normalized pairs.

(b) Every endomorphism of $E$ is defined over the compositum $LK$.

Proof. (a) Let $\alpha \in R_K, \sigma \in \text{Aut}(C)$, and $\omega \neq 0$ be an invariant differential on $E$. Then $\omega^\sigma \neq 0$ is an invariant differential on $E^\sigma$, and we have
\[ ([\alpha]_E^\sigma)^* \omega^\sigma = ([\alpha]_{E^\sigma})^\sigma = (\alpha \omega)^\sigma = \sigma(\alpha) \omega = [\sigma(\alpha)]^{E^\sigma} \omega^\sigma. \]
Since $\omega^{\sigma} \neq 0$, from (10) we have $[\alpha]_E = [\sigma(\alpha)]_{E^{\sigma}}$ since we are in characteristic zero (see the end of the proof of Corollary 2).

(b) Let $\sigma : \mathbb{C} \rightarrow \mathbb{C}$ be an automorphism of $\mathbb{C}$ that fixes $LK$. Then since $\sigma$ fixes $L$ and $E$ is defined over $L$, we have $E^{\sigma} = E$. Also, if $\alpha \in R_K$ we have $\sigma(\alpha) = \alpha$, so by part (a) we have

$$[\alpha]_E^{\sigma} = [\sigma(\alpha)]_{E^{\sigma}} = [\alpha]_{E^{\sigma}} = [\alpha]_E.$$ 

Since $\sigma$ is any automorphism that fixes $LK$, it follows that the endomorphism $[\alpha]_E$ is defined over $LK$. □

4. THE ANALYTIC AND THE ALGEBRAIC ACTIONS ON $\mathcal{ELLL}(R_K)$

In view of Corollary 9, we will from now on consider $\mathcal{ELLL}(R_K)$ as the set of elliptic curves over $\mathbb{Q}$ with complex multiplication by $R_K$ modulo isomorphisms over $\mathbb{Q}$. So if we let $E \in \mathcal{ELLL}(R_K)$, then $E$ is an elliptic curve over $\mathbb{Q}$.

Fix $E \in \mathcal{ELLL}(R_K)$, and let $\sigma \in \text{Gal}(\overline{K}/K)$. Then since we are assuming that $E$ is an elliptic curve over $\overline{\mathbb{Q}}$, we can apply $\sigma$ to $E$ and obtain $E^{\sigma}$, given by changing the coefficients of the equations defining $E$ to their images by $\sigma$. This means we have an action

$$\text{Gal}(\overline{K}/K) \times \mathcal{ELLL}(R_K) \rightarrow \mathcal{ELLL}(R_K)$$

$$ (\sigma, E) \mapsto E^{\sigma}$$

of $\text{Gal}(\overline{K}/K)$ on $\mathcal{ELLL}(R_K)$.

Now, given $\sigma \in \text{Gal}(\overline{K}/K)$ and $E \in \mathcal{ELLL}(R_K)$, there exists a fractional ideal $a$ of $K$ such that $E^{\sigma} = \overline{a} \ast E$ by Proposition 4. Since the ideal class $\overline{a}$ is unique (we are considering elliptic curves modulo isomorphisms over $\overline{\mathbb{Q}}$), we can define a function

$$F : \text{Gal}(\overline{K}/K) \rightarrow \mathcal{CL}(R_K)$$

$$ \sigma \mapsto \overline{a}$$

given by the above property; if $\sigma \in \text{Gal}(\overline{K}/K)$, we define $F(\sigma) = \overline{a}$ to be the unique ideal class such that

$$E^{\sigma} = F(\sigma) \ast E.$$

The function $F$ is a very important function that, in a way, translates the algebraic action (11) of the Galois group to the analytic action (6) of the ideal class group.

We will now prove some properties of $F$.

**Theorem 11.** The function $F : \text{Gal}(\overline{K}/K) \rightarrow \mathcal{CL}(R_K)$ defined by (12) is a homomorphism, and it is independent of the choice of the elliptic curve $E$.

First we need more information about how the action (11) of the Galois group interacts with the action (6) of the ideal class group;
Lemma 12. Let $E/\overline{\mathbb{Q}}$ be an elliptic curve with complex multiplication by $K$. Let $\mathfrak{a}$ be a fractional ideal of $K$ and $\sigma \in \text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$. Then

$$(\mathfrak{a} \ast E)^\sigma = \sigma(\mathfrak{a}) \ast E^\sigma.$$ 

Proof. Let $\Lambda$ be a lattice in $\mathbb{C}$ such that $E_\Lambda \simeq E$. We can assume that $E_\Lambda$ is also an elliptic curve over $\overline{\mathbb{Q}}$, and that $E_\Lambda$ and $E$ are isomorphic over $\mathbb{Q}$ (see Theorem VI.5.1 of [Sil09]).

Since $\mathfrak{a}$ is a finitely-generated $R_K$-module, we can fix a presentation of $\mathfrak{a}$; that is, we fix an $m \times n$ matrix $A$ with coefficients in $R_K$ such that

$$R_K^m \xrightarrow{A} R_K^n \xrightarrow{\mathfrak{a}} 0$$

is an exact sequence. We take the “product” of this sequence and the sequence of $R_K$-modules

$$(13) \quad 0 \to \Lambda \to \mathbb{C} \to E \to 0$$

and we obtain the following diagram

$$(14) \quad \begin{array}{cccc}
0 & 0 & 0 & 0 \\
\downarrow & \downarrow & \downarrow & \downarrow \\
0 & \text{Hom}(\mathfrak{a}, \Lambda) & \text{Hom}(\mathfrak{a}, \mathbb{C}) & \text{Hom}(\mathfrak{a}, E) \\
\downarrow & \downarrow & \downarrow & \downarrow \\
0 & \text{Hom}(R_K^m, \Lambda) & \text{Hom}(R_K^m, \mathbb{C}) & \text{Hom}(R_K^m, E) \\
\downarrow & \downarrow & \downarrow & \downarrow \\
0 & \text{Hom}(R_K^m, \Lambda) & \text{Hom}(R_K^m, \mathbb{C}) & \text{Hom}(R_K^m, E) \\
\end{array}$$

where $\text{Hom}(M, N)$ denotes the $R_K$-homomorphisms from the $R_K$-modules $M$ to $N$. This way, $\text{Hom}(R_K^m, M) \simeq M^n$. More generally, we have

Claim. If $M \subseteq \mathbb{C}$ is an $R_K$-module, then the map

$$\phi : \mathfrak{a}^{-1}M \to \text{Hom}(\mathfrak{a}, M)$$

$$x \mapsto \phi_x,$$

where $\phi_x(\alpha) = \alpha x$, is an isomorphism.

One can prove directly that $\phi$ is an $R_K$-monomorphism, so we only prove that $\phi$ is surjective. Given $\psi \in \text{Hom}(\mathfrak{a}, M)$, we need to find $x \in \mathfrak{a}^{-1}M$ such that $\psi = \phi_x$. To this end, we extend $\psi$ to $R_K$ in the following way: we know that $R_K = \mathfrak{a}^{-1} \cdot \mathfrak{a}$, so given $r \in R_K$, we write $r = \sum_i \beta_i \alpha_i$ with $\beta_i \in \mathfrak{a}^{-1}$ and $\alpha_i \in \mathfrak{a}$, and we let

$$\bar{\psi}(r) = \bar{\psi} \left( \sum_i \beta_i \alpha_i \right) = \sum_i \beta_i \psi(\alpha_i) \in \mathfrak{a}^{-1}M.$$
Let us verify that $\bar{\psi}$ is well-defined. If $\sum_i \beta_i \alpha_i = 0$, then let $d \in \mathbb{R}_K$, $d \neq 0$, be such that $d \alpha_i^{-1} \subseteq \mathbb{R}_K$. Then $\sum_i d \beta_i \alpha_i \in \mathbb{R}_K$, so

$$0 = \psi(0) = \psi \left( \sum_i d \beta_i \alpha_i \right) = \sum_i d \beta_i \psi(\alpha_i)$$

and cancelling $d$ we get $\sum_i \beta_i \psi(\alpha_i) = 0$. Hence $\bar{\psi}$ is well-defined. Also $\bar{\psi}$ is an $\mathbb{R}_K$-homomorphism from $\mathbb{R}_K$ to $\alpha^{-1} M$, so if we let $x = \bar{\psi}(1)$, we have $\bar{\psi}(r) = rx$ for any $r \in \mathbb{R}_K$. This implies that $\psi = \phi_x$, and proves the Claim.

So applying the Claim to the diagram (14), we get

$$0 \rightarrow \Lambda \rightarrow \mathbb{C} \rightarrow \text{Hom}(\alpha, E) \rightarrow 0$$

$$0 \rightarrow \Lambda^n \rightarrow \mathbb{C}^n \rightarrow \Lambda^n \rightarrow 0$$

$$0 \rightarrow \Lambda^m \rightarrow \mathbb{C}^m \rightarrow \Lambda^m \rightarrow 0$$

where $A^t$ is the transpose of $A$. We also add the arrows to the right at the last two lines of (15) since they are just $n$ and $m$ copies of the sequence (13). Now we apply the Snake Lemma (see Exercise 6.3.1 of [Jac89]) to the bottom two lines of (15) and obtain

$$0 \rightarrow \Lambda^{-1} \rightarrow \mathbb{C} \rightarrow \ker(E^a A^t \rightarrow E^m) \rightarrow \Lambda^m / A^t \Lambda^n \rightarrow \cdots$$

Hence $\bar{a} * E \simeq \mathbb{C} / \alpha^{-1} \Lambda \simeq \ker \Delta$.

Since $A$ is a matrix of coefficients in $\mathbb{R}_K = \text{End}(E)$, the map $A^t : E^n \rightarrow E^m$ is an algebraic map of algebraic varieties, so the kernel $\ker(E^n A^t \rightarrow E^m)$ is an algebraic subvariety of $E^n$. Moreover, $\ker(E^n A^t \rightarrow E^m)$ is a subgroup of $E^n$. Now $\Lambda^m / A^t \Lambda^n$ is discrete, so $\ker \Delta$ must be the union of connected components of $\ker(E^n A^t \rightarrow E^m)$. On the other hand, $\ker \Delta \simeq \mathbb{C} / \alpha^{-1}$, so $\ker \Delta$ is connected. Therefore $\ker \Delta$ is the connected component of the identity in $\ker(E^n A^t \rightarrow E^m)$. This way

$$\bar{a} * E \simeq \mathbb{C} / \alpha^{-1} \simeq \text{the identity component of } \ker(E^n A^t \rightarrow E^m).$$

So now if we apply $\sigma \in \text{Gal}(\overline{\mathbb{Q}} / \mathbb{Q})$ to $\bar{a} * E$ and use the identification (16) we get

$$(\bar{a} * E)^\sigma \simeq \left( \text{the identity component of } \ker(E^n A^t \rightarrow E^m) \right)^\sigma$$

$$\simeq \text{the identity component of } \ker((E^n)^\sigma A^t \rightarrow (E^m)^\sigma)$$

$$\simeq \sigma(\bar{a}) * E^\sigma.$$  \hfill \Box

Now we can prove Theorem 11.
Proof of Theorem 11. Let us prove the fact that $F$ is independent of the choice of the elliptic curve. That is, given $\sigma \in \text{Gal}(\overline{K}/K)$, $E, E' \in \mathcal{EL}(R_K)$, and $a, b$ fractional ideals of $K$ such that

$$\bar{a} \cdot E = E^\sigma, \quad \bar{b} \cdot E' = (E')^\sigma,$$

we need to prove that $\bar{a} = \bar{b}$. Let $c$ be a fractional ideal of $K$ such that $E' = c \cdot E$. Then applying Lemma 12 we have

$$(\bar{b} \cdot \bar{c}) \cdot E = \bar{b} \cdot E' = (E')^\sigma = (\bar{c} \cdot E)^\sigma = \sigma(\bar{c}) \cdot E^\sigma = (\bar{c} \cdot \bar{a}) \cdot E.$$ 

Hence $\bar{b} \cdot \bar{c} = \bar{c} \cdot \bar{a}$, and so $\bar{a} = \bar{b}$.

Now we use the fact that the definition of $F$ is independent of the choice of $E$ to prove that $F$ is a homomorphism. Let $E \in \mathcal{EL}(R_K)$ and $\sigma, \tau \in \text{Gal}(\overline{K}/K)$. Then using Lemma 12 again we have

$$F(\sigma \tau) \cdot E = E^{\sigma \tau} = (E^\tau)^\sigma = (F(\tau) \cdot E)^\sigma = \sigma(F(\tau)) \cdot E^\sigma = F(\sigma) \cdot (F(\tau) \cdot E) = (F(\tau)F(\sigma)) \cdot E$$

and so $F(\sigma \tau) = F(\sigma)F(\tau)$. $\square$

5. Notation for class field theory

Let us fix some notation from class field theory. To learn more about this area of algebraic number theory, see for example [Lan94] or [Neu99].

Let $L/K$ be a finite abelian extension, and let $c$ be an integral ideal of $K$ that is divisible by all primes that ramify in $L/K$. Then we denote the Artin map of $L/K$ by

$$(\cdot, L/K) : I(c) \to \text{Gal}(L/K).$$

The Artin map is multiplicative in $I(c)$, and we write $\sigma_p = (p, L/K)$. This element $\sigma_p$ is uniquely determined by the property that, if $\mathfrak{p}$ is a prime in $L$ lying over $p$, then

$$\sigma_p(x) \equiv x^{N_{K/Q}(p)} \pmod{\mathfrak{p}}, \quad \text{for all } x \in L,$$

in the sense that the element $\sigma_p(x) - x^{N_{K/Q}(p)}$ has positive $\mathfrak{p}$-adic valuation.

For some choice of $\mathfrak{c}$ we have $((\alpha), L/K) = 1$ for every $\alpha \in K^*$ such that $\alpha \equiv 1 \pmod{c}$. The largest such $\mathfrak{c}$ is called the conductor of $L/K$, and will be denoted $\mathfrak{c}_{L/K}$. We also define

$$P(c) = \{ (\alpha) : \alpha \equiv 1 \pmod{c} \},$$

so $P(c)_{L/K}$ is contained in the kernel of the Artin map $(\cdot, L/K) : I(c)_{L/K} \to \text{Gal}(L/K)$.

We will also need Dirichlet’s Theorem on primes in arithmetic progressions:

**Theorem 13.** Let $L$ be a number field and $\mathfrak{c}$ an integral ideal of $L$. Then every ideal class of $I(c)/P(c)$ contains infinitely many degree 1 primes of $L$. 

6. Abelian extensions

Our first application of the theory of elliptic curves with complex multiplication gives us a way to build certain abelian extensions:

**Theorem 14.** Let $E/F$ be an elliptic curve with complex multiplication by $K$, $F \subseteq \mathbb{C}$. Let $L = FK(j(E), E_{\text{tors}})$ be the field extension of $FK$ generated by $j(E)$ and the all the coefficients of the $R_K$-torsion points of $E$. Then $L/FK(j(E))$ is an abelian extension.

**Proof.** Let $H = FK(j(E))$, $a$ an integral ideal of $R_K$, and let $L_a = H(E[a])$. Then $L$ is the compositum of all the $L_a$, so all we need to prove is that $L_a/H$ is an abelian extension. We define a homomorphism

$$\rho : \text{Gal}(L_a/H) \to \text{Aut}(E[a])$$

by

$$\rho(\sigma)P = P^\sigma, \quad \text{for all } \sigma \in \text{Gal}(L_a/H), P \in E[a].$$

Given $\sigma \in \text{Gal}(L_a/H)$ and $P \in E[a]$, we indeed have $P^\sigma \in E[a]$ by Proposition 10 if $a \in a$ we have

$$[\alpha]P^\sigma = [\sigma(\alpha)]P^\sigma = [\alpha]^\sigma P^\sigma = ([\alpha]P)^\sigma = O,$$

since $E^\sigma = E$, given that $E$ is defined over $H$. If also $Q \in E[a]$, then $(P + Q)^\sigma = P^\sigma + Q^\sigma$ (again since $E$ is defined over $H$), so $\rho$ is indeed well-defined.

Now note that the image of $\text{Gal}(L_a/H)$ by $\rho$ is actually contained in the automorphisms of $E[a]$ that are also $R_K/a$-automorphisms (see $E[a]$ as an $R_K/a$-module) by a calculation similar to (18). Also, the map $\rho$ is injective, since if two maps $\sigma, \tau \in \text{Gal}(L_a/H)$ are mapped to the same element of $E[a]$, then $\sigma$ and $\tau$ act the same way on the coordinates of the elements of $E[a]$, but since $L_a$ is generated by these coordinates, we conclude that $\sigma = \tau$. Therefore we have a monomorphism

$$\rho : \text{Gal}(L_a/H) \hookrightarrow \text{Aut}_{R_K/a}(E[a]) \simeq (R_K/a)^*$$

by using Proposition 5(b). This implies that $\text{Gal}(L_a/H)$ is abelian. \hfill $\square$

Our next goal is to prove the following big theorem:

**Theorem 15.** Let $E \in \mathcal{E}\mathcal{L}\mathcal{L}(R_K)$. Then $H = K(j(E))$ is the Hilbert class field of $K$.

**Proof.** Here we will heavily use the function $F$ defined in Section 4. Since $F$ is a homomorphism, we have $\text{Gal}(\overline{K}/K)/\ker F \simeq \text{Im } F$ a subgroup of $\mathcal{C}\mathcal{L}(R_K)$, and hence $\text{Gal}((\overline{K}/K)/\ker F$ is an abelian group. So let $L$ be the fixed field of $\ker F$. Then $\text{Gal}(L/K) \simeq \text{Gal}(\overline{K}/K)/\ker F$ is abelian so $L/K$ is a finite abelian extension.

Now if $\sigma \in \text{Gal}(\overline{K}/K)$, then $\sigma \in \ker F$ if, and only if $E^\sigma \simeq E$, that is; if, and, only if $j(E) = j(E^\sigma) = \sigma(j(E))$. Thus $\ker F = \{ \sigma \in \text{Gal}(\overline{K}/K) : \sigma(j(E)) = j(E) \}$, which is just $\text{Gal}(\overline{K}/K(j(E)))$, and so $L = K(j(E))$. 

In fact, $F$ is an injective map from $\text{Gal}(L/K)$ to $\mathcal{CL}(R_K)$. Given $\sigma \in \text{Gal}(\overline{K}/K)$, the value of $F(\sigma)$ is given by the relation

$$j(F(\sigma) \ast E) = \sigma(j(E)),$$

that is, to calculate $F(\sigma)$ we need only know the value of $\sigma(j(E))$. But then we only needed to know the values of $\sigma$ on the field $L$. Moreover, since $L/K$ is Galois, all the conjugates of $j(E)$ also belong to $L$.

To prove Theorem 15, we will need the following result, the proof of which we postpone:

**Lemma 16.** There exists a finite set of rational primes $S \subseteq \mathbb{Z}$ such that, if $p \in \mathbb{Z} \setminus S$ is a prime which splits in $K$ as $pR_K = p^r$, then

$$F(\sigma_p) = \bar{p},$$

where $\sigma_p = (p, L/K)$.

From Lemma 16 we can prove the following

**Claim.** For any $a \in I(\mathfrak{c}_{L/K})$ we have

$$F((a, L/K)) = \bar{a}.$$

Given $a \in I(\mathfrak{c}_{L/K})$, by Theorem 13 there exists a degree 1 prime ideal $p \in I(\mathfrak{c}_{L/K})$ in the same ideal class as $a$ in $I(\mathfrak{c}_{L/K})/P(\mathfrak{c}_{L/K})$, and we can also assume that $p$ does not lie above any prime in the set $S$ of Lemma 16. Hence there exists $\alpha \in K$, $\alpha \equiv 1 \pmod{\mathfrak{c}_{L/K}}$, such that $a = p(\alpha)$. But then $(\alpha)$ is in the kernel of the Artin map, so

$$F((a, L/K)) = F((p, L/K)((\alpha), L/K)) = F((p, L/K)) = \bar{p} = \bar{a}$$

by Lemma 16. This proves the Claim.

Note that this Claim implies the fact that, if $(\alpha) \in I(\mathfrak{c}_{L/K})$ is a principal ideal, then $F(((\alpha), L/K)) = 1$. This implies that the conductor of $L/K$ is $(1)$, which in turn means that $L/K$ is an unramified extension. Since $H$ is the maximal abelian unramified extension of $K$, we conclude that $L \subseteq H$.

Also note that, from the Claim, it follows that $F$ is surjective, so $\text{Gal}(L/K) \simeq \mathcal{CL}(R_K)$. In particular $[L : K] = h_K = \#\mathcal{CL}(R_K)$. But also $[H : K] = h_K$, therefore $L = H$. \hfill $\Box$

Using the proof of Theorem 15 we can also obtain the following result:

**Theorem 17.** If $E \in \mathcal{ECL}(R_K)$, then we have

$$[\mathbb{Q}(j(E)) : \mathbb{Q}] = [K(j(E)) : K] = h,$$

where $h = \#\mathcal{CL}(R_K)$. In particular, if $E_1, \ldots, E_h$ form a set of representatives for the isomorphism classes of $\mathcal{ECL}(R_K)$, then $j(E_1), \ldots, j(E_h)$ are all the conjugates of $j(E)$ under $\text{Gal}(\overline{K}/K)$. Moreover, if $a$ is an integral ideal of $R_K$, then

$$a(H/K)(j(E)) = j(\bar{a} \ast E).$$
Remark. Equation (20) is the reason why we defined the action \( \bar{a} \ast E_\Lambda \) to be \( E_{a^{-1}\Lambda} \) and not \( E_{a\Lambda} \); this way the action of \( \mathcal{CL}(R_K) \) on \( \mathcal{E}\mathcal{L}(R_K) \) is more "compatible" with the Artin symbol.

Proof. From Proposition 8 and the fact that \([K(j(E)) : K] = h\) we get (19);

\[
\begin{array}{c}
  K(j(E)) \\
  \downarrow^{\leq 2} \\
  \downarrow^{\leq h}
\end{array}
\]

\[
\begin{array}{c}
  \mathbb{Q}(j(E)) \\
  \downarrow^{2}
\end{array}
\]

Equation (20) follows directly from the Claim in the proof of Theorem 15, noting that \( c_{L/K} = (1) \). □

So now it remains to prove Lemma 16. First, we need a result on what happens with elliptic curves and their isogenies when we reduce them modulo a prime.

Proposition 18. Let \( E_1, E_2 \) be elliptic curves over some number field \( L \). Let \( \mathfrak{P} \) be a maximal ideal of \( L \). Let \( \tilde{E}_1, \tilde{E}_2 \) be the reductions modulo \( \mathfrak{P} \) of \( E_1, E_2 \). We assume that \( E_1, E_2 \) both have good reduction at \( \mathfrak{P} \), that is; \( \tilde{E}_1 \) and \( \tilde{E}_2 \) are both nonsingular, and are both elliptic curves. Then the natural reduction map

\[
\text{Hom}(E_1,E_2) \to \text{Hom}(\tilde{E}_1,\tilde{E}_2)
\]

\[
\phi \mapsto \tilde{\phi}
\]

preserves the degrees of the isogenies. In particular, this map is injective.

Proof. Choose a prime \( l \) relatively prime to \( \mathfrak{P} \). Let \( e_E : T_l(E) \times T_l(E) \to T_l(\mu) \) denote the Weil pairing of an elliptic curve \( E \) defined over \( L \). If \( \phi : E_1 \to E_2 \) is an isogeny, then we recall that for any \( x, y \in T_l(E) \) we have

\[
e_{E_1}(x,y)^{\deg \phi} = e_{E_1}([\deg \phi]x,y) = e_{E_1}(\hat{\phi}x,y) = e_{E_2}(\phi x, \phi y).
\]

Similarly,

\[
e_{E_1}(\tilde{x},\tilde{y})^{\deg \tilde{\phi}} = e_{E_2}(\hat{\phi}x\tilde{y}).
\]

Also, if \( E \) has good reduction modulo \( \mathfrak{P} \), then \( T_l(E) \simeq T_l(\tilde{E}) \) (see Proposition VII.3.1 of [Sil09]). Furthermore, note that from the definition of the Weil pairing we have

\[
e_{\tilde{E}}(\tilde{x},\tilde{y}) = e_{\tilde{E}}(\tilde{x},\tilde{y}).
\]

With this information about how the Weil pairing behaves under reduction, we can use it to relate \( \deg \phi \) and \( \deg \tilde{\phi} \):

\[
e_{\tilde{E}_1}(\tilde{x},\tilde{y})^{\deg \phi} = e_{\tilde{E}_1}(\tilde{x},\tilde{y})^{\deg \phi} = e_{E_2}(\phi x, \phi y) = e_{E_2}(\hat{\phi}x\tilde{y}) = e_{\tilde{E}_1}(\tilde{x},\tilde{y})^{\deg \tilde{\phi}}.
\]

Since \( x, y \in T_l(E) \) are arbitrary, we conclude that \( \deg \phi = \deg \tilde{\phi} \). □
Now we proceed to the proof of Lemma 16.

Proof of Lemma 16. Let $E_1, \ldots, E_h$ be a set of representatives of each isomorphism class of $\mathcal{EL}^R(K)$. We can assume that $E_1, \ldots, E_h$ are defined over $\overline{\mathbb{Q}}$. Let $M'$ be a field containing all the coefficients of the equations defining $E_1, \ldots, E_h$, and let $M$ be an extension of $M'$ over which all the isogenies between the curves $E_1, \ldots, E_h$ are defined. Note that we can choose $M$ so that $M/K$ is finite. Let us prove this fact for the isogenies in $\text{Hom}(E_1, E_2)$.

Since this is a finitely-generated group by Corollary III.7.5 of [Sil09], it suffices to find a finite extension of $M'$ over which a given isogeny $\phi \in \text{Hom}(E_1, E_2)$ is defined. Given $\sigma \in \text{Aut}(\mathbb{C})$ that fixed $L$, we have $\phi^{\sigma} \in \text{Hom}(E_1, E_2)$ with $\text{deg} \phi = \text{deg} \phi^{\sigma}$. But the number of isogenies of a fixed degree in $\text{Hom}(E_1, E_2)$ is finite by Corollary III.4.11 of [Sil09], since the number of subgroups of $E_1$ of bounded order is finite, and the number of automorphisms of $E_2$ is also finite (they correspond to the units of $R_K$). Therefore we can choose $M/K$ a finite extension.

Now let $S$ be the set of rational primes satisfying at one of the following:

(i) $p$ ramifies in $M$;
(ii) some $E_i$ has bad reduction over a prime lying over $p$; or
(iii) $p$ divides either the denominator or the numerator of some of the numbers $N_{M/Q}(j(E_i) - j(E_k))$ for some $i \neq k$.

We will prove the result for this set $S$. So let $p \in \mathbb{Z} \setminus S$ be an unramified prime such that $pR_K = pp'$ in $K$, and let $\mathfrak{P}$ be a prime lying over $p$. Note also that $L \subseteq M$, but the definition of $\sigma_p$ shows that $(p, M/K)|L = (p, L/K)$. So it is enough to consider $\sigma_p = (p, M/K)$.

Let $E \in \mathcal{EL}(R_K)$, and let $\Lambda$ be a lattice in $\mathbb{C}$ such that $E \cong E_{\Lambda}$. Choose an integral ideal $a$ of $R_K$ such that $a$ is prime with $p$, and $ap = (\alpha)$ is a principal ideal. We have seen that we can define maps such as in (7), so we obtain the following diagram:

$$
\begin{array}{cccc}
\mathbb{C}/\Lambda & \longrightarrow & \mathbb{C}/p^{-1}\Lambda & \longrightarrow & \mathbb{C}/a^{-1}p^{-1}\Lambda = \mathbb{C}/(\alpha^{-1})\Lambda & \longrightarrow & \mathbb{C}/\Lambda,
\end{array}
$$

where the maps are all $z \mapsto z$, except for the last one, which is $z \mapsto \alpha z$. In terms of the invariant differential $dz$ on $\mathbb{C}/\Lambda$, the pullback through all these maps would be just $d(\alpha z) = \alpha dz$.

Now, in terms of the isomorphic elliptic curves, we have maps

$$
E \longrightarrow \tilde{\mathfrak{P}} \ast E \longrightarrow (\tilde{\mathfrak{P}} \ast \tilde{a}) \ast E = (\alpha) \ast E \longrightarrow E,
$$
say, $\phi$, $\psi$, and $\lambda$, respectively. We assume that $E$ is given by a Weierstrass equation that is minimal at $\mathfrak{P}$ and let

$$
\omega = \frac{dx}{2y + a_1x + a_2}
$$

be the invariant differential of $E$ associated to this Weierstrass equation. Then taking the pullback and comparing to (21) we get

$$
(\lambda \circ \psi \circ \phi)^*\omega = \alpha\omega.
$$
Now we reduce modulo $\mathfrak{p}$. Since we chose a Weierstrass equation minimal at $\mathfrak{p}$, the reduced curve $\tilde{E}$ has a Weierstrass equation obtained by just taking each coefficient modulo $\mathfrak{p}$ in the equation for $E$ (see Sections 1 and 2 of Chapter VII of [Sil94]). This way the reduced differential

$$\tilde{\omega} = \frac{dx}{2y\tilde{a}_1 x + \tilde{a}_2}$$

is also an invariant differential of $\tilde{E}$, but now from (22) we have

$$(\tilde{\lambda} \circ \tilde{\psi} \circ \tilde{\phi})^* \tilde{\omega} = (\lambda \circ \psi \circ \phi)^* \omega = \tilde{\alpha} \tilde{\omega} = 0$$

since $\alpha \in \mathfrak{p}$. Since $\tilde{\omega}$ is an invariant differential, it follows that $\tilde{\lambda} \circ \tilde{\psi} \circ \tilde{\phi}$ is inseparable.

By Proposition 18 we have $\deg \tilde{\lambda} = \deg \lambda = 1$, since $\lambda$ is an isomorphism. Similarly, by Corollary 6 we have $\deg \tilde{\psi} = \deg \psi = N_{K/Q} \mathfrak{a}$, and $\deg \tilde{\phi} = N_{K/Q} \mathfrak{p} = p$. Now we know that any isogeny of curves over $\mathbb{F}_p$ can be written as a composition of a $p^k$-th power Frobenius map (of degree $p^k$) and a separable map. Since $\mathfrak{a}$ is prime with $p$ by hypothesis, it follows that $\tilde{\psi}$ is separable. Therefore $\tilde{\phi}$ must be inseparable. Since $\tilde{\phi}$ has degree $p$, it must be the composition of the $p$-th power Frobenius map and an isogeny of degree 1, that is; an isomorphism. Say, $\tilde{\psi} = \text{Fr}_p \circ \theta$, where $\theta : \tilde{E}(p) \to \tilde{\mathfrak{p}}^* \tilde{E}$ is an isomorphism.

This isomorphism $\theta$ is what we were looking for. Since $\tilde{E}(p)$ and $\tilde{\mathfrak{p}}^* \tilde{E}$ are isomorphic, we have

$$j(\tilde{\mathfrak{p}}^* \tilde{E}) = j(\tilde{E}(p)) = j(\tilde{E})^p,$$

since $\tilde{E}(p)$ is just $\tilde{E}$ with each coefficient of the defining Weierstrass equation changed to its $p$-th power. But considering the coefficients, we see that $j(E) \equiv j(\tilde{E}) \pmod{\mathfrak{p}}$, so

$$j(\tilde{\mathfrak{p}}^* E) \equiv j(E)^p \pmod{\mathfrak{p}}.$$ 

Now, by (17) we have $j(E)^p \equiv \sigma_p(j(E)) = j(E^{\sigma_p}) \pmod{\mathfrak{p}}$, so

$$j(E^{\sigma_p}) \equiv j(\tilde{\mathfrak{p}}^* E) \pmod{\mathfrak{p}}.$$ 

But by (iii) of the definition of the set $S$, this implies that $j(E^{\sigma_p}) = j(\tilde{\mathfrak{p}}^* E)$, and this means that $F(\sigma_p) = \tilde{\mathfrak{p}}$. 

References


