Complex Multiplication and Hilbert Class Fields for Imaginary Quadratic Fields

Wei Wenqing

May 2023

Abstract

The goal of this paper is to prove that the Hilbert class field for an imaginary quadratic field K is by adjoining the j-invariant of elliptic curve over $\mathbb{C}$ with complex multiplication by $\mathcal{O}_K$. In Section 1 we briefly introduce the theory of elliptic curves, especially the equivalence between elliptic curves over $\mathbb{C}$ and complex tours. In Section 2 we study elliptic curves with complex multiplication. In Section 3 we state some relevant results of class field theory. Finally, we prove our main theorem in Section 4.

1 Introduction to elliptic curves

In this section, we give a brief introduction to the theory of elliptic curves. First, we will introduce properties that hold for elliptic curves defined over arbitrary fields. Then we will discuss more about elliptic curves over $\mathbb{C}$, since the elliptic curves in which we are primarily interested is defined over $\mathbb{C}$.

Definition 1.1. *A curve C over an algebraically closed field K is an irreducible regular projective K-scheme of dimension 1. A curve C over arbitrary field k is a k-scheme such that $C_{\overline{k}} = C \times_k \mathit{Spec}\ \overline{k}$ is a curve over algebraically closed field.*

Definition 1.2. *A curve E is called elliptic curve if the genus is 1.*

For elliptic curve E over k, fix a k-point $x \in E$, then there is a bijection between $E(k)$ and $\mathrm{Pic}^0(E)$, given by:

$$E(k) \longrightarrow \mathrm{Pic}^0(E) \qquad x \longmapsto \mathcal{O}((x) - (e))$$

This bijection gives $E(k)$ an abelian group structure with identity e. By Riemann-Roch theorem, $\dim(\mathcal{O}(ne)) = n$, one can prove that

Theorem 1.3. *Let E be an elliptic curve over k, char $k \neq 2, 3$, then there is a closed embedding $E \longrightarrow \mathbb{P}^2$ such that the image is a closed subscheme defined by Weierstrass equation $y^2 = x^3 + ax + b$, $a, b \in k$.*

Definition 1.4. *Let E be an elliptic curve defined by $y^2 = x^3 + ax + b$, the j-invariant for E is*

$$j(E) = 1728 \frac{4a^3}{4a^3 + 27b^2}$$

j-invariant is indeed an invariant for elliptic curve, it does not dependent on the choices of Weierstrass equations. Moreover, j-invariant completely characterize the elliptic curve:

Theorem 1.5. *Let k be a field.*

1. *Two elliptic curves are isomorphic over $\overline{k}$ if and only if they have same j-invariant.*
2. *Let $j_0 \in \overline{k}$. There exists an elliptic curve defined over $k(j_0)$ whose j-invariant is equal to j_0.*

Let E be an elliptic curve over L, $\sigma \in \mathrm{Aut}(L)$. Define E^σ by fiber product:

$$\begin{tikzcd}
E & E^\sigma \arrow[l] \arrow[d] \\
\mathrm{Spec}(L) \arrow[from=u] & \mathrm{Spec}(L) \arrow[l, "\sigma^*"']
\end{tikzcd}$$

E^σ is also an elliptic curve. If E is defined by equation $y^2 = x^3 + ax + b$, then E^σ is defined by equation $y^2 = x^3 + \sigma(a)x + \sigma(b)$. Thus, the j-invariant satisfies

$$j(E^\sigma) = \sigma(j(E))$$

If E_1, E_2 are defined over L, $\phi : E_1 \to E_2$. Then $\sigma \in \mathrm{Aut}(L)$ induces a morphism $\phi^\sigma : E_1^\sigma \to E_2^\sigma$.

Let k be a subfield of L. We say E/L is an elliptic curve defined over k if there exist an elliptic curve E_k over k, such that $E = E_k \times_k \mathrm{Spec}\ L$. Base change doesn't change the defining equation of elliptic curve. Thus, the j-invariant of elliptic curves doesn't change under the base change. Together with Theorem 1.5, we have the following lemma:

Lemma 1.6. *Let E be an elliptic curve defined over $\overline{k}$, then E is defined over $k(j(E))$*

Let $\Lambda \subset \mathbb{C}$ be a lattice, that is, Λ is a discrete subgroup of $\mathbb{C}$ that contains an $\mathbb{R}$-basis for $\mathbb{C}$. Assume ω_1, ω_2 is a $\mathbb{Z}$-basis for Λ such that $Im(\frac{\omega_2}{\omega_1}) > 0$. The quotient group $\mathbb{C}/\Lambda$ is a compact riemann surface of genus one. The meromorphic functions on $\mathbb{C}/\Lambda$ are equivalent to a meromorphic functions on $\mathbb{C}$ with double periods ω_1 and ω_2.

Definition 1.7. *The Weierstrass $\wp$-function relative to Λ is defined by the series:*

$$\wp(z, \Lambda) = \frac{1}{z^2} + \sum_{\omega \in \Lambda, \omega \neq 0} \left(\frac{1}{(z-w)^2} - \frac{1}{\omega^2} \right)$$

Theorem 1.8. *Let Λ be a lattice.*

1. $\wp'(z)^2 = 4\wp(z)^3 - g_2(\Lambda)\wp(z) - g_3(\Lambda)$ *and* $\Delta(\Lambda) = g_2(\Lambda)^3 - 27g_3(\Lambda)^2 \neq 0$.
2. *The set of meomorphic functions on $\mathbb{C}/\Lambda$ is*

$$\mathbb{C}(\wp, \wp') \cong \mathrm{Frac}(C[x, y]/(y^2 - 4x^3 - g_2x - g_3))$$

Theorem 1.9. *Let Λ be a lattice, $g_2 = g_2(\Lambda), g_3 = g_3(\Lambda)$. Let E be the elliptic curve defined by $y^2 = 4x^3 - g_2x - g_3$. Then the map:*

$$\Phi : \mathbb{C}/\Lambda \longrightarrow E(\mathbb{C}) \qquad z \longmapsto [\wp(z) : \wp'(z) : 1]$$

is a complex analytic isomorphism of complex Lie groups, i.e., it is an isomorphism of Riemann surfaces that is also a group homomorphism.

Theorem 1.10. *1. For any $A, B \in \mathbb{C}$, $A^3 - 27B^2 \neq 0$, there exist q unique Λ, such that $g_2(\Lambda) = A$, $g_3(\Lambda) = B$.*

2. Let $E/\mathbb{C}$ be an elliptic curve. There exist a lattice Λ, unique up to homothety (multiplication by complex numbers), and a complex analytic isomorphism

$$\Phi : \mathbb{C}/\Lambda \longrightarrow E(\mathbb{C}) \qquad z \longmapsto [\wp(z, \Lambda) : \wp'(z, \Lambda) : 1]$$

Let Λ_1 and Λ_2 be lattices in $\mathbb{C}$, and suppose that $\alpha \in \mathbb{C}$ satisfies $\alpha\Lambda_1 \subset \Lambda_2$. Then scalar multiplication by α induces a well-defined holomorphic homomorphism $\phi_\alpha : \mathbb{C}/\Lambda_1 \longrightarrow \mathbb{C}/\Lambda_2$, $\phi_\alpha(z) = \alpha \cdot z \mod \Lambda_2$. In fact, these are essentially the only holomorphic maps from $\mathbb{C}/\Lambda_1$ to $\mathbb{C}/\Lambda_2$.

Theorem 1.11. *Let Λ_1 and Λ_2 be lattices in $\mathbb{C}$, $\phi : \mathbb{C}/\Lambda_1 \longrightarrow \mathbb{C}/\Lambda_2$ is a holomorphic map with $\phi(0) = 0$, then there exists $\alpha \in \mathbb{C}$ such that $\alpha\Lambda_1 \subset \Lambda_2$ and $\phi(z) = \alpha \cdot z \mod \Lambda_2$. Moreover, ϕ is an isomorphism if and only if $\alpha \cdot \Lambda_1 = \Lambda_2$*

Theorem 1.12. *The following categories are equivalent:*

1. *Objects: Elliptic curves over C. Maps: Isogenies.*

2. *Objects: Lattices $\Lambda \subset \mathbb{C}$, up to homothety. Maps: $Hom(\Lambda_1, \Lambda_2) = \alpha \in \mathbb{C} : \alpha \cdot \Lambda_1 \subset \Lambda_2$.*

2 Complex multiplication over $\mathbb{C}$

2.1 Definition of complex multiplication

Let $E/\mathbb{C}$ be an elliptic curve. Denote End(E) as the ring of isogenies from E to itself. The Theorem 1.12 allow us to identify End(E) with certain subring of $\mathbb{C}$. For example, Let Λ be a lattice associated to E, $\mathrm{End}(\Lambda) = \{\alpha \in \mathbb{C} : \alpha\Lambda \subset \Lambda\}$, then $\mathrm{End}(E) \cong \mathrm{End}(\Lambda)$ can identify $\mathrm{End}(E)$ as a subring of $\mathbb{C}$. If Λ' is another lattice associated to E, then there exists $\beta \in \mathbb{C}$ such that $\beta\Lambda = \Lambda'$. So $\mathrm{End}(\Lambda') = \{\alpha \in \mathbb{C} : \alpha\Lambda' \subset \Lambda'\} = \{\alpha \in \mathbb{C} : \alpha\beta\Lambda \subset \beta\Lambda\} = \mathrm{End}(\Lambda)$. Therefore, the identification above is well-defined.

Definition 2.1. *Let K be a number field. An order R of K is a subring of K that is finitely generated $\mathbb{Z}$-module and satisfies $R \otimes \mathbb{Q} = K$.*

Theorem 2.2. *Let $E/\mathbb{C}$ be an elliptic curve with an associated lattice Λ. Let w_1, w_2 be the generators of Λ. Then, one of the following is true:*

1. *$End(E) = \mathbb{Z}$*

2. *The field $K = \mathbb{Q}(\frac{w_2}{w_1})$ is an imaginary quadratic extension of $\mathbb{Q}$, and $End(E)$ is isomorphic to an order in K.*

Proof. Without loss of generality, we can assume that Λ is generated by 1 and τ. Let $R = \{\alpha \in \mathbb{C} : \alpha\Lambda \subset \Lambda\}$. Then, for any $\alpha \in R$, there are integers a, b, c, d, such that

$$\alpha = a + b\tau \qquad \alpha\tau = c + d\tau$$

Eliminating τ from these equations yields

$$\alpha^2 - (a + d)\alpha + ad - bc = 0$$

Thus, R is an integral extension of $\mathbb{Z}$.

Now suppose that $R \neq \mathbb{Z}$ and choose some $\alpha \in R \setminus \mathbb{Z}$. Then, with notation as above, we have $b \neq 0$, so eliminating α gives a nontrivial equation

$$b\tau^2 + (a-d)\tau - c = 0$$

It follows that $\mathbb{Q}(\tau)$ is an imaginary quadratic extension of $\mathbb{Q}$ ($\tau \notin \mathbb{R}$). Finally, since $R \subset \mathbb{Q}(\tau)$ and R is integral over $\mathbb{Z}$, it follows that R is an order in $\mathbb{Q}(\tau)$. □

Definition 2.3. *Let $E/\mathbb{C}$ be an elliptic curve. If $End(E) = R \subset \mathbb{C}$ and $K = R \otimes \mathbb{Q}$, then E is said to have complex multiplication by R.*

In this paper, we are primarily interested in elliptic curve E with a complex multiplication by $\mathcal{O}_K$, where $\mathcal{O}_K$ is the ring of integer of a quadratic imaginary field K. Notice that if we only consider the Z-algebra structure of $\mathrm{End}(E)$, there are two ways to embed the $\mathrm{End}(E)$ into $\mathbb{C}$ (or K), which are conjugated to each other by a Galois action. We need to pin down one of these embedding. We hope that with our choice of isomorphism $\mathrm{End}(E) \cong \mathcal{O}_K$, the isogeny $[\alpha] : E \longrightarrow E$, $\alpha \in \mathcal{O}_K$, should be just multiplication by α, when consider it as an endomorphism of $\mathbb{C}/\Lambda$. The following proposition describes this property in a coordinate independent way:

Proposition 2.4. *Let $E/\mathbb{C}$ be an elliptic curve with complex multiplication by R. There is a unique isomorphism $[\cdot] : R \longrightarrow End(E)$ such that for any invariant differential $\omega \in \Omega_E$ and $\alpha \in R$*

$$[\alpha]^*\omega = \alpha\Omega$$

In order to understand particular type of elliptic curves, it's often useful to study the set of all elliptic curves of this kind. Therefore, we should look at the set of all elliptic curves with same complex multiplication ring.

$$\mathcal{ELL}(R) = \{\text{elliptic curve } E/\mathbb{C} \text{ with } \mathrm{End}(E) = R\}$$

Now we start with a quadratic imaginary field K. Let $\mathfrak{a}$ be a fractional ideal of K. $\mathfrak{a}$ is a free $\mathbb{Z}$-module of rank 2. Thus $\mathfrak{a} \subset K \subset \mathbb{C}$ is a lattice. Denote $E_\mathfrak{a}$ as the elliptic curve associated with lattices $\mathfrak{a}$. $\mathrm{End}(E_\mathfrak{a}) \cong \{\alpha \in \mathbb{C} : \alpha\mathfrak{a} \subset \mathfrak{a}\} = \mathcal{O}_K$. Thus, $E_\mathfrak{a}$ is an elliptic curve with complex multiplication by $\mathcal{O}_K$.

On the other hand, Let $\alpha \in K$, $\alpha\mathfrak{a}$ and $\mathfrak{a}$ are homothetic, which give the same elliptic curve in $\mathcal{ELL}(\mathcal{O}_K)$. Thus, there is a well-defined map from the class group of $\mathcal{O}_K$ to $\mathcal{ELL}(\mathcal{O}_K)$, given by

$$\mathcal{CL}(\mathcal{O}_K) \longrightarrow \mathcal{ELL}(\mathcal{O}_K) \qquad \overline{\mathfrak{a}} \longmapsto E_\mathfrak{a}$$

Proposition 2.5. *Let Λ be a lattice with $E_\Lambda \in \mathcal{ELL}(\mathcal{O}_K)$, and let $\mathfrak{a}$ and $\mathfrak{b}$ be non-zero fractional ideals of K.*

1. *$\mathfrak{a}\Lambda$ is a lattice in $\mathbb{C}$.*

2. *The elliptic curve $E_{\mathfrak{a}\Lambda}$ satisfies $End(E_{\mathfrak{a}\Lambda}) \cong \mathcal{O}_K$.*

3. *$E_{\mathfrak{a}\Lambda} \cong E_{\mathfrak{b}\Lambda}$ if and only if $\overline{\mathfrak{a}} = \overline{\mathfrak{b}}$ in $\mathcal{CL}(\mathcal{O}_K)$.*

Proof. See [1] Proposition 1.2. □

We define an action of $\mathcal{CL}(\mathcal{O}_K)$ on $\mathcal{ELL}(\mathcal{O}_K)$determined by

$$\overline{\mathfrak{a}} * E_\Lambda = E_{\mathfrak{a}^{-1}\Lambda}$$

Proposition 2.5 shows that this group action is well-defined. Moreover, $\mathcal{ELL}(\mathcal{O}_K)$ is a $\mathcal{CL}(\mathcal{O}_K)$-torsor.

Corollary 2.6. *$\mathcal{ELL}(\mathcal{O}_K)$ is a finite set, $|\mathcal{ELL}(\mathcal{O}_K)| = |\mathcal{CL}(\mathcal{O}_K)|$.*

For elliptic curve with complex multiplication by $\mathcal{O}_K$, we can generalize the definition of torsion point.

Definition 2.7. *Let $(E/\mathbb{C}, e)$ be an elliptic curve with complex multiplicationby $\mathcal{O}_K$. $\mathfrak{a}$ is an ideal of $\mathcal{O}_K$, define the $\mathfrak{a}$-torsion points to be*

$$E[\mathfrak{a}] = \{P \in E : [\alpha]P = e, \forall \alpha \in \mathfrak{a}\}$$

Specially, for $\alpha \in \mathcal{O}_K$, $E[\alpha] = ker[\alpha] = \{P \in E : [\alpha]P = e\}$.

If $\mathfrak{a}$ is an ideal of $\mathcal{O}_K$, then $\Lambda \subset \mathfrak{a}^{-1}\Lambda$, there is a natural homomorphism $\mathbb{C}/\Lambda \longrightarrow \mathbb{C}/\mathfrak{a}^{-1}\Lambda$. This induces an isogeny $E_\Lambda \longrightarrow \overline{\mathfrak{a}} * E_\Lambda$.

Proposition 2.8. *Let $E \in \mathcal{ELL}(\mathcal{O}_K)$, and Let $\mathfrak{a}$ be an ideal of $\mathcal{O}_K$.*

1. *$E[\mathfrak{a}]$ is the kernel of the natural map $E_\Lambda \longrightarrow \overline{\mathfrak{a}} * E_\Lambda$*
2. *$E[\mathfrak{a}]$ is a free $\mathcal{O}_K/\mathfrak{a}$-module of rank 1.*
3. *the natural map $E_\Lambda \longrightarrow \overline{\mathfrak{a}} * E_\Lambda$ has degree $N^K_{\mathbb{Q}}\mathfrak{a}$.*

Proof. See [1] Proposition 1.4. □

2.2 Rationality questions

In this section we will study the field of definition for complex multiplication elliptic curves and their endomorphisms.

Proposition 2.9. *(a) Let $E/\mathbb{C}$ be an elliptic curve, and $\sigma \in Aut(\mathbb{C})$. Then*

$$End(E^\sigma) \cong End(E)$$

(b) Let $E/\mathbb{C}$ be an elliptic curve with complex multiplication by $\mathcal{O}_K$ Then $j(E) \in \overline{\mathbb{Q}}$.

(c)

$$\mathcal{ELL}(\mathcal{O}_K) \cong \left\{\text{elliptic curves } E/\overline{\mathbb{Q}} \text{ with } End(E) \cong \mathcal{O}_K\right\} / \text{isomorphism over } \overline{\mathbb{Q}}$$

Proof. 1. This is clear.

2. We claim that the set $\{\sigma(j(E)) : \sigma \in \text{Aut}(\mathbb{C})\}$ is finite. Let $\sigma \in \text{Aut}(\mathbb{C})$. (a) implies that $\text{End}(E^\sigma) = \mathcal{O}_K$, thus $[E^\sigma] \in \mathcal{ELL}(\mathcal{O}_K)$. By Corollary 2.6, $\mathcal{ELL}(\mathcal{O}_K)$ is a finite set. Since isomorphism class of an elliptic curve is determined by its j-invariant, it follows that $\{j(E^\sigma) : \sigma \in \text{Aut}(\mathbb{C})\} = \{\sigma(j(E)) : \sigma \in \text{Aut}(\mathbb{C})\}$ is a finite set. Therefore, $[\mathbb{Q}(j(E)) : \mathbb{Q}]$ is finite, $j(E) \in \overline{\mathbb{Q}}$.

3. For any subfield F of $\mathbb{C}$, define

$$\mathcal{ELL}_F(\mathcal{O}_K) = \{\text{elliptic curves } E/F \text{ with } End(E) \cong \mathcal{O}_K\} \,/\text{isomorphism over } F$$

Fix an embedding $\overline{\mathbb{Q}} \subset \mathbb{C}$, there is a natural map

$$\epsilon : \mathcal{ELL}_{\overline{\mathbb{Q}}}(\mathcal{O}_K) \longrightarrow \mathcal{ELL}_{\mathbb{C}}(\mathcal{O}_K) \qquad [E] \longmapsto [E \times_{\overline{\mathbb{Q}}} \mathrm{Spec}(\mathbb{C})]$$

For any $[E] \in \mathcal{ELL}_{\mathbb{C}}(\mathcal{O}_K)$, $j(E) \in \overline{\mathbb{Q}}$. By Theorem 1.5, there exists a elliptic curve $E'/\overline{\mathbb{Q}}$, such that $j(E') = j(E)$. Then $\epsilon(E')$ has same j-invariant with E. By Theorem 1.5, $\epsilon(E')$ is isomorphic to E over $\mathbb{C}$. Thus ϵ is surjective. Suppose $\epsilon([E]) = \epsilon([E'])$, then $j(E') = j(E)$. Since $\overline{\mathbb{Q}}$ is algebraically closed, by Theorem 1.5, E and E' are isomorphic over $\overline{\mathbb{Q}}$. Thus ϵ is injective. Therefore, ϵ is a bijection.

□

Next we study the effect that field automorphism have on the isogeny $[\alpha] : E \longrightarrow E$.

Theorem 2.10. *1. Let $E/\mathbb{C}$ be an elliptic curve with complex multiplication by $R \subset \mathbb{C}$. Then*

$$[\alpha]_E^\sigma = [\sigma(\alpha)]_{E^\sigma} \qquad \textit{for all } \alpha \in R \textit{ and all } \sigma \in Aut(\mathbb{C})$$

2. Let E be an elliptic curve defined over $L \subset \mathbb{C}$ and with complex multiplication by $\mathcal{O}_K$. Then every endomorphism of E is defined over the composition LK.

Proof. 1. Let $\omega \in \Omega_E$ be a non-zero invariant differential on E. To figure out $[\alpha]_E^\sigma$ corresponds to complex multiplication by which complex number, We only need to compute the pull back of $\tilde{\sigma}^*\omega \in \Omega_{E^\sigma}$ by $[\alpha]_E^\sigma$.

$$\begin{tikzcd}
E \arrow[r, "{[\alpha]}"] & E \\
E^\sigma \arrow[u, "\tilde{\sigma}"] \arrow[r, "{[\alpha]^\sigma}"] & E^\sigma \arrow[u, "\tilde{\sigma}"]
\end{tikzcd}$$

$$([\alpha]_E^\sigma)^*(\tilde{\sigma}^*\omega) = (\tilde{\sigma} \circ [\alpha]_E^\sigma)^*\omega = ([\alpha] \circ \tilde{\sigma})^*\omega = \tilde{\sigma}^*([\alpha]^*\omega) = \tilde{\sigma}^*(\alpha\omega) = \sigma(\alpha)\tilde{\sigma}^*\omega$$

Thus, $[\alpha]_E^\sigma = [\sigma(\alpha)]_{E^\sigma}$ (Here we use the fact that $\mathrm{End}(E) \longrightarrow \mathrm{End}(\Omega_E)$ is injective).

2. Let $\sigma \in \mathrm{Aut}(\mathbb{C}/LK)$, then $\sigma(\alpha) = \alpha$, for $\alpha \in (O)_K$. Thus, $[\alpha]_E^\sigma = [\sigma(\alpha)]_E = [\alpha]_E$. Hence, $[\alpha]$ is defined over LK.

□

Suppose the elliptic curve (E, e) is defined over $\overline{\mathbb{Q}}$ by the equation $y^2 = x^3 + ax + b$, then we can identify $E[m]$ as a subset of $E(\overline{\mathbb{Q}}) = \{(x, y) \in \overline{\mathbb{Q}}^2 : y^2 = x^3 + ax + b\} \cup \{e\}$

Theorem 2.11. *Let (E, e) be an elliptic curve over $\mathbb{C}$ with complex multiplication by $\mathcal{O}_K$, and let*

$$L = K(j(E), E_{tors})$$

be the field generated by the j-invariant of E and the coordinates of all of the torsion points of E. The L is an abelian extension of $K(j(E))$.

Proof. Denote $H = K(j(E))$, then the elliptic curve E and all endomorphisms of E are defined over H. Let $L_m = H(E[m])$ be the extension of H generated by the coordinates of m-torsion points of E. Since L is the composition of all L_m, it suffices to show that L_m is an abelian extension of H.

The Galois group $\mathrm{Gal}(\overline{K}/H)$ acts on $E[m]$ gives a representation

$$\rho : \mathrm{Gal}(\overline{K}/H) \longrightarrow \mathrm{Aut}(E[m]) \qquad \sigma \longmapsto \tilde{\sigma}|_{E[m]}$$

This action factors through $\mathrm{Gal}(L_m/H)$. Thus, we get a monomorphism of groups

$$\tilde{\rho} : \mathrm{Gal}(L_m/H) \longrightarrow \mathrm{Aut}(E[m])$$

So, the $\mathrm{Gal}(L_m/H)$ is a subgroup of $\mathrm{Aut}(E[m]) = \mathrm{GL}_2(\mathbb{Z}/m\mathbb{Z})$.

On the other hand, all the endomorphisms of E are defined over H. Hence, for any $\alpha \in \mathcal{O}_K$ and $\sigma \in \mathrm{Gal}(\overline{K}/H)$,

$$[\alpha] \circ \tilde{\sigma} = \tilde{\sigma} \circ [\alpha]$$

By Proposition 2.8, $E[m]$ is an $\mathcal{O}_K/m\mathcal{O}_K$-module with action of $\alpha \in \mathcal{O}_K$ given by $[\alpha]$. Thus, $\tilde{\sigma}$ is a $\mathcal{O}_K/m\mathcal{O}_K$-module isomorphism, the image of $\tilde{\rho}$ lies in $\mathrm{Aut}_{\mathcal{O}_K/m\mathcal{O}_K}(E[m])$. Besides, $E[m] \cong \mathcal{O}_K/m\mathcal{O}_K$. Thus, $\mathrm{Aut}_{\mathcal{O}_K/m\mathcal{O}_K}(E[m]) = \mathrm{Aut}_{\mathcal{O}_K/m\mathcal{O}_K}(\mathcal{O}_K/m\mathcal{O}_K) = (\mathcal{O}_K/m\mathcal{O}_K)^\times$ is an abelian group. Therefore, $\mathrm{Gal}(L_m/H)$ is abelian. □

Now we consider the natural action of $\mathrm{Gal}(\overline{K}/K)$ on $\mathcal{ELL}(\mathcal{O}_K)$ defined by

$$\forall \sigma \in \mathrm{Gal}(\overline{K}/K), \quad \sigma([E]) = [E^\sigma]$$

We have proved that the action of $\mathcal{CL}(\mathcal{O}_K)$ on $\mathcal{ELL}(\mathcal{O}_K)$ is simply transitive. Thus, for each class $[E] \in \mathcal{ELL}(\mathcal{O}_K)$, $\sigma \in \mathrm{Gal}(\overline{K}/K)$, there exists a unique $\bar{\mathfrak{a}} \in \mathcal{CL}(\mathcal{O}_K)$, such that $\sigma([E]) = [E^\sigma] = \bar{\mathfrak{a}} * [E]$. In fact, this element $\bar{\mathfrak{a}}$ turns out to be independent of $[E]$. Thus, there is a well-defined group homomorphism $\mathrm{Gal}(\overline{K}/K) \longrightarrow \mathcal{CL}(\mathcal{O}_K)$.

Proposition 2.12. *Let $K/\mathbb{Q}$ be a quadratic imaginary field. There exists a homomorphism*

$$F : \mathit{Gal}(\overline{K}/K) \longrightarrow \mathcal{CL}(\mathcal{O}_K)$$

uniquely characterized by the condition

$$E^\sigma = F(\sigma) * E \qquad \textit{for all } \sigma \in \mathit{Gal}(\overline{K}/K) \textit{ and all } E \in \mathcal{ELL}(\mathcal{O}_K)$$

We have explained above that for each $E \in \mathcal{ELL}(\mathcal{O}_K)$, there is a map

$$F_E : \mathrm{Gal}(\overline{K}/K) \longrightarrow \mathcal{CL}(\mathcal{O}_K)$$

such that $E^\sigma = F(\sigma) * E$ for all $\sigma \in \mathrm{Gal}(\overline{K}/K)$. It's easy to check that F is a group homomorphism

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

Note that $\mathcal{CL}(O_K)$ is an abelian group.

Thus, we only need to prove that this map is independent of $E \in \mathcal{ELL}(\mathcal{O}_K)$. Let $E_1, E_2 \in \mathcal{ELL}(\mathcal{O}_K)$, and $E_2 = \bar{\mathfrak{b}} * E_1$. Let $\sigma \in \mathrm{Gal}(\overline{K}/K)$, and $F_{E_1}(\sigma) = \bar{\mathfrak{a}}_1$, $F_{E_2}(\sigma) = \bar{\mathfrak{a}}_2$. We need to show that $\bar{\mathfrak{a}}_1 = \bar{\mathfrak{a}}_2$. Notice that

$$(\bar{\mathfrak{b}} * E_1)^\sigma = E_2^\sigma = \bar{\mathfrak{a}}_2 * E_2 = \bar{\mathfrak{a}}_2 * (\bar{\mathfrak{b}} * E) = \bar{\mathfrak{a}}_2\bar{\mathfrak{b}}\bar{\mathfrak{a}}_1^{-1} * E_1^\sigma$$

If we can show that $(\bar{\mathfrak{b}} * E_1)^\sigma = \bar{\mathfrak{b}} * E_1^\sigma$, then $\bar{\mathfrak{b}} = \bar{\mathfrak{a}}_2\bar{\mathfrak{b}}\bar{\mathfrak{a}}_1^{-1}$ gives us $\bar{\mathfrak{a}}_1 = \bar{\mathfrak{a}}_2$.

Proposition 2.13. *Let $E/\overline{\mathbb{Q}}$ be an elliptic curve representing an element of $\mathcal{ELL}(\mathcal{O}_K)$, let $\overline{\mathfrak{a}} \in \mathcal{CL}(\mathcal{O}_K)$, and let $\sigma \in Gal(\overline{\mathbb{Q}}/\mathbb{Q})$. Then*

$$(\overline{\mathfrak{a}} * E)^\sigma = \sigma(\overline{\mathfrak{a}}) * E^\sigma$$

Proof. See [1] Proposition 2.5. □

3 Class field theory

Let K be a number field, and let I_K be the group of fractional ideals in K. For a finite set S of primes in K, we define I_K^S to be the subgroup of I_K generated by primes not in S.

Definition 3.1. *A modulus for K is a function*

$$m : \textit{primes of } K \longrightarrow \mathbb{Z}$$

such that

1. *$m(\mathfrak{p}) \geq 0$ for all primes $\mathfrak{p}$, and $m(\mathfrak{p}) = 0$ for all but finite many $\mathfrak{p}$;*

2. *if $\mathfrak{p}$ is real, then $m(\mathfrak{p}) = 0$ or 1.*

3. *if $\mathfrak{p}$ is complex, then $M(\mathfrak{p}) = 0$.*

Traditionally, one writes

$$m = \prod_{\mathfrak{p}} \mathfrak{p}^{m(\mathfrak{p})}$$

For a modulus m, denote $K_{m,1}$ to be the set of $a \in K^\times$ such that

$$\begin{cases} ord_{\mathfrak{p}}(a-1) \geq m(\mathfrak{p}) & \text{all finite } \mathfrak{p} \text{ dividing } m \\ a_{\mathfrak{p}} > 0 & \text{all real } \mathfrak{p} \text{ dividing } m \end{cases}$$

For a modulus m, denote $S(m) = \{\text{primes dividing } m\}$. It's easy to see that there exists an injection $i : K_{m,1}^\times \longrightarrow I_K^{S(m)}$. The quotient

$$\mathcal{CL}_m = I_K^{S(m)}/i(K_{m,1})$$

is called the ray class group modulo m.

Let L/K be an abelian extension. $\mathfrak{P}$ is a prime ideal in $\mathcal{O}_L$ that is unramified over a prime ideal $\mathfrak{p}$ in $\mathcal{O}_K$. The Frobenius element

$$\left(\frac{L/K}{\mathfrak{p}}\right)$$

is defined to be the unique element $\sigma \in \mathrm{Gal}(L/K)$ satisfying the following condition:

1. $\sigma(\mathfrak{P}) = \mathfrak{P}$

2. for all $\alpha \in \mathcal{O}_L$, $\sigma(\alpha) \equiv \alpha^q \mod \mathfrak{P}$, where q is the number of elements in $\mathcal{O}_K/\mathfrak{p}$.

For every finite set S of primes of K containing all primes that ramify in L, we have a homomorphism

$$\psi_{L/K} : I_K^S \longrightarrow \mathrm{Gal}(L/K) \qquad \mathfrak{a} = \mathfrak{p}_1^{n_1} \cdots \mathfrak{p}_t^{n_t} \longmapsto \left(\frac{L/K}{\mathfrak{a}}\right) = \prod_{i=1}^{t} \left(\frac{L/K}{\mathfrak{p}_i}\right)^{n_i}$$

called the global Artin map.

We say that a homomorphism $\psi : I_K^S \longrightarrow G$ admits a modulus if there exists a modulus m with $S(m)$ containing S such that $\psi(i(K_{m,1})) = 0$. Thus, ψ admits a modulus if and only if it factors through C_m for some m with $S(m) \supset S$. Now we state the main theorem of Class Field Theory.

Theorem 3.2. *Let L be a finite abelian extension of K, and let S be the set of primes of K ramifying in L. Then the Artin map $\psi : I^S \longrightarrow Gal(L/K)$ admits a modulus m with $S(m) = S$, and it defines an isomorphism*

$$I_K^{S(m)}/i(K_{m,1}) \cdot Nm(I_L^{S(m)}) \longrightarrow Gal(L/K)$$

We call a subgroup H of $I_K^{S(m)}$ a congruence subgroup modulus m if

$$I_K^{S(m)} \supset H \supset i(K_{m,1})$$

Theorem 3.3. *For every congruence subgroup H modulus m, there exists a finite abelian extension L/K, unramified at the primes not dividing m such that $H = i(K_{m,1}) \cdot Nm(I_L^{S(m)})$*

In particular, for each modulus m, there is a field, called the ray class field modulo m, such that the Artin map defines an isomorphism $C_m \longrightarrow \mathrm{Gal}(L_m/K)$.

Let L/K be an abelian extension with Galois group G, The Reciprocity Law tells us that there exists a modulus m, such that the Artin map $\psi_{L/K}$ factors through $C_m \longrightarrow G$.

Theorem 3.4. *There is a modulus $\mathfrak{f}$, called the conductor of L/K, such that the Artin map $\psi_{L/K}$ factors through $C_{\mathfrak{f}}$, and for any modulus m such that $\psi_{L/K}$ factors through C_m, we have $\mathfrak{f}|m$.*

Now, we take $m = 1$, means that $m(\mathfrak{p}) = 0$ for all prime $\mathfrak{p}$. Denote the ray class field modulo $m = 1$ by H, then H/K is an unramified abelian extension. If H' is another unramified abelian extension, then the Artin map $\psi_{H'/K}$ must factors through C_m. By class field theory, H' is a subfield of H. Therefore, H is a maximal unramified abelian extension of K.

Definition 3.5. *Let K be a number field. The Hilbert class field of K is the maximal unramified abelian extension of K.*

So we have used the class field theory to prove the existence of Hilbert class field for any number field. Note that the ray class group for $m = 1$ is just the class group of $\mathcal{O}_K$, thus

Proposition 3.6. *Let K be a number field, H be the Hilbert class field of K. Then the Artin map $\mathcal{CL}(\mathcal{O}_K) \longrightarrow Gal(H/K)$ is an isomorphism.*

We will need the following version of Dirichlet theorem:

Theorem 3.7. *Let K be a number field and m is a modulus. Then every ideal class in $\mathcal{CL}_m$ contains infinitely many degree 1 primes of K.*

4 Hilbert class fields of imaginary quadratic fields

The goal of this section is to prove the following theorem:

Theorem 4.1. *Let $K/\mathbb{Q}$ be a quadratic imaginary field, and let $E/\mathbb{C}$ be an elliptic curve with complex multiplication by $\mathcal{O}_K$. Then $K(j(E))$ is the Hilbert class field H of K.*

We will actually prove much more then this theorem. We can given an explicit description of how the Galois group $\mathrm{Gal}(H/K)$ acts on $\mathcal{ELL}(\mathcal{O}_K)$. Recall that the action of $\mathrm{Gal}(\overline{K}/K)$ factors through the action of class group $\mathcal{CL}(\mathcal{O}_K)$ by the map

$$F : \mathrm{Gal}(\overline{K}/K) \longrightarrow \mathcal{CL}(\mathcal{O}_K)$$

Since $\mathcal{CL}(\mathcal{O}_K)$ is abelian, this map factors through

$$F : \mathrm{Gal}(K^{ab}/K) \longrightarrow \mathcal{CL}(\mathcal{O}_K)$$

The following proposition, together with with results from class field theory, will completely determine F.

Proposition 4.2. *There is a finite set S of rational primes such that if $p \notin S$ is a prime which splits in K, says as $p\mathcal{O}_K = \mathfrak{p}\mathfrak{p}'$, and $\sigma_p \in$ Gal(K^{ab}/K) is the Frobenius element corresponding to p, then*

$$F(\sigma_p) = \overline{\mathfrak{p}} \in \mathcal{CL}(\mathcal{O}_K)$$

Proof. We know that $\mathcal{ELL}(\mathcal{O}_K)$ is finite and every elliptic curve in $\mathcal{ELL}(\mathcal{O}_K)$ is defined over $\overline{\mathbb{Q}}$. Choose a finite extension L/K and representatives $E_1, ..., E_n$ of $\mathcal{ELL}(\mathcal{O}_K)$, such that $E_1, ..., E_n$ together with all isogenies between them are defined over L. Now Let S be the finite set of rational primes satisfying any of the following three conditions:

(i) p ramifies in L;

(ii) some E_i has bad reduction at some primes of L lying over p;

(iii) p divides either the numerator or the denominator of one of the number $\mathrm{N}^L_{\mathbb{Q}}(j(E_i) - j(E_j))$ for some $i \neq j$.

Notice that condition (iii) means that if $p \notin S$ and if $\mathfrak{P}$ is a prime of L dividing p, then $\tilde{E}_i$ is not isomorphic to $\tilde{E}_j$, under the reduction by $\mathfrak{P}$, since their j-invariant are not the same modulo $\mathfrak{P}$.

Now let $p \notin S$ be a prime which splits as $p\mathcal{O}_{\mathcal{K}} = \mathfrak{p}\mathfrak{p}'$ in $\mathcal{O}_{\mathcal{K}}$. Let Λ be a lattice associated to E. There exists an ideal $\mathfrak{a} \subset \mathcal{O}_{\mathcal{K}}$ relatively prime to p such that $\mathfrak{a}\mathfrak{p}$ is a principal ideal, say $\mathfrak{a}\mathfrak{p} = (\alpha)$ (For example, take $\alpha \in \mathfrak{p} \setminus \mathfrak{p}^2 \cup (p)$ and $(\alpha) = \mathfrak{p}\mathfrak{a}$). There are isogenies connecting $E, \overline{\mathfrak{p}} * E$, and $\overline{\mathfrak{a}} * \overline{\mathfrak{p}} * E$ corresponding to the natural analytic maps as indicated in the following diagram:

$$\begin{tikzcd}
\mathbb{C}/\Lambda \arrow[r, "z \mapsto z"] \arrow[d, "\sim"] & \mathbb{C}/\mathfrak{p}^{-1}\Lambda \arrow[r, "z \mapsto z"] \arrow[d, "\sim"] & \mathbb{C}/\mathfrak{a}^{-1}\mathfrak{p}^{-1}\Lambda = \mathbb{C}/\alpha^{-1}\Lambda \arrow[r, "z \mapsto \alpha z"] \arrow[d, "\sim"] & \mathbb{C}/\Lambda \arrow[d, "\sim"] \\
E \arrow[r, "\phi"] & \overline{\mathfrak{p}} * E \arrow[r, "\psi"] & \overline{\mathfrak{a}} * \overline{\mathfrak{p}} * E = (\alpha) * E \arrow[r, "\lambda"] & E
\end{tikzcd}$$

Let ω be an invariant differential on E such that $\widetilde{\omega}$ is a non-zero invariant differential on $\widetilde{E}$ with reduction modulo $\mathfrak{P}$. By tracing the diagram, we conclude that

$$(\lambda \circ \psi \circ \phi)^* \omega = \alpha\omega$$

Since $\mathfrak{p}|\alpha$, $\widetilde{\alpha} = 0 \mod \mathfrak{P}$. Thus, by modulo $\mathfrak{P}$, we have

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

This implies $\widetilde{\lambda} \circ \widetilde{\psi} \circ \widetilde{\phi}$ is inseparable. On the other hand, $\deg(\widetilde{\phi}) = \mathrm{N}^K_{\mathbb{Q}}(\mathfrak{p}) = p$, $\deg(\widetilde{\psi}) = \mathrm{N}^K_{\mathbb{Q}}(\mathfrak{a})$, $\deg(\widetilde{\lambda}) = 1$. Since $p \nmid \mathfrak{a}$, both $\widetilde{\psi}$ and $\widetilde{\lambda}$ are separable, so we conclude that

$$\widetilde{\phi} : \widetilde{E} \longrightarrow \widetilde{\overline{\mathfrak{p}} * E}$$

is an inseparable map with deg $= p$. Thus, there is an isomorphism between $\widetilde{E}^{(p)}$ and $\widetilde{\overline{\mathfrak{p}} * E}$. In particular, we find that

$$j(\widetilde{\overline{\mathfrak{p}} * E}) = j(\widetilde{E}^{(p)}) = j(\widetilde{E})^p$$

So

$$j(\overline{\mathfrak{p}} * E) \equiv j(E)^p \equiv \sigma_p(j(E)) = j(E^{\sigma_p}) = j(F(\sigma_p) * E) \mod \mathfrak{P}$$

As discussed above, the condition (iii) implies $\overline{\mathfrak{p}} * E \cong F(\sigma_p) * E$. □

Now we can prove our main theorem.

Theorem 4.3. *Let E be an elliptic curve with complex multiplication by $\mathcal{O}_K$. Then $K(j(E))$ is the Hilbert class field of K.*

Proof. Assume the kernel of map $F : \mathrm{Gal}(\overline{K}/K) \longrightarrow \mathcal{CL}(\mathcal{O}_K)$ is $\mathrm{Gal}(\overline{K}/L)$. Then

$$F : \mathrm{Gal}(L/K) \hookrightarrow \mathcal{CL}(\mathcal{O}_K)$$

$$\begin{aligned}
\mathrm{Gal}(\overline{K}/L) = & \ \ker F \\
&= \{\sigma \in \mathrm{Gal}(\overline{K}/K) : F(\sigma) * E = E\} \\
&= \{\sigma \in \mathrm{Gal}(\overline{K}/K) : E^\sigma = E\} \\
&= \{\sigma \in \mathrm{Gal}(\overline{K}/K) : j(E^\sigma) = j(E)\} \\
&= \{\sigma \in \mathrm{Gal}(\overline{K}/K) : \sigma(j(E)) = j(E)\} \\
&= \mathrm{Gal}(\overline{K}/K(j(E))).
\end{aligned}$$

Hence $L = K(j(E))$. Further, since F maps injectively into $\mathcal{CL}(\mathcal{O}_K)$, L/K is an abelian extension.

Let $\mathfrak{f}$ be the conductor of L/K, and consider the composition of the Artin map with F:

$$I_K^{S(\mathfrak{f})} \xrightarrow{\psi_{L/K}} \mathrm{Gal}(L/K) \xrightarrow{F} \mathcal{CL}(\mathcal{O}_K)$$

We claim that for all $\mathfrak{a} \in I_K^{S(\mathfrak{f})}$, $F(\psi_{L/K}(\mathfrak{a})) = \overline{\mathfrak{a}}$.

Let $\mathfrak{a} \in I_K^{S(\mathfrak{f})}$, and let S be the finite set of primes described in Proposition 4.2. By Dirichlet theorem, there exists a prime $\mathfrak{p}$ in the same class as $\mathfrak{a}$ in the ray class group modulo $\mathfrak{f}$, such that $\mathfrak{p}$ does not lie over a prime in S. Therefore, there is a $\alpha \in K^\times$ satisfying $\alpha \equiv 1 \mod \mathfrak{f}$ and $\mathfrak{a} = (\alpha)\mathfrak{p}$. By Proposition 4.2, $F\left(\frac{L/K}{\mathfrak{p}}\right) = \overline{\mathfrak{p}}$, thus

$$F\left(\frac{L/K}{\mathfrak{a}}\right) = F\left(\frac{L/K}{(\alpha)\mathfrak{p}}\right) = F\left(\frac{L/K}{\mathfrak{p}}\right) = \overline{\mathfrak{p}} = \overline{\mathfrak{a}}$$

In particular, for principal ideal $(\alpha) \in I_K^{S(\mathfrak{f})}$, $F\left(\frac{L/K}{(\alpha)}\right) = 1$. But the conductor of L/K is the smallest integral ideal $\mathfrak{b}$ with the property that

$$\alpha \equiv 1 \mod \mathfrak{b} \text{ implies } \left(\frac{L/K}{(\alpha)}\right) = 1$$

Thus, $\mathfrak{f} = 1$, L/K is an unramified extension. Therefore L is contained in the Hilbert class field H of K. On the other hand, the natural map $I_K^{S(\mathfrak{f})} \longrightarrow \mathcal{CL}(\mathcal{O}_K)$ is surjective. So $F : \mathrm{Gal}(L/K) \longrightarrow \mathcal{CL}(\mathcal{O}_K)$ is an isomorphism.

$$[L : K] = |\mathcal{CL}(\mathcal{O}_K)| = [H : K]$$

This implies $H = L = K(j(E))$. Therefore, $K(j(E))$ is the Hilbert class field of K.

□

References

[1] Joseph Silverman. Advanced Topics in the Arithmetic of Elliptic Curves. Publishedby Springer Science+Business Media New York, Inc. 1994.

[2] Joseph Silverman. The Arithmetic of Elliptic Curves. Publishedby Springer Science+Business Media, LLC. 2nd edition, 2009.

[3] James Milne, Class Field Theory. Online course notes.