CM Elliptic Curves and the Maximal Extension of an Imaginary Quadratic Field

Student: Xu Song
Supervisor: Emmanuel Lecouturier

Abstract

The theory of complex multiplication began with Kronecker's *Jugendtraum*, which aimed to construct abelian extensions of a number field by adjoining some special values of some special functions. Apart from $\mathbb{Q}$, this goal has only been fully achieved for imaginary quadratic fields.

In this paper, we will introduce the CM theory of elliptic curves and show how to use it to construct the maximal abelian extension of an imaginary quadratic field. In section 1, we briefly introduce some background of this problem and review the classical Kronecker-Weber Theorem. In section 2, we first introduce some basic notions of elliptic curves. Then we define the CM elliptic curves and prove some of their properties. In section 3, we prove the Hilbert class field of an imaginary quadratic field can be obtained by joining the $j-$invariant of an elliptic curve with CM by $\mathcal{O}_{\mathrm{K}}$. In section 4, we introduce the modular function and the modular equation and use them to prove the $j-$invariant of a CM elliptic is an algebraic integer. In section 5, we prove the maximal abelian extension of an imaginary quadratic field can be obtained by joining the $j-$invariant and the torsion points. Finally in section 6 we introduce the main theorem of complex multiplication and compare it with its $\mathbb{Q}-$analogue.

Contents

1 Kronecker's Jugendtraum

We first recall the famous Kronecker-Weber Theorem.

Theorem 1.1. *Every finite abelian extension of $\mathbb{Q}$ is contained in a cyclotomic extension.*

This theorem tells us the maximal abelian extension of $\mathbb{Q}$ can be obtained by joining all the roots of unity to $\mathbb{Q}$. We expect to do the same thing to a general number field K , that is, we want to obtain the maximal abelian extension of K by joining some special values. This is exactly Hilbert's 12th problem.

Besides $\mathbb{Q}$, this problem has only been fully solved for imaginary quadratic field, by applying the theory of CM elliptic curves. This is the main result of Kronecker's *Jugendtraum.*

2 Elliptic curves

In this section, we will introduce some basic facts about elliptic curves.

2.1 Weierstrass equation and j-invariant

We first give the definition of an elliptic curve.

Definition 2.1. *Let K be a field. An elliptic curve over K is a pair (E, O), where*
1. E is a projective curve over K of genus 1.
2. O is a K-rational point of E.

An isogeny between two elliptic curves $(E_1, O_1), (E_2, O_2)$ is a nonconstant algebraic map ϕ which sends O_1 to O_2. The elliptic curves over K together with isogenies form a category.

By Riemann-Roch theorem, an elliptic curve E over K can be embedded into $\mathbb{P}^2$ by the Weierstrass equation(for a proof, see[4], III.3.1):

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6, \quad a_i \in K, \ i = 1, 2, ..., 6$$

When $charK \neq 2, 3$, the Weierstrass equation can be simplified to be

$$y^2 = 4x^3 - g_2x - g_3, \quad g_2, g_3 \in K$$

Then one can define the j-invariant of E to be

$$j(E) = 1728\frac{g_2^3}{g_2^3 - 27g_3^2}$$

The key fact is that two elliptic curves $E/K, E'/K$ are isomorphic over $\bar{K}$ if and only if their j-invariants are equal. For a proof, see [4].1.4.

2.2 j-invariant of a lattice

For a lattice $\Lambda \subset \mathbb{C}$, one has the Weierstrass $\wp$-function

$$\wp(z; \Lambda) = \frac{1}{z^2} + \sum_{\omega \in \Lambda^*} \frac{1}{(z - \omega)^2} - \frac{1}{\omega^2}$$

Here $\Lambda^* = \Lambda - 0$. We also have the following functional equation:

$$\wp'^2(z) = 4\wp^3(z) - g_2\wp(z) - g_3$$

Here $g_2 = 60G_4, g_3 = 140G_6$, where

$$G_n = \sum_{\omega \in \Lambda^*} \frac{1}{\omega^n}, \qquad n = 3, 4, ...$$

are Eisenstein series. Then we can define the j-invariant of Λ to be

$$j(\Lambda) = 1728 \frac{g_2^3}{g_2^3 - 27g_3^2}.$$

2.3 Equivalence of three categories

In this part, we are going to briefly explain the following results. For a detailed proof, see [4] VI.4.1.

Theorem 2.2. *The following categories are equivalent.*

(1) Objects: elliptic curves over $\mathbb{C}$
Morphisms: Isogenies and the zero maps.

(2) Objects: compact Riemann surfaces of the form $\mathbb{C}/\Lambda$
Morphisms: holomorphic maps sending 0 to 0.

(3) Objects: lattices in $\mathbb{C}$
Morphisms: Hom(Λ_1, Λ_2)= $\{\alpha \in \mathbb{C} : \alpha\Lambda_1 \subset \Lambda_2\}$

Proof. For any lattice Λ, we associate it to the compact Riemann surface $\phi(\Lambda) := \mathbb{C}/\Lambda$. Let Λ_1, Λ_2 be two lattices. For any $\alpha \in \mathrm{Hom}(\Lambda_1, \Lambda_2)$, we can define the following map

$$\begin{aligned} \phi_\alpha : \mathbb{C}/\Lambda_1 &\longrightarrow \mathbb{C}/\Lambda_2 \\ z &\longmapsto \alpha z \end{aligned}$$

It is a holomorphic map sending 0 to 0. One can actually show that every holomorphic map from $\mathbb{C}/\Lambda_1$ to $\mathbb{C}/\Lambda_2$ must be of the form ϕ_α for some $\alpha \in \mathrm{Hom}(\Lambda_1, \Lambda_2)$. Then functor ϕ is an equivalence of the third category and the second category.

For any lattice Λ, one can define the elliptic curve E_Λ over $\mathbb{C}$ given by the following Weierstrass equation:

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

We associate the compact Riemann surface $\mathbb{C}/\Lambda$ to the elliptic curve $\mathcal{F}(\mathbb{C}/\Lambda) := E_\Lambda$. Let Λ_1, Λ_2 be two lattices. For any $\phi_\alpha \in \mathrm{Hom}(\mathbb{C}/\Lambda_1, \mathbb{C}/\Lambda_2)$, we define $\mathcal{F}(\phi_\alpha)$ to be the map such as the following diagram commutes:

$$\begin{tikzcd}
\mathbb{C}/\Lambda_1 \arrow[r, "f_1"] \arrow[d, "\phi_\alpha"] & E_{\Lambda_1} \arrow[d, "\mathcal{F}(\phi_\alpha)"] \\
\mathbb{C}/\Lambda_2 \arrow[r, "f_2"] & E_{\Lambda_2}
\end{tikzcd}$$

where

$$\begin{aligned} f_1 : \mathbb{C}/\Lambda_1 &\longrightarrow E_{\Lambda_1} \\ z &\longmapsto [\wp(z;\Lambda_1), \wp'(z;\Lambda_1), 1] \\ f_2 : \mathbb{C}/\Lambda_2 &\longrightarrow E_{\Lambda_2} \\ z &\longmapsto [\wp(z;\Lambda_2), \wp'(z;\Lambda_2), 1] \end{aligned}$$

One can actually show that the map $\mathcal{F}(\phi_\alpha)$ is an isogeny (or a zero map if $\alpha = 0$). On the other hand, every isogeny from E_{Λ_1} to E_{Λ_2} is a rational map in coordinates and therefore a holomorphic map if we view the elliptic curve as a complex manifold. Thus every isogeny(or zero map) is of the form $\mathcal{F}(\phi_\alpha)$. This proves $\mathcal{F}$ is an equivalence between the second category and the first category. □

2.4 CM elliptic curves

Definition 2.3. *Let $K \subset \mathbb{C}$ be a field. We say an elliptic curve E/K has complex multiplication(CM) if its ring of endomorphism over $\bar{K}$ is strictly larger than $\mathbb{Z}$.*

In the rest pages, the ring of endomorphism of an elliptic curve E/K means the ring of endomorphism over $\bar{K}$, and we denote it by $\mathrm{End}(E)$.

For an elliptic curve $E/\mathbb{C}$, it is isomorphic to some E_Λ for some lattice Λ. By the equivalence of those three categories proved in last section, we have

$$\mathrm{End}(E_\Lambda) \cong R := \{\alpha \in \mathbb{C} : \alpha\Lambda \subset \Lambda\}$$

When it comes to the case of complex multiplication, we have the following results:

Theorem 2.4. *If E_Λ is an elliptic curve over $\mathbb{C}$ with complex multiplication, then*
1. R is an order in an imaginary quadratic field.
2. Λ is homethetic to a proper fractional ideal of R.

Proof. The condition is equivalent to the existence of $\alpha \in \mathbb{C} - \mathbb{Z}$ such that $\alpha\Lambda \subset \Lambda$. Up to homethety, one may assume the lattice Λ is the free $\mathbb{Z}-$module spanned by 1 and some $\tau \in \mathbb{H}$, here $\mathbb{H}$ denotes the upper half plane of $\mathbb{C}$. Then

$$\alpha \cdot 1 = a + b\tau$$
$$\alpha \cdot \tau = c + d\tau$$

with some $a, b, c, d \in \mathbb{Z}$. Then we get the following equation:

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

b must be nonzero, otherwise $\alpha = a$ is an integer, contradiction. Since τ is not real, $K := \mathbb{Q}(\tau)$ is an imaginary quadratic field. Since $R \subset \mathbb{Z} + \mathbb{Z}\tau$, R is a finitely generated $\mathbb{Z}-$module. Note that $1, b\tau \in R$, then R must be a free $\mathbb{Z}-$module of rank 2. Therefore R is an order in K. Λ is naturally an $R-$module by the definition of R. Since Λ is a free $\mathbb{Z}-$module of rank 2, it is *fortiori* a finitely generated $R-$module. And also $\{\alpha \in K : \alpha\Lambda \subset \Lambda\} = R$. Therefore Λ is a proper fractional ideal of R. □

We also have the following theorem.

Theorem 2.5. *Let K be an imaginary quadratic field and R be an order of K. Then there is a bijection between*

$$\{E/\mathbb{C} : \mathrm{End}(E) \cong R\}/\{\textit{isomorphism over } \mathbb{C}\}$$

and

$$\{\textit{ideal class group } Cl(R) \textit{ of the order } R\}$$

Proof. See [1]10.20. □

Corollary 2.6. *Let K be an imaginary quadratic field. Let $E/\mathbb{C}$ be a CM elliptic curve with $\mathrm{End}(E) \cong R$, where R is an order in K. Then $j(E)$ is an algebraic number. Moreover, $[\mathbb{Q}(j(E)) : \mathbb{Q}] \leq \#Cl(R)$.*

Proof. Let $\sigma \in \mathrm{Aut}(\mathbb{C})$. Then we have $j(E^\sigma) = j(E)^\sigma$. Note that $\mathrm{End}(E^\sigma) \cong \mathrm{End}(E) \cong R$. So E^σ is also an elliptic over $\mathbb{C}$ with CM by R. By the theorem, the number of $\mathbb{C}-$isomorphism classes of elliptic curves over C with CM by R is equal to $\#Cl(R)$. Therefore when σ varies, $\sigma(j(E))$ takes not more than $\#Cl(R)$ values. This implies that $j(E)$ is an algebraic number and its degree over $\mathbb{Q}$ is not more than $\#Cl(R)$. □

Remark 2.7. *In fact,* $[\mathbb{Q}(j(E)) : \mathbb{Q}] = \#Cl(R)$ *, and* $j(E)$ *is an algebraic integer.*

Corollary 2.8.

$$\frac{\{\textit{elliptic curves } E \textit{ over } \mathbb{C} \textit{ with } \mathrm{End}(E) \cong R\}}{\{\textit{isomorphism over } \mathbb{C}\}}$$

is equivalent to

$$\frac{\{\textit{elliptic curves } E \textit{ over } \bar{\mathbb{Q}} \textit{ with } \mathrm{End}(E) \cong R\}}{\{\textit{isomorphism over } \bar{\mathbb{Q}}\}}$$

Proof. For any elliptic curve E over $\bar{\mathbb{Q}}$ with CM by R, one can always extend the scalar to $\mathbb{C}$ and get an elliptic curve E' over $\mathbb{C}$ with CM by R. For any elliptic curve E' over $\mathbb{C}$ with CM by R, by Corollary 2.6, $j(E') \in \bar{\mathbb{Q}}$. Since E' can find a Weierstrass equation with coefficients in $\mathbb{Q}(j(E'))$(See [4] III.1.4.), E' can be defined over $\bar{\mathbb{Q}}$. Let E_1, E_2 be two elliptic curves over $\bar{\mathbb{Q}}$ with CM by R. If E_1', E_2' are isomorphic over $\mathbb{C}$, then their $j-$invariants are equal. And thus they are isomorphic over $\bar{\mathbb{Q}}$(See [4]III.1.4). Therefore the correspondence $E \mapsto E'$ is bijective. □

Corollary 2.8 tells us, when it comes to isomorphism classes of CM elliptic curves, it doesn't matter whether one works over $\mathbb{C}$ or over $\bar{\mathbb{Q}}$.

2.5 Action by the absolute Galois group

In the rest pages, K is an imaginary quadratic field, $\mathcal{O}_\mathrm{K}$ is the ring of integer of K.

By Theorem 2.5, we can define the action of $Cl(\mathcal{O}_\mathrm{K})$ on the set of $\bar{\mathbb{Q}}-$isomorphism classes of elliptic curves with CM by $\mathcal{O}_\mathrm{K}$:

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

Here E_Λ represents the $\bar{\mathbb{Q}}-$isomorphism class with $j-$invariant equal to $j(E_\Lambda)$, $\mathfrak{a}$ is a fractional ideal of $\mathcal{O}_\mathrm{K}$ and $\bar{\mathfrak{a}}$ denotes its class in $Cl(\mathcal{O}_\mathrm{K})$. By Theorem 2.5, the action is free and transitive.

Let E be an elliptic curve over $\bar{\mathbb{Q}}$ with CM by $\mathcal{O}_\mathrm{K}$. For $\sigma \in \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$, we know E^σ is also CM by $\mathcal{O}_\mathrm{K}$. Thus there is a unique element $\bar{\mathfrak{a}} \in Cl(\mathcal{O}_\mathrm{K})$ such that

$$\bar{\mathfrak{a}} * E \cong E^\sigma$$

Then we get a map

$$F : \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}) \longrightarrow Cl(\mathcal{O}_\mathrm{K})$$

satisfying $F(\sigma) * E \cong E^\sigma$, for any $\sigma \in \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$. For any E over $\bar{\mathbb{Q}}$ with CM by $\mathcal{O}_\mathrm{K}$, one can define such a map. However, the restriction map

$$F : \mathrm{Gal}(\bar{K}/K) \longrightarrow Cl(\mathcal{O}_\mathrm{K})$$

does not depend on the choice of E (See [3]II.2.4). Moreover, since $Cl(\mathcal{O}_{\mathrm{K}})$ is an abelian group, F factors through $\mathrm{Gal}(\bar{K}/K)^{ab} \cong \mathrm{Gal}(K^{ab}/K)$:

$$F : \mathrm{Gal}(K^{ab}/K) \longmapsto Cl(\mathcal{O}_{\mathrm{K}})$$

3 The Hilbert class field of K

We have the following results.

Theorem 3.1. *Let $E/\mathbb{C}$ be an elliptic curve with* $\mathrm{End}(E) \cong \mathcal{O}_K$*.Then*
(a) $K(j(E))$ is the Hilbert class field H of K.
(b) $[K(j(E)) : K] = [\mathbb{Q}(j(E)) : \mathbb{Q}] = h := \#Cl(\mathcal{O}_K)$.
(c) Let $E_1, ..., E_h$ be a complete set of representatives for the isomorphism classes of elliptic curves E over $\mathbb{C}$ with $\mathrm{End}(E) \cong \mathcal{O}_K$*. Then $j(E_1), ..., j(E_h)$ is a complete set of* $\mathrm{Gal}(\bar{K}/K)$ *conjugates for $j(E)$.*
(d) Moreover, let $\mathfrak{p}$ be a prime in K and $\sigma_{\mathfrak{p}}$ be the Frobenius element in $\mathrm{Gal}(K^{ab}/K)$ *corresponding to $\mathfrak{p}$. Then*

$$j(E)^{\sigma_{\mathfrak{p}}} = j(\bar{\mathfrak{p}} * E)$$

And therefore for any fractional ideal $\mathfrak{a}$ in K we have

$$j(E)^{(\mathfrak{a},H/K)} = j(\bar{\mathfrak{a}} * E)$$

where $(-, H/K)$ denotes the Artin symbol.

We are going to use the following proposition to prove Theorem 3.1. The proof of the proposition can be found in [3] II p.125 ∼ p.127.

Proposition 3.2. *There is a finite set of rational primes $S \subset \mathbb{Z}$ such that if $p \notin S$ is a prime which splits in K, say as $p\,\mathcal{O}_{\mathrm{K}} = \mathfrak{p}\mathfrak{p}'$, then*

$$F(\sigma_{\mathfrak{p}}) = \bar{\mathfrak{p}} \in Cl(\mathcal{O}_{\mathrm{K}})$$

Proof (of Theorem 3.1). Let $F : \mathrm{Gal}(\bar{K}/K) \longrightarrow Cl(\mathcal{O}_{\mathrm{K}})$ be the group homomorphism constructed in section 2.5. Since F is continuous, $\ker F$, the kernel of F, is a closed normal subgroup of $\mathrm{Gal}(\bar{K}/K)$. By Galois theory, it corresponds to a field $L \subset \bar{K}$ such that $\ker F = \mathrm{Gal}(\bar{K}/L)$. Then we have

$$\begin{aligned}
\mathrm{Gal}(\bar{K}/L) &= \ker F \\
&= \{\sigma \in \mathrm{Gal}(\bar{K}/K) : F(\sigma) = 1\} \\
&= \{\sigma \in \mathrm{Gal}(\bar{K}/K) : E^{\sigma} \cong E\} \\
&= \{\sigma \in \mathrm{Gal}(\bar{K}/K) : j(E^{\sigma}) = j(E)\} \\
&= \{\sigma \in \mathrm{Gal}(\bar{K}/K) : j(E)^{\sigma} = j(E)\} \\
&= \mathrm{Gal}(\bar{K}/K(j(E)))
\end{aligned}$$

Therefore $K(j(E)) = L$. Since $\mathrm{Gal}(L/K) \cong \mathrm{Gal}(\bar{K}/K)/\mathrm{Gal}(\bar{K}/L) \cong F(\mathrm{Gal}(\bar{K}/K)) \subset Cl(\mathcal{O}_{\mathrm{K}})$ is abelian, $K(j(E))/K$ is an abelian extension.
Let $\mathfrak{c}$ be the conductor of L/K. Consider the composition of the Artin map with F:

$$I(\mathfrak{c}) \xrightarrow{(\cdot,L/K)} \mathrm{Gal}(L/K) \xrightarrow{F} Cl(\mathcal{O}_{\mathrm{K}})$$

where $I(\mathfrak{c}) = \{$fractional ideals of Kwhich are coprime to $\mathfrak{c}\}$.

Claim: $F(\mathfrak{a}, L/K) = \bar{\mathfrak{a}}$ for all $\mathfrak{a} \in I(\mathfrak{c})$.

which means the composition is just the natural projection of $I(\mathfrak{c})$ onto $Cl(\mathcal{O}_{\mathrm{K}})$.

Let $\mathfrak{a} \in I(\mathfrak{c})$. Let S be the finite set described in Proposition 3.2. Denote

$$P_{\mathfrak{c}} = \{(x) : x \equiv 1 \mod \mathfrak{c}\}$$

Then by Dirichlet's theorem(see [3] II.3.4.), there exists a degree 1 prime $\mathfrak{p} \in I(\mathfrak{c})$ in the same $P_{\mathfrak{c}}-$class as $\mathfrak{a}$ and $\mathfrak{p}$ does not lie on primes of S. In a word, there exists $\alpha \in K^*$ satisfying

$$\alpha \equiv 1 \mod \mathfrak{c}, \qquad \mathfrak{a} = (\alpha)\mathfrak{p}$$

Therefore

$$\begin{aligned} F((\mathfrak{a}, L/K)) &= F((\alpha)\mathfrak{p}, L/K) \\ &= F(\mathfrak{p}, L/K) \\ &= \bar{\mathfrak{p}} \\ &= \bar{\mathfrak{a}} \end{aligned}$$

This completes the proof of the claim.

By the claim, for any principal ideal $(\alpha) \in I(\mathfrak{c})$, we have $F((\alpha), L/K) = 1$. Note that F is injective, therefore

$$((\alpha), L/K) = 1 \quad \text{for all } (\alpha) \in I(\mathfrak{c})$$

This implies that $\mathfrak{c} = 1$. In particular, L/K is everywhere unramified. Thus L is contained in the Hilbert class field H of K.

By the claim we have proved, the map $F : \mathrm{Gal}(L/K) \longrightarrow Cl(\mathcal{O}_{\mathrm{K}})$ is surjective. Since it is also injective, F is actualy an isomorphism from $\mathrm{Gal}(L/K)$ to $Cl(\mathcal{O}_{\mathrm{K}})$. In particular, $[L : K] = \# \mathrm{Gal}(L/K) = \#Cl(\mathcal{O}_{\mathrm{K}}) = h$, where h is the class number of $\mathcal{O}_{\mathrm{K}}$. Since L is contained in H and $[H : K] = h$, we must have $L = H$, i.e. $K(j(E)) = H$. This proves (a).

Moreover, $[\mathbb{Q}(j(E) : \mathbb{Q})] \geq [K(j(E) : K)]$. But Corollary 2.6, $[\mathbb{Q}(j(E)) : \mathbb{Q}] \leq \#Cl(\mathcal{O}_{\mathrm{K}}) = h$, thus $[\mathbb{Q}(j(E)); \mathbb{Q}] = [K(j(E)) : K] = h$. This proves (b).

We turn to prove (c). Let

$$\mathcal{J} = \{j(E_1), ..., j(E_h)\}$$

Since $Cl(\mathcal{O}_{\mathrm{K}})$ acts transitively on $\{E_1, ..., E_h\}$ (see Section 2.5), $Cl(\mathcal{O}_{\mathrm{K}})$ acts transitively on $\mathcal{J}$. Since $F : \mathrm{Gal}(\bar{K}/K) \longrightarrow Cl(\mathcal{O}_{\mathrm{K}})$ is surjective, $\mathrm{Gal}(\bar{K}/K)$ acts transitively on $\mathcal{J}$. Thus $\mathcal{J}$ is a complete set of all $\mathrm{Gal}(\bar{K}/K)$ conjugates of $j(E)$.

Finally, (d) follows directly by the claim.

□

Remark 3.3. *Theorem 3.1(d) tells us that for any prime $\mathfrak{p}$ of K, we have*

$$F(\sigma_{\mathfrak{p}}) = \bar{\mathfrak{p}}$$

i.e. $E^{\sigma_{\mathfrak{p}}} = \bar{\mathfrak{p}} * E$ (up to isomorphism). The action of $\sigma_{\mathfrak{p}}$ on E is intuitively the action of $\sigma_{\mathfrak{p}}$ on the coefficients of the Weierstrass equation of E. And the action of $\bar{\mathfrak{p}}$ on E is basically the action of $\bar{\mathfrak{p}}$ on the lattice corresponding to E. The map F builds a bridge between the algebraic action(Galois action) and the analytic action(action on lattices).

4 Integrality of the $j-$invariant

In this section, we are going to prove the following theorem:

Theorem 4.1. *Let E be a CM elliptic curve over $\mathbb{C}$. Then $j(E)$ is an algebraic integer.*

Before proving the theorem, we need to introduce the notion of $j-$function, modular function and modular equation.

4.1 The $j-$function

Let α, β be two arbitrary nonzero complex numbers satisfying $\frac{\alpha}{\beta} \notin \mathbb{R}$. We denote $[\alpha, \beta]$ to be the lattice $\mathbb{Z}\alpha + \mathbb{Z}\beta$. Recall in section 2.2, we define the $j-$invariant of a lattice. The $j-$function is a function

$$j : \mathbb{H} \longrightarrow \mathbb{C}$$

satisfying $j(\tau) = j([1, \tau])$. Here $\mathbb{H} = \{z \in \mathbb{C} : Im(z) > 0\}$ is the upper half plane. Explicitly, let

$$g_2(\tau) = g_2([1, \tau]) = 60 \sum_{m,n \in \mathbb{Z}, (m,n) \neq (0,0)} \frac{1}{(m + n\tau)^4}$$

$$g_3(\tau) = g_3([1, \tau]) = 140 \sum_{m,n \in \mathbb{Z}, (m,n) \neq (0,0)} \frac{1}{(m + n\tau)^6}$$

Then

$$j(\tau) = 1728 \frac{g_2(\tau)^3}{g_2(\tau)^3 - 27g_3(\tau)^2}$$

Here are some basic properties of the $j-$function. The proof of these properties can be found in [1].11.2.

Proposition 4.2. *(i) $j(\tau)$ is a holomorphic function on $\mathbb{H}$.*
(ii) The special linear group $\mathrm{SL}(2, \mathbb{Z})$ *acts on the upper half plane $\mathbb{H}$ by*

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \tau = \frac{a\tau + b}{c\tau + d}$$

for $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}(2, \mathbb{Z})$ *and $\tau \in \mathbb{H}$. Then for any $\tau, \tau' \in \mathbb{H}$, we have*

$$j(\tau) = j(\tau') \iff \tau' = \gamma\tau' \textit{ for some } \gamma \in \mathrm{SL}(2, \mathbb{Z})$$

(iii) $j : \mathbb{H} \to \mathbb{C}$ is surjective.

To conclude this section, let us consider the $q-$expansion of $j-$function. Let $q = e^{2\pi i\tau}$, then

$$j(\tau) = \frac{1}{q} + \sum_{n=0}^{\infty} c_n q^n$$

where $c_n \in \mathbb{Z}$. For the details of the $q-$expansion, see [2] §4.1.

Remark 4.3. *In the definition of $j-$invariant, we have multiplied by 1728 so that the coefficient of $\frac{1}{q}$ in the $q-$expansion is 1.*

4.2 Modular functions for $\Gamma_0(m)$

In this subsection, we define the modular functions of $\Gamma_0(m)$ and introduce some of their properties.

Definition 4.4. *Let m be a positive integer. Define*

$$\Gamma_0(m) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}(2, \mathbb{Z}) : c \equiv 0 \mod m \right\}.$$

Definition 4.5. *A modular function for $\Gamma_0(m)$ is a complex-valued function defined on the upper half plane $\mathbb{H}$ except for isolated singularities, satisfying the following three conditions:*
(i) $f(\tau)$ is meromorphic on $\mathbb{H}$.
(ii) $f(\tau)$ is invariant under $\Gamma_0(m)$.
(iii) $f(\tau)$ is meromorphic at the cusps.

By (ii) we mean that for any $\gamma \in \Gamma_0(m)$, $f(\gamma\tau) = f(\tau)$. Now assume f satisfies (i) and (ii). By (iii), we mean that for any $\gamma \in \mathrm{SL}(2, \mathbb{Z})$, $f(\gamma\tau)$ has a $q-$expansion of the following form:

$$f(\gamma\tau) = \sum_{n=-N}^{\infty} a_n q^{n/m}$$

Here $q = e^{2\pi i\tau}, N \in \mathbb{Z}_{\geq 0}$.

We have the following theorem:

Theorem 4.6. *Let m be a positive integer.*
(i) $j(\tau)$ is a modular function for $\mathrm{SL}(2, \mathbb{Z})$ and every modular function for $\mathrm{SL}(2, \mathbb{Z})$ is a rational function in $j(\tau)$.
(ii) $j(\tau)$ and $j(m\tau)$ are modular functions for $\Gamma_0(m)$, and every modular function for $\Gamma_0(m)$ is a rational function in $j(\tau)$ and $j(m\tau)$.

To prove the theorem, one of the key is the following lemma:

Lemma 4.7.
(i) A holomorphic modular function for $\mathrm{SL}(2, \mathbb{Z})$ which is holomorphic at ∞ is constant.
(ii) A holomorphic modular function for $\mathrm{SL}(2, \mathbb{Z})$ is a polynomial in $j(\tau)$.

The proof of Lemma 4.7 and Theorem 4.6 can be found in [1]11.9.and 11.10.

4.3 Modular equation

In this part, we will introduce the Modular function and use it to prove the integrality of the $j-$invariant of a CM elliptic curve.

We want to understand the right cosets of $\Gamma_0(m)$ in $\mathrm{SL}(2, \mathbb{Z})$. First, $\Gamma_0(m)$ is of finite index in $\mathrm{SL}(2, \mathbb{Z})$. To see this, we consider the following set:

$$C(m) = \left\{ \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} : ad = m, a > 0, 0 \leq b < d, gcd(a, b, d) = 1 \right\}.$$

Let $\sigma_0 = \begin{pmatrix} m & 0 \\ 0 & 1 \end{pmatrix} \in C(m)$. We have the following lemma (the proof can be seen in [1].Exercise 11.8.):

Lemma 4.8. *For $\sigma \in C(m)$, the set*

$$(\sigma_0^{-1} \mathrm{SL}(2, \mathbb{Z})\sigma) \cap \mathrm{SL}(2, \mathbb{Z})$$

is a right coset of $\Gamma_0(m)$ in $\mathrm{SL}(2, \mathbb{Z})$. Moreover, it induces a one-to-one correspondence between the elements in $C(m)$ and right cosets of $\Gamma_0(m)$ in $\mathrm{SL}(2, \mathbb{Z})$.

By the lemma $[\mathrm{SL}(2, \mathbb{Z}) : \Gamma_0(m)] = |C(m)|$. It is not hard to see

$$|C(m)| = m \prod_{p|m} (1 + \frac{1}{p})$$

Let the right cosets of $\Gamma_0(m)$ in $\mathrm{SL}(2, \mathbb{Z})$ be $\Gamma_0(m)\gamma_i, i = 1, ..., |C(m)|$. Consider the following polynomial in X:

$$\Phi_m(X, \tau) = \prod_{i=1}^{|C(m)|} (X - j(m\gamma_i\tau))$$

We are going to prove that it is a polynomial in X and $j(\tau)$. It suffices to prove the coefficients are polynomials in $j(\tau)$. To do this, we need another form of $\Phi_m(X, \tau)$. First, for any $\gamma \in \mathrm{SL}(2, \mathbb{Z})$, let σ be the element in $C(m)$ corresponding to the right coset $\Gamma_0(m)\gamma$ in Lemma 4.1. That is,

$$(\sigma_0^{-1} \mathrm{SL}(2, \mathbb{Z})\sigma) \cap \mathrm{SL}(2, \mathbb{Z}) = \Gamma_0(m)\gamma$$

Then there exists $\bar{\gamma} \in \mathrm{SL}(2,\mathbb{Z})$, such that $\sigma_0\gamma = \bar{\gamma}\sigma$. Therefore

$$\begin{aligned} j(m\gamma\tau) &= j(\sigma_0\gamma\tau) \\ &= j(\bar{\gamma}\sigma\tau) \\ &= j(\sigma\tau) \end{aligned}$$

Therefore

$$\Phi_m(X,\tau) = \prod_{\sigma\in C(m)} (X - j(\sigma\tau))$$

Since $\sigma = \begin{pmatrix} a & b \\ 0 & d \end{pmatrix}$ for some nonnegative integers $a, b, d,$ and $a, d \neq 0$, then $j(\sigma\tau) = j(\frac{a\tau+b}{d})$ is holomorphic. Thus the coefficients of $\Phi_m(X,\tau)$ are holomorphic functions in τ. We also see that, for any $\gamma \in \mathrm{SL}(2,\mathbb{Z})$,

$$\begin{aligned} \Phi_m(X,\gamma\tau) &= \prod_{i=1}^{|C(m)|} (X - j(m\gamma_i\gamma\tau)) \\ &= \prod_{i=1}^{|C(m)|} (X - j(m\gamma_i\tau)) \qquad \text{(since } j(m\tau) \text{ is } \Gamma_0(m)\text{−invariant)} \\ &= \Phi_m(X,\tau) \end{aligned}$$

Thus the coefficients are $\mathrm{SL}(2,\mathbb{Z})-$invariant.

To prove the coefficients are meromorphic at the cusps, we look into the $q-$expansions. Let $\sigma = \begin{pmatrix} a & b \\ 0 & d \end{pmatrix}$, where $ad = m, a > 0, 0 \leq b < d, \gcd(a,b,d) = 1$. We know $j(\tau)$ has the following $q-$expansion:

$$j(\tau) = \frac{1}{q} + \sum_{n=0}^{\infty} c_n q^n, c_n \in Z$$

Denote $\zeta_m = e^{\frac{2\pi i}{m}}$. Since $e^{\frac{2\pi i(a\tau+b)}{d}} = (e^{2\pi i\tau})^{\frac{a}{d}} e^{\frac{2\pi ib}{d}} = q^{\frac{a}{d}} e^{\frac{2\pi ib}{d}} = q^{\frac{a^2}{m}} \zeta_m^{ab}$, the $q-$expansion of $j(\sigma\tau)$ is

$$j(\sigma\tau) = \frac{\zeta_m^{-ab}}{(q^{1/m})^{a^2}} + \sum_{n=0}^{\infty} c_n \zeta_m^{abn} (q^{1/m})^{a^2 n}$$

We see that the $q-$expansion of $j(\sigma\tau)$ has only finitely many negative terms. Since the coefficients of $\Phi_m(X,\tau)$ are polynomials of $j(\sigma\tau)'s$, their $q-$expansion also only have finitely many negative terms. Therefore the coefficients are meromorphic at the cusps. So far we have proved that the coefficients are holomorphic modular functions for $\mathrm{SL}(2,\mathbb{Z})$. By Lemma 4.7, the coefficients are polynomials in $j(\tau)$. Thus $\Phi_m(X,\tau)$ is a polynomial in X and $j(\tau)$, i.e. there exists a polynomial $\Phi_m(X,Y) \in \mathbb{C}[X,Y]$, such that

$$\Phi_m(X, j(\tau)) = \prod_{i=1}^{|C(m)|} (X - j(m\gamma_i\tau))$$

We call the polynomial $\Phi_m(X,Y)$ the *modular equation.* The modular equation has the following properties:

Theorem 4.9. *Let m be a positive integer.*
(i) $\Phi_m(X,Y) \in \mathbb{Z}[X,Y]$
(ii) $\Phi_m(X,Y)$ is irreducible if it is regarded as a polynomial in X.
(iii) $\Phi_m(X,Y) = \Phi_m(Y,X)$ if $m > 1$.
(iv) If m is not a square, then $\Phi_m(X,X)$ is a polynomial of degree > 1 whose leading coefficient is ± 1.

Proof. See [1]11.18. □

Next, we are going to explain the following result:

Theorem 4.10. *Let m be a positive integer. Let K be an imaginary quadratic field and R be an order of K. Let E, E' be two elliptic curves over $\mathbb{C}$ with CM by R. Then*

$$\Phi_m(j(E_1), j(E_2)) = 0 \iff \textit{There exists a cyclic isogeny } \phi : E_1 \to E_2 \textit{ of degree } m$$

Here the cyclic isogeny ϕ means there exist analytic isomorphisms

$$f_1 : \mathbb{C}/\Lambda_1 \longrightarrow E_1$$
$$f_2 : \mathbb{C}/\Lambda_2 \longrightarrow E_2$$

such that the following diagram commutes:

$$\begin{tikzcd}
\mathbb{C}/\Lambda_1 \arrow[r, "f_1"] \arrow[d, "\phi_\alpha"] & E_1 \arrow[d, "\phi"] \\
\mathbb{C}/\Lambda_2 \arrow[r, "f_2"] & E_1
\end{tikzcd}$$

and moreover $\alpha\Lambda_1$ is a cyclic subgroup of Λ_2 of order m, i.e. $\Lambda_2/\alpha\Lambda_1 \cong \mathbb{Z}/m\mathbb{Z}$.

It is not hard to see Theorem 4.10 is equivalent the following result:

Theorem 4.11. *Let $u, v \in \mathbb{C}$. Then $\Phi_m(u, v) = 0$ if and only if there is a lattice Λ and a cyclic sublattice $\Lambda' \subset \Lambda$ of index m such that $u = j(\Lambda)$ and $v = j(\Lambda')$.*

To prove Theorem 4.11, we need the following lemma:

Lemma 4.12. *Let $\tau \in \mathbb{H}$ and $\Lambda = [1, \tau]$. For any $\sigma = \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \in C(m)$, the lattice $\Lambda' = d[1, \sigma\tau]$ is a sublattice of Λ of order m. Moreover, the map*

$$\sigma \mapsto d[1, \sigma\tau]$$

induces a bijection from $C(m)$ to the set of cyclic subgroup of Λ of order m.

The proof of Lemma 4.12 only involves basic properties of abelian groups. For the details, one can see [1].11.24.

Proof of Theorem 4.11. Let $u, v \in \mathbb{C}$ satisfying $\Phi_m(u, v) = 0$. Since the map $j : \mathbb{H} \to \mathbb{C}$ is surjective, we can choose $\tau \in \mathbb{H}$ such that $u = j(\tau)$. By the definition of Φ_m, we must have $v = j(\sigma\tau)$ for some $\sigma \in C(m)$. Let $\Lambda = [1, \tau], \Lambda' = d[1, \sigma\tau]$. Then by Lemma 4.12, Λ' is a cyclic sublattice of Λ of of order m. We have $u = j(\Lambda)$ and $v = j(\Lambda')$.

Conversely, let Λ' be a cyclic sublattice of Λ of order m. Then up to homethety we can assume $\Lambda = [1, \tau]$ for some $\tau \in \mathbb{H}$. Then by Lemma 4.12, $\Lambda' = d[1, \sigma\tau]$ for some $\sigma \in C(m)$. Then $j(\Lambda) = j(\tau)$ and $j(\Lambda') = j(\sigma\tau)$. Therefore $\Phi_m(u, v) = 0$. This completes the proof of Theorem 4.11. □

There is a criterion of when a lattice is a cyclic sublattice of another lattice. We will need the notion of primitive ideal.

Definition 4.13. *Given an order R, we say that a proper $R-$ideal is primitive if it is not of the form $d\mathfrak{a}$ where $d > 1$ is an integer and $\mathfrak{a}$ is a proper $R-$ideal.*

We have the following proposition:

Proposition 4.14. *Let R be an order in an imaginary quadratic field, and let $\mathfrak{b}$ be a proper fractional $R-$ideal. Then given a proper $R-$ideal $\mathfrak{a}$, $\mathfrak{ab}$ is a sublattice of $\mathfrak{b}$ of index $N(\mathfrak{a})$, and $\mathfrak{ab}$ is a cyclic sublattice if and only if $\mathfrak{a}$ is a primitive ideal.*

We explain the notation $N(\mathfrak{a})$ in Proposition 4.14. For any proper $R-$-ideal $\mathfrak{a}$, we can define its norm to be $N(\mathfrak{a}) = |R/\mathfrak{a}| = [R : \mathfrak{a}]$. The norm has the following properties:

Proposition 4.15. *Let R be an order in an imaginary quadratic field. Then:*
(i) $N(\alpha R) = N(\alpha)$ for $\alpha \in R, \alpha \neq 0$
(ii) $N(\mathfrak{a}\mathfrak{b}) = N(\mathfrak{a})N(\mathfrak{b})$ for proper $R-$ideals $\mathfrak{a}$ and $\mathfrak{b}$
(iii) $\mathfrak{a}\bar{\mathfrak{a}} = N(\mathfrak{a})R$

Proof. See [1] 7.14. □

By Proposition 4.15. and some basic algebra, we can prove Proposition 4.14. The details can be found in [1] 11.26.

We can finally prove the integrality of the $j-$invariant.

Proof of Theorem 4.1. Let K be an imaginary quadratic field and R be an order of K. Let E be an elliptic curve over $\mathbb{C}$ with CM by R. We try to find a cyclic isogeny from E to E whose degree is not a square. There exists a proper $R-$ideal $\mathfrak{a}$ such that $E \cong \mathbb{C}/\mathfrak{a}$. Let $\alpha \in R$. Consider the endomorphism

$$[\alpha] : E \cong \mathbb{C}/\mathfrak{a} \longrightarrow E \cong \mathbb{C}/\mathfrak{a}$$

We know $\deg[\alpha] = \#\ker[\alpha] = |\alpha^{-1}\mathfrak{a}/\mathfrak{a}|$ (See [4] III 4.10). By Proposition 4.14, $\alpha\mathfrak{a}$ is a cyclic sublattice of $\mathfrak{a}$ if and only if αR is a primitive ideal of R, and it is equivalent to that α is a primitive element in R. And by Proposition 4.15(i), we have $|\alpha^{-1}\mathfrak{a}/\mathfrak{a}| = |\mathfrak{a}/\alpha\mathfrak{a}| = N(\alpha R) = N(\alpha)$. We notice that $\mathfrak{a}$ is a cyclic sublattice of $\alpha^{-1}\mathfrak{a}$ if and only if $\alpha\mathfrak{a}$ is a cyclic sublattice of $\mathfrak{a}$. Therefore to find a cyclic isogeny from E to E whose degree is not a square, it suffices to find $\alpha \in R$ such that $N(\alpha)$ is not a square.

Let f be the conductor of R (which means the index of R in $\mathcal{O}_{\mathrm{K}}$ is f). By [1] 7.2, $R = [1, fw_K]$, where $w_K = (d_K + \sqrt{d_K})/2$ and d_K is the discriminant of K. Then $\alpha = fw_K$ is primitive in R, and one can easily show its norm $N(\alpha) = m$ is not a square.

Now by Theorem 4.10, $\Phi_m(j(E), j(E)) = 0$. Then the integrality of $j(E)$ follows from (iv) of Theorem 4.9. □

5 The maximal abelian extension

The goal of this section is to prove the torsion points of an elliptic curve with CM by $\mathcal{O}_{\mathrm{K}}$ can be used to generate the maximal abelian extension of K. Here K is an imaginary quadratic field.

5.1 Torsion points

Let K be an imaginary quadratic field and $E/\mathbb{C}$ be an elliptic curve with CM by $\mathcal{O}_{\mathrm{K}}$. By [3] II.1.1, there is unique isomorphism

$$[\ ] : \mathcal{O}_{\mathrm{K}} \longrightarrow \mathrm{End}(E)$$

such that for any invariant differential $\omega \in \Omega_E$ on E,

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

Define the set of torsion points of E to be

$$E_{tors} = \{P \in E(\mathbb{C}) : \exists m \in \mathbb{N} \text{ s.t. } [m]P = 0\}$$

For any positive integer m, we can define the $m-$torsion points to be

$$E[m] = \{P \in E(\mathbb{C}) : [m]P = 0\}$$

More generally, let $\mathfrak{a} \subset \mathcal{O}_{\mathrm{K}}$ be an ideal of $\mathcal{O}_{\mathrm{K}}$. We can also define the $\mathfrak{a}-$*torsion* points of E to be

$$E[\mathfrak{a}] = \{P \in E(\mathbb{C}) : [\alpha]P = 0, \forall\alpha \in \mathfrak{a}\}$$

We know E can be defined over the Hilbert class field H of K. Fix a Weierstrass equation for E with coefficients in H. We have the following results:

Theorem 5.1. *Let*

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

be the field generated by the $j-$invariant and the coordinates of all the torsion points of E. Then L is an abelian extension of H.

Proof. Let $L_m = K(j(E), E[m]) = H(E[m])$ be the extension of generated by the $m-$torsion points of E. Since L is the composition of all the L_m's, we only need to prove L_m is an abelian extension of H. For any $\sigma \in \mathrm{Gal}(\bar{K}/H)$ and $T \in E[m]$, since E is defined over H, then $T^\sigma \in E[m]$. Since $j(E)^\sigma = j(E^\sigma) \in H$, then we have $\sigma(L_m) \subset L_m$ for all $\sigma \in \mathrm{Gal}(\bar{K}/H)$. This implies that L_m/H is a Galois extension. In addition, we have the following representation

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

determined by the condition

$$\rho(\sigma)(T) = T^\sigma, \ \forall \sigma \in \mathrm{Gal}(\bar{K}/H), T \in E[m]$$

We have

$$\begin{aligned} \ker \rho &= \{\sigma \in \mathrm{Gal}(\bar{K}/H) : T^\sigma = T \text{ for all } T \in E[m]\} \\ &= \{\sigma \in \mathrm{Gal}(\bar{K}/H) : \sigma \text{ fixes the coordinates of } E[m]\} \\ &= \mathrm{Gal}(\bar{K}/L_m) \end{aligned}$$

Therefore ρ induces an injection from $\mathrm{Gal}(L_m/H) \cong \mathrm{Gal}(\bar{K}/H)/\mathrm{Gal}(\bar{K}/L_m)$ to $\mathrm{Aut}(E[m])$. By [4] 6.4, $E[m] \cong (\mathbb{Z}/m\mathbb{Z}) \times (\mathbb{Z}/m\mathbb{Z})$ and then $\mathrm{Aut}(E[m]) \cong \mathrm{GL}_2(\mathbb{Z}/m\mathbb{Z})$. Thus $\mathrm{Gal}(\text{Ł}_m/H)$ is isomorphic to a subgroup of $\mathrm{GL}_2(\mathbb{Z}/m\mathbb{Z})$.

We also know that each endomorphism of E can be defined over H(see [3] 2.2(b)). So elements of $\mathrm{Gal}(L_m/H)$ will commutes with element of $\mathcal{O}_\mathrm{K}$ in their action on $E[m]$, i.e.

$$([\alpha]T)^\sigma = [\alpha](T^\sigma) \qquad \text{for all } \sigma \in \mathrm{Gal}(L_m/H), T \in E[m] \text{ and } \alpha \in \mathcal{O}_\mathrm{K}$$

This implies that ρ is actually a homomorphism from $\mathrm{Gal}(\bar{K}/H)$ to the group of $\mathcal{O}_\mathrm{K}/m\,\mathcal{O}_\mathrm{K}-$module automorphisms of $E[m]$. That is to say, ρ induces an injection

$$\phi : \mathrm{Gal}(L_m/H) \hookrightarrow \mathrm{Aut}_{\mathcal{O}_\mathrm{K}/m\,\mathcal{O}_\mathrm{K}}(E[m])$$

By [3] 1.4(b), $E[m]$ is a free $\mathcal{O}_\mathrm{K}/m\,\mathcal{O}_\mathrm{K}$ module of rank 1. Then $\mathrm{Aut}_{\mathcal{O}_\mathrm{K}/m\,\mathcal{O}_\mathrm{K}}(E[m]) \cong (\mathcal{O}_\mathrm{K}/m\,\mathcal{O}_\mathrm{K})^\times$ is an abelian group. So $\mathrm{Gal}(L_m/H)$ is an abelian group. □

Remark 5.2. *In general, $L = K(j(E), E_{tors})$ is not an abelian extension of K. To get the maximal abelian extension of K, we need some modification.*

5.2 Weber function

For an elliptic curve with CM by $\mathcal{O}_\mathrm{K}$, we can take a model(a Weierstrass equation) for E defined over H. Fix a morphism

$$h : E \longrightarrow E/\mathrm{Aut}(E) \cong \mathbb{P}^1$$

which is defined over H. Such a morphism is called a *Weber function* for E/H.

Example 5.1. *If we take a Weierstrass equation for E of the form*

$$y^2 = x^3 + ax + b \quad \textit{with } a, b \in H$$

then

$$h(P) = h(x,y) = \begin{cases} x & \textit{if } ab \neq 0 \\ x^2 & \textit{if } b = 0 \\ x^3 & \textit{if } a = 0 \end{cases}$$

is a Weber function for E/H.

Example 5.2. *We choose a lattice Λ and an isomorphism*

$$f : \mathbb{C}/\Lambda \to E(\mathbb{C}), \quad z \mapsto (\wp(z;\Lambda), \wp'(z;\Lambda))$$

Then the Weber function can be

$$h(f(z)) = \begin{cases} \frac{g_2(\Lambda)g_3(\Lambda)}{\Delta(\Lambda)}\wp(z;\Lambda) & \textit{if } j(E) \neq 0, 1728 \\ \frac{g_2(\Lambda)^2}{\Delta(\Lambda)}\wp(z;\Lambda)^2 & \textit{if } j(E) = 1728 \\ \frac{g_3(\Lambda)}{\Delta(\Lambda)}\wp(z;\Lambda)^3 & \textit{if } j(E) = 0 \end{cases}$$

The function $h : E \to \mathbb{P}^1$ does not depend on the choice of f. It only depends on the $\mathbb{C}$-isomorphism class of E. So it is an intrinsic construction of Weber function.

5.3 The ray class field

Now we are prepared to state the main result in this section.

Theorem 5.3. *Let K be an imaginary quadratic field and E be an elliptic curve with CM by $\mathcal{O}_{\mathrm{K}}$. Fix a Weber function $h : E \to \mathbb{P}^1$ for E/H. Let $\mathfrak{c}$ be an integral ideal of K Then the field*

$$K(j(E), h(E[\mathfrak{c}]))$$

is the ray class field of K of level $\mathfrak{c}$.

To prove Theorem 5.3, we need the following lemma:

Lemma 5.4. *Let K be an imaginary quadratic field, H the Hilbert class field of K, and E/H an elliptic curve with CM by $\mathcal{O}_{\mathrm{K}}$. For all but finitely many degree 1 prime ideals $\mathfrak{p}$ of K that satisfy*

$$(\mathfrak{p}, H/K) = 1,$$

there is a unique $\pi = \pi_{\mathfrak{p}} \in \mathcal{O}_{\mathrm{K}}$ such that $\mathfrak{p} = \pi\,\mathcal{O}_{\mathrm{K}}$ and

$$\begin{tikzcd} E \arrow[r, "{[\pi]}"] \arrow[d] & E \arrow[d] \\ \tilde{E} \arrow[r, "\phi"] & \tilde{E} \end{tikzcd}$$

Here the vertical maps are reduction of E modulo some prime $\mathfrak{P}$, where $\mathfrak{P}$ is a prime of H over some suitable prime $\mathfrak{p}$ of K and ϕ is the p^{th} power Frobenius map.

Proof. See [3] 5.4. □

Proof of Theorem 5.3. Let

$$L = K(j(E), h(E[\mathfrak{c}]))$$

Proving that L is the ray class field of K of level $\mathfrak{c}$ is equivalent to proving that

$$(\mathfrak{p}, L/K) = 1 \iff \mathfrak{p} \in P_{\mathfrak{c}}$$

where $P_{\mathfrak{c}} = \{(x) : x \in K, x \equiv 1 \mod \mathfrak{c}\}$. It suffices to prove this for all but finitely many degree 1 primes in K.

Suppose $\mathfrak{p}$ is a degree 1 prime of K with $\mathfrak{p} \in P_{\mathfrak{c}}$. By definition, this means that

$$\mathfrak{p} = \mu\,\mathcal{O}_{\mathrm{K}} \qquad \text{for some } \mu \in \mathcal{O}_{\mathrm{K}} \text{ with } \mu \equiv 1 \mod \mathfrak{c}$$

In particular, $\mathfrak{p}$ is principal, so $(\mathfrak{p}, H/K) = 1$. Therefore by Lemma 5.4(after excluding finitely many $\mathfrak{p}$'s) there exists some $\pi \in \mathcal{O}_{\mathrm{K}}$ such that $\mathfrak{p} = \pi\,\mathcal{O}_{\mathrm{K}}$ and the following diagram commutes:

$$\begin{tikzcd} E \arrow[r, "{[\pi]}"] \arrow[d] & E \arrow[d] \\ \tilde{E} \arrow[r, "\phi"] & \tilde{E} \end{tikzcd} \tag{1}$$

Since $\pi\,\mathcal{O}_{\mathrm{K}} = \mathfrak{p} = \mu\,\mathcal{O}_{\mathrm{K}}$, there exists some $\xi \in {\mathcal{O}_{\mathrm{K}}}^{\times}$ such that $\pi = \xi\mu$. Note that $[\xi] \in \mathrm{Aut}(E)$, so $[\pi]$ and $[\mu]$ differ by an automorphism of E. We already see that $(\mathfrak{p}, H/K)$ fixes $H = K(j(E))$, in order to show it fixes all of L, it remains to show it fixes $h(E[\mathfrak{c}])$. Let $T \in E[\mathfrak{c}]$ be an arbitrary $\mathfrak{c}-$torsion point. Then the commutative diagram gives

$$\widetilde{T^{(\mathfrak{p},L/K)}} = \phi(\widetilde{T}) = \widetilde{[\pi]T}.$$

On the other hand, by [4] VII 3.1(b), the reduction map $E \to \widetilde{E}$ is injective on torsion points whose order is prime to $\mathfrak{p}$. So if we ignore the finitely many $\mathfrak{p}$'s which divide $\#E[\mathfrak{c}]$, then the reduction map

$$E[\mathfrak{c}] \longrightarrow \tilde{E}[\mathfrak{c}]$$

is injective. Therefore

$$T^{(\mathfrak{p},L/K)} = [\pi]T.$$

Now we compute

$$\begin{aligned} h(T)^{(\mathfrak{p},L/K)} &= h(T^{(\mathfrak{p},L/K)}) \quad \text{since } (\mathfrak{p}, H/K) = 1 \text{ and } h \text{ is defined over } H \\ &= h([\pi]T) \\ &= h([\xi] \circ [\mu]T) \\ &= h([\mu]T) \quad \text{since } h \text{ is } \mathrm{Aut}(E)\text{-invariant} \\ &= h(T) \quad \text{since } T \in E[\mathfrak{c}] \text{ and } \mu \equiv 1 \mod \mathfrak{c} \end{aligned}$$

This completes the proof of the implication

$$\mathfrak{p} \in P_{\mathfrak{c}} \implies (\mathfrak{p}, L/K) = 1$$

To prove the converse, we take a prime $\mathfrak{p}$ of degree 1 satisfying $(\mathfrak{p}, L/K) = 1$. Then

$$(\mathfrak{p}, H/K) = (\mathfrak{p}, L/K)|_H = 1.$$

So by Lemma 5.4, except for finitely many $\mathfrak{p}$'s, there exists $\pi \in \mathcal{O}_{\mathrm{K}}$ such that $\mathfrak{p} = \pi\,\mathcal{O}_{\mathrm{K}}$ and

$$\begin{tikzcd} E \arrow[r, "{[\pi]}"] \arrow[d] & E \arrow[d] \\ \tilde{E} \arrow[r, "\phi"] & \tilde{E} \end{tikzcd} \tag{2}$$

commmutes. We choose some $\sigma \in \mathrm{Gal}(\bar{K}/K)$ such that $\sigma|_{K^{ab}} = (\mathfrak{p}, K^{ab}/K)$. In particular $\sigma|_L = (\mathfrak{p}, L/K)$ and also $\sigma|_H = 1$ since $H \subset L$.

Now let $T \in E[\mathfrak{c}]$ be an arbitrary $\mathfrak{c}$-torsion point. Then

$$\begin{aligned}
\tilde{h}(\widetilde{[\pi]}\tilde{T}) &= \tilde{h}(\widetilde{[\pi]T}) \\
&= \tilde{h}(\phi(\tilde{T})) \quad \text{from the commutative diagram} \\
&= \tilde{h}(\widetilde{T^{\sigma}}) \\
&= \widetilde{h(T^{\sigma})} \\
&= \widetilde{h(T)^{\sigma}} \quad \text{since } \sigma|_{H} = 1 \text{ and } h \text{ is defined over } H \\
&= \widetilde{h(T)}. \quad \text{since } h(T) \in L \text{ and } \sigma|_{L} = 1
\end{aligned}$$

where h is the reduction of h modulo (some prime of H above $\mathfrak{p}$) $\mathfrak{P}$:

$$\tilde{h} : \tilde{E} \longrightarrow E/\widetilde{\mathrm{Aut}(E)} \cong \tilde{E}/\widetilde{\mathrm{Aut}(E)}.$$

It follows from this and the equality $\tilde{h}(\widetilde{[\pi]}\tilde{T}) = \tilde{h}(\tilde{T})$ that there exists an automorphism $[\xi] \in \mathrm{Aut}(E)$ such that

$$\widetilde{[\pi]}\tilde{T} = \widetilde{[\xi]}\tilde{T}$$

By the injectivity of the map $E[\mathfrak{c}] \hookrightarrow \tilde{E}[\mathfrak{c}]$ (see [4] VII 3.1(b)), we immediately have

$$[\pi - \xi]T = O.$$

This implies that for any $T \in E[\mathfrak{c}]$, we can find $\xi \in {\mathcal{O}_{\mathrm{K}}}^{\times}$ such that $[\pi - \xi]T = O$. Note that $E[\mathfrak{c}]$ is a free $\mathcal{O}_{\mathrm{K}}/\mathfrak{c}-$module of rank 1(see [3] II 1.4(b)), we can choose T to be a generator of this free module. Then $[\pi - \xi]$ annihilates all of $E[\mathfrak{c}]$, which implies that $\pi \equiv \xi \mod \mathfrak{c}$ and therefore

$$\xi^{-1}\pi \equiv 1 \mod \mathfrak{c}.$$

Then we have $\mathfrak{p} = \pi\,\mathcal{O}_{\mathrm{K}} = (\xi^{-1}\pi)\,\mathcal{O}_{\mathrm{K}}$. This shows that $\mathfrak{p} \in P_{\mathfrak{c}}$, which completes the proof of Theorem 5.3. □

Since the maximal abelian extension is the composition of all the ray class fields of K, we have the corollary:

Corollary 5.5. *The maximal abelian extension of K is*

$$K^{ab} = K(j(E), h(E_{tors})).$$

6 The main theorem of complex multiplication

In this section, we are going to state the idelic version of the main theorem of complex multiplication.

6.1 $\mathfrak{p}-$primary decomposition

Before stating the main theorem, we need to introduce some notions. Let K be an imaginary quadratic field with ring of integer $\mathcal{O}_{\mathrm{K}}$. For each prime ideal $\mathfrak{p}$ of K, let $K_{\mathfrak{p}}$ be the completion of K at $\mathfrak{p}$ and let $\mathcal{O}_{\mathfrak{p}}$ be the ring of integer of $K_{\mathfrak{p}}$. For a fractional ideal $\mathfrak{a}$ of K, let $\mathfrak{a}_{\mathfrak{p}} = \mathfrak{a}\mathcal{O}_{\mathfrak{p}}$ be the fractional ideal of $K_{\mathfrak{p}}$ generated by $\mathfrak{a}$.

Let M be an $\mathcal{O}_{\mathrm{K}}-$module. The $\mathfrak{p}-$*primary component* of M, which by definition is that part of M annihilated by some power of $\mathfrak{p}$, is denoted by

$$M[p^{\infty}] = \{m \in M : \mathfrak{p}^{e}m = 0 \text{ for some } e \in \mathbb{Z}^{+}\}.$$

Then we have the following lemma:

Lemma 6.1. *(a) Let M be a torsion $\mathcal{O}_{\mathrm{K}}$ −module. Then the natural map*

$$S : \bigoplus_{\mathfrak{p}} M[\mathfrak{p}^{\infty}] \longrightarrow M$$
$$\mu = (\mu_{\mathfrak{p}}) \longmapsto \sum_{\mathfrak{p}} \mu_{\mathfrak{p}}$$

is an isomorphism. Here the sum is over all prime ideals of $\mathcal{O}_{\mathrm{K}}$, and $\mu_{\mathfrak{p}}$ denotes the $\mathfrak{p}$−component of μ. $\bigoplus_{\mathfrak{p}} M[p^{\infty}]$ is called the $\mathfrak{p}$−primary decomposition of M.
(b) Let $\mathfrak{a}$ be a fractional ideal of K. Then for each prime ideal $\mathfrak{p}$ of K, the inclusion $K \hookrightarrow K_{\mathfrak{p}}$ induces an isomorphism

$$T : (K/\mathfrak{a})[\mathfrak{p}^{\infty}] \xrightarrow{\sim} K_{\mathfrak{p}}/\mathfrak{a}_{\mathfrak{p}}.$$

(c) Again let $\mathfrak{a}$ be a fractional ideal of K. Then there is a canonical isomorphism

$$K/\mathfrak{a} \cong \bigoplus_{\mathfrak{p}} K_{\mathfrak{p}}/\mathfrak{a}_{\mathfrak{p}}.$$

Proof. See [3]II 8.1. □

Let $x \in \mathbb{A}_K^{\times}$ be an idele. We define *the ideal of* x to be the fractional ideal

$$(x) := \prod_{\mathfrak{p}} \mathfrak{p}^{\mathrm{ord}_{\mathfrak{p}}(x_{\mathfrak{p}})}.$$

If $\mathfrak{a}$ is any fractional ideal of K, we define $x\mathfrak{a}$ to be the fractional ideal $(x)\mathfrak{a}$. Note that $(x)_{\mathfrak{p}} = (x)\mathcal{O}_{\mathfrak{p}} = x_{\mathfrak{p}}\mathcal{O}_{\mathfrak{p}}$, so we have

$$(x\mathfrak{a})_{\mathfrak{p}} = x_{\mathfrak{p}}\mathfrak{a}_{\mathfrak{p}}.$$

Then by Lemma 6.1(c), we have

$$K/\mathfrak{a} \cong \bigoplus_{\mathfrak{p}} K_{\mathfrak{p}}/\mathfrak{a}_{\mathfrak{p}} \quad \text{and} \quad K/x\mathfrak{a} \cong \bigoplus_{\mathfrak{p}} K_{\mathfrak{p}}/x_{\mathfrak{p}}\mathfrak{a}_{\mathfrak{p}}$$

Now we define the *multiplication-by-x* map on $K/\mathfrak{a}$ to be multiplication of the $\mathfrak{p}$−primary component by $x_{\mathfrak{p}}$. That is, multiplication-by-x map is the map $x : K/\mathfrak{a} \to K/x\mathfrak{a}$ such that the following diagram commutes:

$$\begin{tikzcd}
K/\mathfrak{a} \arrow[r, "x"] \arrow[d, "\wr"] & K/x\mathfrak{a} \arrow[d, "\wr"] \\
\bigoplus_{\mathfrak{p}} K_{\mathfrak{p}}/\mathfrak{a}_{\mathfrak{p}} \arrow[r] & \bigoplus_{\mathfrak{p}} K_{\mathfrak{p}}/x_{\mathfrak{p}}\mathfrak{a}_{\mathfrak{p}} \\
(t_{\mathfrak{p}}) \arrow[r, mapsto] & (x_{\mathfrak{p}}t_{\mathfrak{p}})
\end{tikzcd}$$

6.2 Main theorem

Now we are ready to state the main theorem.

Theorem 6.2 (The main theorem of complex multiplication)**.** *Fix the following data:*
$K/\mathbb{Q}$ *a quadratic imaginary field with ring of integer* $\mathcal{O}_{\mathrm{K}}$
$E/\mathbb{C}$ *an elliptic curve with* $End(E) \cong \mathcal{O}_{\mathrm{K}}$
$\sigma \in \mathrm{Aut}_K(\mathbb{C})$ *an automorphism of* $\mathbb{C}$ *which fixes* K
$s \in \mathbb{A}_K^{\times}$ *an idèle of* K *satisfying* $[s, K] = \sigma|_{K^{ab}}$

Further, fix a complex analytic isomorphism

$$f : \mathbb{C}/\mathfrak{a} \xrightarrow{\sim} E(\mathbb{C})$$

where $\mathfrak{a}$ is a fractional ideal of K. Then there exists a unique complex analytic isomorphism

$$f' : \mathbb{C}/s^{-1}\mathfrak{a} \xrightarrow{\sim} E^{\sigma}(\mathbb{C})$$

(depending on f and σ) so that the following diagram commutes:

$$\begin{tikzcd}
K/\mathfrak{a} \arrow[r, "s^{-1}"] \arrow[d, "f"] & K/s^{-1}\mathfrak{a} \arrow[d, "f'"] \\
E(\mathbb{C}) \arrow[r, "\sigma"] & E^{\sigma}(\mathbb{C})
\end{tikzcd}$$

Proof. See [3] II 8.2. □

In the main theorem, f induces a bijection from $K/\mathfrak{a}$ to the torsion points of E, f' induces a bijection from $K/s^{-1}\mathfrak{a}$ to the torsion points of E^{σ}. Thus the commutative diagram explicitly describes how σ sends the torsion points of E to the torsion points of E^{σ}.

There is a $\mathbb{Q}-$analogue of the main theorem. Consider the multiplicative group $\mathbb{G}_m(\mathbb{C}) \cong \mathbb{C}^{\times}$. We have the following analytic isomorphism:

$$\begin{aligned} f : \mathbb{C}/\mathbb{Z} &\longrightarrow \mathbb{G}_m(\mathbb{C}) \\ t &\longmapsto e^{2\pi i t} \end{aligned}$$

The torsion subgroup $\mathbb{G}_m(\mathbb{C})_{tors}$ is exactly the image of $\mathbb{Q}/\mathbb{Z}$ under the map f.

Let M be a $\mathbb{Z}-$module. For any prime integer p, the $p-$primary component of M is denoted by

$$M[p^{\infty}] = \{m \in M : p^e m = 0 \text{ for some } e \in \mathbb{Z}^+\}$$

Similarly, we have the notion of $p-$primary decomposition. Here are some properties.

Lemma 6.3. *(a) Let M be a torsion $\mathbb{Z}-$module(or torsion abelian group). Then the natural map*

$$\begin{aligned} S : \bigoplus_p M[p^{\infty}] &\longrightarrow M \\ \mu = (\mu_p) &\longmapsto \sum_p \mu_p \end{aligned}$$

is an isomorphism.
(b) The $p-$component of $\mathbb{Q}/\mathbb{Z}$ is $\mathbb{Z}[p^{-1}]/\mathbb{Z}$. The inclusion $\mathbb{Z}[p^{-1}] \hookrightarrow \mathbb{Q}_p$ induces an isomorphism

$$\mathbb{Z}[p^{-1}]/\mathbb{Z} \xrightarrow{\sim} \mathbb{Q}_p/\mathbb{Z}_p$$

(c) Moreover, for any nonzero element $a \in \mathbb{Q}$, the $p-$component of $\mathbb{Q}/a\mathbb{Z}$ is isomorphic to $\mathbb{Q}_p/a\mathbb{Z}_p$. We have

$$\mathbb{Q}/a\mathbb{Z} \cong \bigoplus_p \mathbb{Q}_p/a\mathbb{Z}_p$$

Proof. See [3] §7. □

Let $x \in \mathbb{A}_{\mathbb{Q}}^{\times}$ be an idele. We define the ideal of x to be the fractional ideal

$$x\,\mathbb{Z} = (x) = \prod_p p^{\operatorname{ord}_p x_p}\,\mathbb{Z} = N_x\,\mathbb{Z}$$

Here N_x is a rational number whose sign is the same as the one of x_∞. Then we can define the multiplication-by-x map to be the multiplication of the $p-$component by x_p, i.e. it is defined to let the following diagram commute:

$$\begin{tikzcd}
\mathbb{Q}\,/\,\mathbb{Z} \arrow[r, "x"] \arrow[d, "\wr"] & \mathbb{Q}\,/x\,\mathbb{Z} \arrow[d, "\wr"] \\
\bigoplus_p \mathbb{Q}_p\,/\,\mathbb{Z}_p \arrow[r] & \bigoplus_p \mathbb{Q}_p\,/x_p\,\mathbb{Z}_p \\
(t_p) \arrow[r, mapsto] & (x_p t_p)
\end{tikzcd}$$

Then we have the $\mathbb{Q}\,-$analogue of the main theorem:

Theorem 6.4. *Fix the following data:*
$\sigma \in \operatorname{Aut}(\mathbb{C})$*, an automorphism of complex numbers,*
$s \in \mathbb{A}_{\mathbb{Q}}^{\times}$*, an idele of* $\mathbb{Q}$ *satisfying* $[s, \mathbb{Q}] = \sigma|_{\mathbb{Q}^{ab}}$.

Further, fix the complex analytic isomorphism

$$\begin{aligned} f : \mathbb{C}\,/\,\mathbb{Z} &\xrightarrow{\sim} \mathbb{G}_m(\mathbb{C}) \\ t &\longmapsto e^{2\pi i t} \end{aligned}$$

Then there exists a unique complex analytic isomorphism

$$f' : \mathbb{C}\,/s^{-1}\,\mathbb{Z} \xrightarrow{\sim} \mathbb{G}_m(\mathbb{C})$$

so that the following diagram commutes:

$$\begin{tikzcd}
\mathbb{Q}\,/\,\mathbb{Z} \arrow[r, "s^{-1}"] \arrow[d, "f"] & \mathbb{Q}\,/s^{-1}\,\mathbb{Z} \arrow[d, "f'"] \\
\mathbb{G}_m(\mathbb{C}) \arrow[r, "\sigma"] & \mathbb{G}_m(\mathbb{C}).
\end{tikzcd}$$

Proof. [3] II 7.1. □

Remark 6.5. *We can actually show that* $f'(t) = e^{2\pi i N_s t}$ *satisfies the requirement. Theorem 6.4 tells us that*

$$f(t)^{[s,\mathbb{Q}]} = f'(s^{-1}t)$$

for all $t \in \mathbb{Q}\,/\,\mathbb{Z}$*. When it is written down explicitly, we have*

$$\left(e^{2\pi i t}\right)^{[s,\mathbb{Q}]} = e^{2\pi i N_s (s^{-1}t)}$$

This formula makes it clear that how the algebraic(Galois action) of $[s, \mathbb{Q}]$ *is transformed into the analytic(multiplication) action* $t \mapsto N_s s^{-1} t$.

We can actually recover many previous results from the main theorem. For example, we can easily prove the Hilbert class field H of K is $K(j(E))$. Let $s \in \mathbb{A}_K^{\times}$ be an idele satisfying $[s, K] = \sigma_{\mathfrak{p}}$, where

$\sigma_{\mathfrak{p}} \in \mathrm{Gal}(K^{ab}/K)$ is the Frobenius of $\mathfrak{p}$. Then

$$\begin{aligned}
&(\mathfrak{p}, K(j(E))/K) = 1 \\
\iff & \sigma_{\mathfrak{p}} \text{ fixes } j(E) \\
\iff & E \cong E^{\sigma_{\mathfrak{p}}} \qquad (\text{since } j(E) = j(E)^{\sigma_{\mathfrak{p}}} = j(E^{\sigma_{\mathfrak{p}}})\ ) \\
\iff & \mathbb{C}/\mathfrak{a} \cong \mathbb{C}/s^{-1}\mathfrak{a} \\
\iff & \mathfrak{a} \text{ is homethetic to } s^{-1}\mathfrak{a} \\
\iff & \mathfrak{p} \text{ is a principal ideal} \qquad (\text{since } (s) = \mathfrak{p})
\end{aligned}$$

By class field theory, we immediately have $H = K(j(E))$.

References

[1] David A. Cox. *Primes of the form $x^2 + ny^2$—Fermat, class field theory, and complex multiplication.* AMS Chelsea Publishing, Providence, RI, third edition, [2022] ©2022. With contributions by Roger Lipsett.

[2] Serge Lang. *Elliptic functions*, volume 112 of *Graduate Texts in Mathematics.* Springer-Verlag, New York, second edition, 1987. With an appendix by J. Tate.

[3] Joseph H. Silverman. *Advanced topics in the arithmetic of elliptic curves*, volume 151 of *Graduate Texts in Mathematics.* Springer-Verlag, New York, 1994.

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