Class Field Theory & Complex Multiplication

Séminaire de Mathématiques Supérieures, CRM, Montréal

June 23-July 4, 2014

Eknath Ghate

1 Introduction

An elliptic curve has complex multiplication (or CM for short) if it has endomorphisms other than the obvious ones given by multiplication by integers.

The main purpose of these notes is to show that the j-invariant of an elliptic curve with CM along with its torsion points can be used to explicitly generate the maximal abelian extension of an imaginary quadratic field. This result is analogous to the Kronecker-Weber theorem which states that the maximal abelian extension of $\mathbb{Q}$ is generated by the values of the exponential function $e^{2\pi ix}$ at the torsion points $\mathbb{Q}/\mathbb{Z}$ of the group $\mathbb{C}/\mathbb{Z}$.

The CM theory of elliptic curves is due to many authors, including Kronecker, Weber, Hasse, Deuring, Shimura. Our exposition is based on Chapters 4 and 5 of Shimura [1], and Chapter 2 of Silverman [3]. For standard facts about elliptic curves we sometimes refer the reader to Silverman [2].

2 What is complex multiplication?

Let E and E' be elliptic curves defined over an algebraically closed field k. A homomorphism $\lambda : E \to E'$ is a rational map that is also a group homomorphism. An isogeny $\lambda : E \to E'$ is a homomorphism with finite kernel. Denote the ring of all endomorphisms of E by $\mathrm{End}(E)$, and set $\mathrm{End}_{\mathbb{Q}}(E) = \mathrm{End}(E) \otimes \mathbb{Q}$.

If E is an elliptic curve defined over $\mathbb{C}$, then E is isomorphic to $\mathbb{C}/L$ for a lattice $L \subset \mathbb{C}$. Therefore every endomorphism $\lambda : E \to E$ of E is induced by

multiplication by a complex number which we again denote by λ and which satisfies $\lambda(L) \subset L$. Thus

$$\begin{aligned} \mathrm{End}(E) &\cong \{\lambda \in \mathbb{C} \,\big|\, \lambda(L) \subset L\}, \\ \mathrm{End}_{\mathbb{Q}}(E) &\cong \{\lambda \in \mathbb{C} \,\big|\, \lambda(\mathbb{Q}L) \subset \mathbb{Q}L\}, \end{aligned}$$

where $\mathbb{Q}L$ is the $\mathbb{Q}$-linear span of L.

Definition 2.1. *An elliptic curve E defined over $\mathbb{C}$ has complex multiplication if $\mathrm{End}(E) \ncong \mathbb{Z}$.*

Let H be the upper half plane in $\mathbb{C}$.

Lemma 2.2. *Let $E \cong \mathbb{C}/L$ be an elliptic curve defined over $\mathbb{C}$. Suppose that $L = \mathbb{Z}\omega_1 \oplus \mathbb{Z}\omega_2$ with $z = \omega_1/\omega_2 \in H$. Then E has* CM *if and only if $\mathbb{Q}(z)$ is an imaginary quadratic field. In this case $\mathrm{End}_{\mathbb{Q}}(E) \cong \mathbb{Q}(z)$ and $\mathrm{End}(E)$ is isomorphic to an order in $\mathbb{Q}(z)$.*

Proof. Take $0 \neq \lambda \in \mathbb{C}$. Then

$$\begin{aligned} \lambda\omega_1 &= a\omega_1 + b\omega_2 \\ \lambda\omega_2 &= c\omega_1 + d\omega_2, \end{aligned}$$

where $\alpha = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{M}_2(\mathbb{Z})$ is invertible in $\mathrm{GL}_2(\mathbb{Q})$. Then we have

$$z = \frac{\lambda\omega_1}{\lambda\omega_2} = \frac{az+b}{cz+d} = \alpha(z),$$

so that $cz^2 + (d-a)z - b = 0$. If $\lambda \notin \mathbb{Z}$ then $b \neq 0$ and $c \neq 0$ so that $\mathbb{Q}(z)$ is an imaginary quadratic field. Moreover in this case

$$\begin{aligned} \mathrm{End}_{\mathbb{Q}}(E) &\cong \{\lambda \in \mathbb{C} \,\big|\, \lambda(\omega_2(\mathbb{Q}z + \mathbb{Q})) \subset \omega_2(\mathbb{Q}z + \mathbb{Q})\} \\ &\cong \{\lambda \in \mathbb{C} \,\big|\, \lambda\mathbb{Q}(z) \subset \mathbb{Q}(z)\} \\ &\cong \mathbb{Q}(z). \end{aligned}$$

Clearly $\mathrm{End}(E)$ will be isomorphic to an order in $\mathbb{Q}(z)$. □

In these notes we shall for simplicity only consider those CM elliptic curves E such that $\mathrm{End}(E)$ is isomorphic to the maximal order in $\mathbb{Q}(z)$. Fix an imaginary quadratic field K which we shall think of as embedded in $\mathbb{C}$, and denote the maximal order (or the ring of integers) of K by $\mathcal{O}_K$. We

shall say that E has CM by $\mathcal{O}_K$ if $\mathrm{End}(E) \tilde{=} \mathcal{O}_K$. Let ω denote an invariant differential on E. Then there is a unique isomorphism

$$[\ ] : \mathcal{O}_K \tilde{\to} \mathrm{End}(E) \tag{2.3}$$

such that that $[\alpha]^*\omega = \alpha\omega$ (see [3], Chapter 2, Proposition 1.1). In what follows we shall always identify $\mathcal{O}_K$ with $\mathrm{End}(E)$ via (2.3).

3 Classification of CM elliptic curves

Let K be an imaginary quadratic field. Let $Cl(K)$ be the class group of K. Let

$$\begin{aligned} \mathcal{E}_{\mathbb{C}}(K) &= \{\mathbb{C}\text{-isomorphism classes of elliptic curves} \\ &\qquad \text{defined over } \mathbb{C} \text{ with CM by } \mathcal{O}_K\}. \end{aligned}$$

If $\mathfrak{a}$ is a fractional ideal of K then, via the embedding of K into $\mathbb{C}$ that we have implicitly fixed, $\mathfrak{a}$ is a lattice in $\mathbb{C}$. Moreover, by construction, $\mathbb{C}/\mathfrak{a}$ has CM by $\mathcal{O}_K$ since for every $\lambda \in \mathcal{O}_K$ one has $\lambda\mathfrak{a} \subset \mathfrak{a}$. If two fractional ideals are in the same ideal class then it is easy to see that the corresponding elliptic curves are isomorphic. Thus we obtain a map

$$\begin{aligned} Cl(K) &\to \mathcal{E}_{\mathbb{C}}(K) \\ [\mathfrak{a}] &\mapsto \mathbb{C}/\mathfrak{a}. \end{aligned}$$

We leave the proof of the following theorem as an exercise.

Theorem 3.1. *The map above is a bijection.*

We now define an important action of $Cl(K)$ on $\mathcal{E}_{\mathbb{C}}(K)$. Let $[\mathfrak{a}] \in Cl(K)$ and let $\mathbb{C}/\mathfrak{b} \in \mathcal{E}_{\mathbb{C}}(K)$ for a fractional ideal $\mathfrak{b}$ of K. Set

$$[\mathfrak{a}] \cdot \mathbb{C}/\mathfrak{b} = \mathbb{C}/(\mathfrak{a}^{-1}\mathfrak{b}).$$

By the theorem $\cdot$ defines a simply transitive action of $Cl(K)$ on $\mathcal{E}_{\mathbb{C}}(K)$.

4 CM elliptic curves have rational models

Lemma 4.1. *Let E be an elliptic curve with CM by $\mathcal{O}_K$. Then $j(E)$ is an algebraic number. In fact $[\mathbb{Q}(j(E)) : \mathbb{Q}] \leq h_k$ where h_k is the class number of K.*

Proof. Let $\sigma \in \mathrm{Aut}(\mathbb{C})$. Let E^σ denote the elliptic curve with σ applied to the coefficients of a Weierstrass equation for E. Note that $j(E^\sigma) = j(E)^\sigma$. Since $\mathrm{End}(E) \xrightarrow{\sim} \mathrm{End}(E^\sigma)$, we see that E^σ also has CM by $\mathcal{O}_K$. By Theorem 3.1, E^σ belongs to one of finitely many isomorphism classes of elliptic curves. In particular $j(E)^\sigma$ takes on less than h_K values, and is algebraic. □

Let $\mathcal{E}_{\bar{\mathbb{Q}}}(K)$ denote the set of $\overline{\mathbb{Q}}$-isomorphism classes of elliptic curves defined over $\overline{\mathbb{Q}}$ with CM by $\mathcal{O}_K$. We have

Lemma 4.2. *The natural map*

$$\mathcal{E}_{\bar{\mathbb{Q}}}(K) \to \mathcal{E}_{\mathbb{C}}(K)$$

is a bijection.

Proof. If $E \in \mathcal{E}_{\mathbb{C}}(K)$ then there is an elliptic curve E' defined over $\mathbb{Q}(j(E))$ such that $E \xrightarrow{\sim} E'$. Lemma 4.1 shows that $E' \in \mathcal{E}_{\bar{\mathbb{Q}}}(K)$ establishing the surjectivity. For the injectivity, say E, $E' \in \mathcal{E}_{\bar{\mathbb{Q}}}(K)$, with Weierstrass equations $y^2 = 4x^3 - g_2x - g_3$ and $y^2 = 4x^3 - g_2'x - g_3'$ respectively. If $\lambda : E \xrightarrow{\sim} E'$ is an isomorphism defined over $\mathbb{C}$ then (see [1], Proposition 4.1) there is an element $\mu \in \mathbb{C}$ such that $g_2' = \mu^4 g_2$, $g_3' = \mu^6 g_3$ and $\lambda(x, y) = (\mu^2 x, \mu^3 y)$. Since the g_i and the g_i' are in $\overline{\mathbb{Q}}$ we see that $\mu \in \overline{\mathbb{Q}}$. Thus λ is defined over $\overline{\mathbb{Q}}$ establishing the injectivity. □

In the following sections we will usually confuse $\mathcal{E}_{\bar{\mathbb{Q}}}(K)$ with $\mathcal{E}_{\mathbb{C}}(K)$ and simply write $\mathcal{E}(K)$. This is justified by Lemma 4.2 above.

5 Class field theory

In this section we review some terminology and results from class field theory.

Let K be a totally imaginary number field. Recall that there is a notion of a modulus $\mathfrak{m}$ (which, when K is totally imaginary, is just an integral ideal of K). Let $I^{\mathfrak{m}}$ be the group of fractional ideals of K generated by the

prime ideals of K that do not divide $\mathfrak{m}$. Let $K_{\mathfrak{m},1}$ denote the subgroup of $I^{\mathfrak{m}}$ consisting of principal ideals generated by elements α of the form

$$\alpha \equiv 1 \bmod \mathfrak{m}.$$

Let L/K be an abelian extension of K. Then there is a modulus $\mathfrak{m}$ divisible by the primes of K that ramify in L and a surjective homomorphism called the Artin map

$$(\ , L/K) : I^{\mathfrak{m}} \to \mathrm{Gal}(L/K)$$

defined by sending a prime ideal $\mathfrak{p}$ to the corresponding Frobenius element $(\mathfrak{p}, L/K)$ at $\mathfrak{p}$ such that

$$K_{\mathfrak{m},1} \quad \subset \quad \ker(\ , L/K). \tag{5.1}$$

In such case the kernel of the Artin map is known: it is

$$\ker(\ , L/K) \quad = \quad K_{\mathfrak{m},1} \cdot \mathrm{N}_{L/K}(I_L^{\mathfrak{m}}),$$

where $I_L^{\mathfrak{m}}$ is the group of fractional ideals of L generated by the primes of L not lying above the primes dividing $\mathfrak{m}$. The greatest common divisor of the $\mathfrak{m}$ such that (5.1) holds is called the conductor of L/K.

Now let $\mathfrak{m}$ be an arbitrary modulus (integral ideal of $\mathcal{O}_K$). The ray class field modulo $\mathfrak{m}$ is an abelian extension $L_{\mathfrak{m}}$ of K such that the conductor of $L_{\mathfrak{m}}/K$ divides $\mathfrak{m}$ and such that if L/K is an abelian extension whose conductor divide $\mathfrak{m}$ then $L \subset L_{\mathfrak{m}}$. Thus the ray class field modulo $\mathfrak{m}$ is the 'maximal abelian extension of conductor $\mathfrak{m}$'. This has been put in quotes since the ray class field modulo $\mathfrak{m}$ may not itself have conductor $\mathfrak{m}$.

The kernel of the Artin map for the ray class field modulo $\mathfrak{m}$ is especially simple:

$$\ker(\ , L_{\mathfrak{m}}/K) \quad = \quad K_{\mathfrak{m},1}. \tag{5.2}$$

The Artin map thus induces an isomorphism between the ray class group modulo $\mathfrak{m}$ which by definition is

$$\frac{I^{\mathfrak{m}}}{K_{\mathfrak{m},1}}$$

and $\mathrm{Gal}(L_{\mathfrak{m}}/K)$.

Conversely if L/K is a (not necessarily abelian) Galois extension of K and $\mathfrak{m}$ is a modulus such that

$$(\mathfrak{p}, L/K) = 1 \iff \mathfrak{p} \in K_{\mathfrak{m},1} \tag{5.3}$$

for all but finitely many primes $\mathfrak{p}$ of K then $L = L_{\mathfrak{m}}$. This follows since (5.2) and (5.3) imply that, apart from a finite set of primes, the set of primes of K which split completely in L and $L_{\mathfrak{m}}$ are the same, namely the primes in $K_{\mathfrak{m},1}$, whence $L = L_{\mathfrak{m}}$. (For an arbitrary Galois extension, even though the Artin symbol $(\mathfrak{p}, L/K)$ depends on a choice of a prime of L lying over $\mathfrak{p}$, the condition that $(\mathfrak{p}, L/K) = 1$ is independent of this choice).

Note that every abelian extension L/K lies in a ray class field $L_{\mathfrak{m}}$ for some $\mathfrak{m}$: just take $\mathfrak{m}$ to be the conductor of L/K. Thus describing all ray class fields is tantamount to describing all abelian extensions of K.

When $\mathfrak{m} = 1$ the ray class field has a special name: it is called the Hilbert class field of K. We shall denote it by H. From what we have said above H is the maximal unramified abelian extension of K and $\mathrm{Gal}(H/K)$ is just the class group of K. Moreover the prime ideals of K that split completely in H are exactly the principal prime ideals of K.

A group H is said to be a congruence subgroup of level $\mathfrak{m}$ if it satisfies

$$K_{\mathfrak{m},1} \subset H \subset I^{\mathfrak{m}}.$$

The key example of a congruence subgroup is the following: if L/K is a finite abelian extension of K, then $H = \ker(\ , L/K)$ is a congruence subgroup of level $\mathfrak{m}$ for some modulus $\mathfrak{m}$.

We now put an equivalence relation $\sim$ on the set of congruence subgroups. Let $\mathfrak{m}$ and $\mathfrak{m}'$ be two moduli, with $\mathfrak{m}'|\mathfrak{m}$. Then $I^{\mathfrak{m}}$ is a subgroup of $I^{\mathfrak{m}'}$. If H' is a congruence subgroup of level $\mathfrak{m}'$ then there may or may not be a congruence subgroup H of level $\mathfrak{m}$ such that $H = I_K^{\mathfrak{m}} \cap H'$. If this does happen then we say that the congruence subgroup H is the restriction of the congruence subgroup H'. Now say $(H_1, \mathfrak{m}_1)$ and $(H_2, \mathfrak{m}_2)$ are two congruence subgroups. We set $H_1 \sim H_2$, if there exists a modulus $\mathfrak{m}$, with $\mathfrak{m}_i \,\big|\, \mathfrak{m}$ for $i = 1, 2$, such that $I^{\mathfrak{m}} \cap H_1 = I^{\mathfrak{m}} \cap H_2$ as restricted congruence subgroups of level $\mathfrak{m}$.

An ideal group $[H]$ is an equivalence class of congruence subgroups $(H, \mathfrak{m})$ with respect to the equivalence relation $\sim$. Class field theory says that the map

$$L/K \ \mapsto \ [\ker(\ , L/K)]$$

is an inclusion reversing bijection between the set of abelian extensions L of K and the set of ideal groups of K. Here 'inclusion reversing' means that if the abelian extensions L_1 and L_2 correspond to the ideal groups $[H_1]$ and $[H_2]$ respectively, then

$$L_1 \subset L_2 \iff [H_2] \subset [H_1].$$

(Note: $[H_2] \subset [H_1]$ simply means that there are congruence subgroups $H \in [H_2]$ and $H' \in [H_1]$ of the same level such that $H \subset H'$; one needs to check that this is well defined).

6 Hilbert class field of K

Let K be an imaginary quadratic field. The aim of this section is to show that if E is an elliptic curve with CM by $\mathcal{O}_K$ then $j(E)$ generates the Hilbert class field of K.

By Theorem 3.1 we know that $Cl(K)$ acts simply transitively on $\mathcal{E}(K)$. In particular, for each $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/K)$ there is a unique ideal class $[\mathfrak{a}] \in Cl(K)$ such that $E^\sigma \cong [\mathfrak{a}] \cdot E$. This allows us to define a map

$$F : \mathrm{Gal}(\overline{\mathbb{Q}}/K) \;\; \to \;\; Cl(K)$$

via $F(\sigma) = [\mathfrak{a}]$. Thus $F(\sigma)$ is the unique ideal class such that $F(\sigma) \cdot E \cong E^\sigma$.

Proposition 6.1. *We have:*

1. *F does not depend on the choice of $E \in \mathcal{E}(K)$,*
2. *F is a homomorphism.*

Proof. Statement 2) follows easily from 1). Indeed if σ, $\tau \in \mathrm{Gal}(\mathbb{Q}/K)$ then

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

where the last equality follows since $Cl(K)$ is abelian. This shows that $F(\sigma\tau) = F(\sigma)F(\tau)$ proving 2).

Let us prove 1). Let $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$. We claim that

$$([\mathfrak{b}] \cdot E)^\sigma \cong [\mathfrak{b}]^\sigma \cdot E^\sigma, \tag{6.2}$$

for each $[\mathfrak{b}] \in Cl(K)$. Fix a presentation of $\mathfrak{b}$ as an $\mathcal{O}_K$ module:

$$\mathcal{O}_K^m \xrightarrow{A} \mathcal{O}_K^n \to \mathfrak{b} \to 0$$

where A is an $m \times n$ matrix with coefficients in $\mathcal{O}_K$. We remark parenthetically that one can take $n = 2$ since every fractional ideal is generated by two elements. Suppose that $E \cong \mathbb{C}/\mathfrak{c}$ for a fractional ideal $\mathfrak{c}$ of K. Then there is an exact sequence

$$0 \to \mathfrak{c} \to \mathbb{C} \to E \to 0$$

of $\mathcal{O}_K$-modules.

Let Hom denote homomorphisms in the category of $\mathcal{O}_K$-modules. We have the following commutative diagram:

$$\begin{array}{ccccccc}
 & & 0 & & 0 & & 0 \\
 & & \downarrow & & \downarrow & & \downarrow \\
0 & \longrightarrow & \mathrm{Hom}(\mathfrak{b}, \mathfrak{c}) & \longrightarrow & \mathrm{Hom}(\mathfrak{b}, \mathbb{C}) & \longrightarrow & \mathrm{Hom}(\mathfrak{b}, E) \\
 & & \downarrow & & \downarrow & & \downarrow \\
0 & \longrightarrow & \mathrm{Hom}(\mathcal{O}_K^n, \mathfrak{c}) & \longrightarrow & \mathrm{Hom}(\mathcal{O}_K^n, \mathbb{C}) & \longrightarrow & \mathrm{Hom}(\mathcal{O}_K^n, E) \\
 & & \downarrow{\scriptstyle A^t} & & \downarrow{\scriptstyle A^t} & & \downarrow{\scriptstyle A^t} \\
0 & \longrightarrow & \mathrm{Hom}(\mathcal{O}_K^m, \mathfrak{c}) & \longrightarrow & \mathrm{Hom}(\mathcal{O}_K^m, \mathbb{C}) & \longrightarrow & \mathrm{Hom}(\mathcal{O}_K^m, E).
\end{array}$$

Now note that $\mathrm{Hom}(\mathcal{O}_K^r, M) = M^r$ for any integer r and that $\mathrm{Hom}(\mathfrak{b}, M) = \mathfrak{b}^{-1}M$ for any torsion free module $\mathcal{O}_K$-module M (proof: localize!). Thus the above diagram becomes:

$$\begin{array}{ccccccccc}
 & & 0 & & 0 & & 0 & & \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & \mathfrak{b}^{-1}\mathfrak{c} & \longrightarrow & \mathbb{C} & \longrightarrow & \mathrm{Hom}(\mathfrak{b}, E) & & \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & \mathfrak{c}^n & \longrightarrow & \mathbb{C}^n & \longrightarrow & E^n & \longrightarrow & 0 \\
 & & \downarrow{\scriptstyle A^t} & & \downarrow{\scriptstyle A^t} & & \downarrow{\scriptstyle A^t} & & \\
0 & \longrightarrow & \mathfrak{c}^m & \longrightarrow & \mathbb{C}^m & \longrightarrow & E^m & \longrightarrow & 0.
\end{array}$$

The snake lemma now shows that we have an exact sequence:

$$0 \to \mathfrak{b}^{-1}\mathfrak{c} \to \mathbb{C} \xrightarrow{f} \ker(E^n \stackrel{A^t}{\to} E^m) \xrightarrow{g} \mathfrak{c}^m/A^t\mathfrak{c}^n.$$

Let $\ker^0(E^n \stackrel{A^t}{\to} E^m)$ denotes the identity component of the abelian variety $\ker(E^n \stackrel{A^t}{\to} E^m)$. Since $\mathfrak{c}^m/A^t\mathfrak{c}^n$ is a finitely generated discrete $\mathbb{Z}$-module and $\ker^0(E^n \stackrel{A^t}{\to} E^m)$ is infinitely divisible we see that $\ker^0(E^n \stackrel{A^t}{\to} E^m) \subset \ker(g)$. (This would also follow from the continuity of g but I don't see why the connecting homomorphism is continuous). On the other hand since f is continuous and $\mathbb{C}$ is connected we see that $\text{image}(f) = \ker(g)$ is connected. Thus

$$\ker^0(E^n \stackrel{A^t}{\to} E^m) = \ker(g),$$

and we get the exact sequence

$$0 \to \mathfrak{b}^{-1}\mathfrak{c} \to \mathbb{C} \to \ker^0(E^n \stackrel{A^t}{\to} E^m) \to 0.$$

Now

$$\begin{aligned}
([\mathfrak{b}] \cdot E)^\sigma &\cong \left(\ker^0(E^n \stackrel{A^t}{\to} E^m)\right)^\sigma \\
&= \ker^0\left((E^\sigma)^n \stackrel{(A^\sigma)^t}{\to} (E^\sigma)^m\right) \\
&\cong [\mathfrak{b}]^\sigma \cdot E^\sigma,
\end{aligned}$$

proving the claim (6.2).

Now suppose that $\sigma \in \text{Gal}(\overline{\mathbb{Q}}/K)$. Let E_1, E_2 in $\mathcal{E}(K)$ and suppose that $E_1^\sigma \cong [\mathfrak{a}_1] \cdot E_1$ and $E_2^\sigma \cong [\mathfrak{a}_2] \cdot E_2$. We wish to show that $[\mathfrak{a}_1] = [\mathfrak{a}_2]$. Choose $[\mathfrak{b}] \in Cl(K)$ such that $E_2 \cong \mathfrak{b} \cdot E_1$. Then since $[\mathfrak{b}]^\sigma = [\mathfrak{b}]$, (6.2) implies that

$$[\mathfrak{b}] \cdot E_1^\sigma \cong ([\mathfrak{b}] \cdot E_1)^\sigma \cong E_2^\sigma \cong [\mathfrak{a}_2] \cdot E_2 \cong [\mathfrak{a}_2][\mathfrak{b}] \cdot E_1 \cong [\mathfrak{a}_2][\mathfrak{b}][\mathfrak{a}_1]^{-1} \cdot E_1^\sigma.$$

Cancelling $[\mathfrak{b}]$ from both sides we get

$$E_1^\sigma \cong [\mathfrak{a}_2][\mathfrak{a}_1]^{-1} \cdot E_1^\sigma.$$

Since $Cl(K)$ acts simply on $\mathcal{E}(K)$ we get

$$[\mathfrak{a}_1] = [\mathfrak{a}_2],$$

as desired. □

Theorem 6.3. *Let E be an elliptic curve with CM by $\mathcal{O}_K$. Suppose that $E = E_1, \ldots, E_{h_K}$ is a complete set of representatives of $\mathcal{E}(K)$. Then*

1. *$H = K(j(E))$ is the Hilbert class field of K,*
2. *$[\mathbb{Q}(j(E)) : \mathbb{Q}] = [K(j(E)) : K] = h_K$,*
3. *$j(E_1), \ldots, j(E_{h_K})$ is a complete set of conjugates for $j(E)$,*
4. (Reciprocity Law) *Let $j(\mathfrak{c}) := j(\mathbb{C}/\mathfrak{c})$ for a fractional ideal $\mathfrak{c}$ of K. If $\mathfrak{a}$ and $\mathfrak{b}$ are fractional ideals of K then*

$$j(\mathfrak{b})^{(\mathfrak{a}, H/K)} = j(\mathfrak{a}^{-1}\mathfrak{b}).$$

Proof. Let L denote the fixed field of $\ker(F)$. Then $\mathrm{Gal}(\overline{\mathbb{Q}}/L) =$

$$\ker(F) = \{\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/K) \;\big|\; E^\sigma = F(\sigma) \cdot E = E\} = \mathrm{Gal}(\overline{\mathbb{Q}}/K(j(E))).$$

This shows that $L = K(j(E))$. Moreover since F maps $\mathrm{Gal}(L/K)$ injectively into $Cl(K)$ we see that $K(j(E))$ is an abelian extension of K.

Let $\mathfrak{m}$ be the conductor of L/K. Consider the composition π of the Artin map with F:

$$\pi : I^{\mathfrak{m}} \overset{(\ ,L/K)}{\longrightarrow} \mathrm{Gal}(L/K) \overset{F}{\longrightarrow} Cl(K).$$

We claim that π is nothing but the natural projection of $I^{\mathfrak{m}}$ to $Cl(K)$. That is we claim that for each fractional ideal $\mathfrak{a} \in I^{\mathfrak{m}}$,

$$F((\mathfrak{a}, L/K)) = [\mathfrak{a}] \in Cl(K). \tag{6.4}$$

Let us assume that $E_1, \ldots, E_{h_K}$ are defined over $\overline{\mathbb{Q}}$. Choose a large number field M such that M contains K and the fields of definitions of the E_i. It is an exercise (see [3], Chapter 2, Theorem 2.2(b)) to check that any isogeny between E_i and E_j is then automatically defined over M. Fix a finite set S of primes p in $\mathbb{Q}$ containing the set of primes

- p ramifying in M,
- p lying under the set of primes of M at which some E_i has bad reduction, and,

- p dividing $\prod_{i<j} \mathrm{N}_{M/\mathbb{Q}}(j(E_i) - j(E_j))$.

Fix a prime $p \notin S$ which splits in K, say $p = \mathfrak{p}\bar{\mathfrak{p}}$. Let $\mathfrak{a} \subset \mathcal{O}_K$ be an ideal that is relatively prime to p and such that $\mathfrak{a}\mathfrak{p}$ is principal, say $\mathfrak{a}\mathfrak{p} = (\alpha)$. Suppose that $E \stackrel{\sim}{=} \mathbb{C}/\mathfrak{b}$. Then there are isogenies ϕ, ψ and λ such that the following diagram commutes

$$\begin{array}{ccccccc} \mathbb{C}/\mathfrak{b} & \xrightarrow{z\mapsto z} & \mathbb{C}/\mathfrak{p}^{-1}\mathfrak{b} & \xrightarrow{z\mapsto z} & \mathbb{C}/\mathfrak{a}^{-1}\mathfrak{p}^{-1}\mathfrak{b} & \xrightarrow{z\mapsto \alpha z} & \mathbb{C}/\mathfrak{b} \\ \downarrow\sim & & \downarrow\sim & & \downarrow\sim & & \downarrow\sim \\ E & \xrightarrow{\phi} & [\mathfrak{p}]\cdot E & \xrightarrow{\psi} & [\mathfrak{a}]\cdot[\mathfrak{p}]\cdot E & \xrightarrow{\lambda} & E. \end{array}$$

Let ω be an invariant differential on E. Then the above diagram shows that

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

Let $\mathfrak{P}$ denote a prime of M lying over $\mathfrak{p}$. Let $\tilde{}$ denote the reduction of an object mod $\mathfrak{P}$. Then $\tilde{\omega}$ is an invariant differential on $\tilde{E}$. Further since $\alpha \in \mathfrak{p} \subset \mathfrak{P}$, we have

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

By [2], Chapter 2, Theorem 4.2(c), $\tilde{\lambda} \circ \tilde{\psi} \circ \tilde{\phi}$ is inseparable. Since reduction preserves the degree of an isogeny (see [3], Chapter 2, Proposition 4.4) we see that $\deg(\tilde{\psi}) = \deg \psi = \mathrm{N}_{K/\mathbb{Q}}(\mathfrak{a})$ is prime to p and $\deg(\tilde{\lambda}) = \deg(\lambda) = 1$. Thus both $\tilde{\psi}$ and $\tilde{\lambda}$ are separable. Hence $\tilde{\phi} : \tilde{E} \to \widetilde{[\mathfrak{p}]\cdot E}$ must be inseparable. Note that $\deg(\tilde{\phi}) = \deg(\phi) = \mathrm{N}_{K/\mathbb{Q}}(\mathfrak{p}) = p$ so that $\tilde{\phi}$ must be purely inseparable. Now by [2], Chapter 2, Corollary 2.12, we can factor $\tilde{\phi}$ as

$$\tilde{E} \xrightarrow{\mathrm{Frob}_p} \tilde{E}^{(p)} \xrightarrow{\epsilon} \widetilde{[\mathfrak{p}]\cdot E}$$

where Frob_p denotes the p^{th}-power homomorphism and $\epsilon : \tilde{E}^{(p)} \to \widetilde{[\mathfrak{p}]\cdot E}$ is an isomorphism. In particular we have

$$j(\widetilde{[\mathfrak{p}]\cdot E}) = j(\tilde{E}^{(p)}) = j(\tilde{E})^p$$

so that

$$\begin{aligned} &j([\mathfrak{p}]\cdot E) \equiv j(E)^p = \\ &\quad j(E)^{\mathrm{N}_{K/\mathbb{Q}}(\mathfrak{p})} \equiv j(E)^{(\mathfrak{p},L/K)} = j(E^{(\mathfrak{p},L/K)}) \equiv j(F((\mathfrak{p},L/K))\cdot E) \bmod \mathfrak{P}. \end{aligned}$$

By the choice of the set S we get

$$[\mathfrak{p}] \cdot E = F((\mathfrak{p}, L/K)) \cdot E.$$

Thus

$$F((\mathfrak{p}, L/K)) = [\mathfrak{p}] \in Cl(K)$$

for each prime $\mathfrak{p} \subset \mathcal{O}_K$ which does not lie above the primes in S and which has residue degree one. This proves our claim (6.4) for 'half' the prime ideals in $\mathcal{O}_K$. But this is enough to deduce (6.4) for all fractional ideal $\mathfrak{a} \in I^{\mathfrak{m}}$. Indeed a result from class field theory says there is a prime $\mathfrak{p}$ as above and an element $\alpha \in K^*$ with $\alpha \equiv 1 \bmod \mathfrak{m}$ with

$$\mathfrak{a} = (\alpha) \cdot \mathfrak{p}.$$

Since $(\mathfrak{a}, L/K) = (\mathfrak{p}, L/K)$ we get

$$F((\mathfrak{a}, L/K)) = F((\mathfrak{p}, L/K)) = [\mathfrak{p}] = [\mathfrak{a}]$$

establishing (6.4) for all fractional ideals in $I^{\mathfrak{m}}$.

We note that claim (6.4) about π also shows that $F : \mathrm{Gal}(\overline{\mathbb{Q}}/K) \to Cl(K)$ is surjective. Moreover (6.4) shows that

$$F(((\alpha), L/K)) = 1$$

for all principal ideals $(\alpha) \in I^{\mathfrak{m}}$. Since F is injective when restricted to $\mathrm{Gal}(L/K)$,

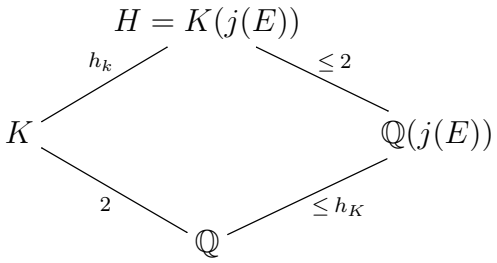
$$((\alpha), L/K) = 1$$

for all $(\alpha) \in I^{\mathfrak{m}}$. But the conductor $\mathfrak{m}$ is the 'largest' (in terms of containment) ideal with the property that

$$\alpha \equiv 1 \bmod \mathfrak{m} \Longrightarrow ((\alpha), L/K) = 1.$$

It follows that $\mathfrak{m} = 1$. This means that L/K is unramified and is therefore contained in the Hilbert class field H of K. But $[L : K] = h_k = [H : K]$, so that $H = L = K(j(E)$, proving 1) and the second equality in 2).

The first equality in 2) follows from Lemma 4.1 and the diagram:



As for 3) note that $Cl(K)$ acts transitively on the set $\{j(E_1), \ldots, j(E_{h_K})\}$ and the map F is defined by identifying the action of $\mathrm{Gal}(\overline{\mathbb{Q}}/K)$ with that of $Cl(K)$. Thus $\mathrm{Gal}(\overline{\mathbb{Q}}/K)$ acts transitively on the set $\{j(E_1), \ldots, j(E_{h_K})\}$ as desired.

Finally 4) is just a restatement of the claim (6.4) which now holds for all fractional ideals $\mathfrak{a}$ since $\mathfrak{m} = 1$. □

The theorem above shows that the $j(E)$ generates an unramified abelian extension of K when $\mathrm{End}(E) \tilde{=} \mathcal{O}_K$. More generally if E is an elliptic curve with $\mathrm{End}(E)$ an arbitrary order of K then it turns out that $j(E)$ generates a not necessarily unramified abelian extension of K.

7 The Weber function

In this section we introduce the Weber function $h : E \to \mathbb{P}^1$ attached to an elliptic curve defined over $\mathbb{C}$. Say E is given by an equation of the form

$$y^2 = 4x^3 - g_2 x - g_3 \quad \text{with } \Delta = g_2^3 - 27g_3^2 \neq 0.$$

If E is an elliptic curve with CM by $\mathcal{O}_K$ then $\mathrm{Aut}(E) = \mathcal{O}_K^\times$ is just the finite group of units of K; otherwise $\mathrm{Aut}(E) = \{\pm 1\}$. One may easily check ([1], Chapter 4.5) that

$$\mathrm{Aut}(E) = \begin{cases} \{\pm 1\} & \text{if } g_2 g_3 \neq 0 \iff j(E) \neq 0, 1728, \\ \{\pm 1, \pm i\} & \text{if } g_3 = 0 \iff j(E) = 1728, \\ \{\pm 1, \pm\omega, \pm\omega^2\} & \text{if } g_2 = 0 \iff j(E) = 0, \end{cases}$$

where $\omega = e^{2\pi i/3}$ is a primitive third root of unity. Let us divide the set of isomorphism classes of elliptic curves over $\mathbb{C}$ into three classes: $\mathcal{E}_i$ for $i = 1$,

2, 3, where $E \in \mathcal{E}_i$ if $\mathrm{Aut}(E)$ has $2i$ automorphisms. One can write down the automorphisms in each case explicitly:

$$\mathrm{Aut}(E) \ni \begin{cases} (x,y) \mapsto (x, \pm y) & \text{if } E \in \mathcal{E}_1, \\ (x,y) \mapsto (x, \pm y), (-x, \pm iy) & \text{if } E \in \mathcal{E}_2, \\ (x,y) \mapsto (\omega^\nu x, \pm y) \text{ with } \nu = 0,1,2, & \text{if } E \in \mathcal{E}_3. \end{cases} \tag{7.1}$$

Now define

$$h : E \to \mathbb{P}^1$$

by

$$h(x,y) = \begin{cases} (g_2 g_3/\Delta) \cdot x & \text{if } E \in \mathcal{E}_1, \\ (g_2^2/\Delta) \cdot x^2 & \text{if } E \in \mathcal{E}_2, \\ (g_3/\Delta) \cdot x^3 & \text{if } E \in \mathcal{E}_3. \end{cases}$$

Note that h is defined over any field of definition of E. The following lemmas about h will be useful.

Lemma 7.2. *Let E be an elliptic curve defined over $\mathbb{C}$. Let P, $P' \in E$. Then*

$$h(P') = h(P) \iff P' = \epsilon P \text{ for some } \epsilon \in \mathrm{Aut}(E).$$

Proof. Say $E \in \mathcal{E}_i$. Let $P = (x,y)$ and $P' = (x',y')$. Then $h(P) = h(P') \iff x^i = x'^i$. When $i = 1$, we get $y^2 = y'^2$, so that $(x',y') = (x, \pm y)$. By (7.1) we have $P' = \epsilon P$ for $\epsilon \in \mathrm{Aut}(E)$ as desired. The cases $i = 2$ and $i = 3$ are proved similarly using (7.1) above. □

Lemma 7.3. *Let E and E' be elliptic curves defined over $\mathbb{C}$. Let $\epsilon : E \to E'$ be an isomorphism. Then*

$$h_E = h_{E'} \circ \epsilon.$$

Proof. Say E has model $y^2 = 4x^3 - g_2 x - g_3$ and E' has model $y^2 = 4x^3 - g_2' x - g_3'$. By [1], Proposition 4.1 one may find $\mu \in \mathbb{C}$ such that $\epsilon(x,y) = (\mu^2 x, \mu^3 y)$ and such that $g_2' = \mu^4 g_2$, $g_3' = \mu^6 g_3$. Then the lemma follows immediately from the definition of h given above. □

Ultimately we wish to generate abelian extensions of K by adjoining the coordinates of the torsion points of an elliptic curve $E \in \mathcal{E}(K)$. If E is defined over $\mathbb{C}$ (and not $\overline{\mathbb{Q}}$) there is no reason why these coordinates need even be algebraic. However if P is a such a torsion point then $h_E(P)$ is necessarily algebraic. Indeed we may always choose an elliptic curve E' defined over $\overline{\mathbb{Q}}$ such that $\epsilon : E \xrightarrow{\sim} E'$. By the lemma above $h_E(P) = h_{E'}(\epsilon(P))$ which is clearly algebraic. This is one of the main reasons for introducing the Weber function.

8 Ray class fields of K

In this section we show how we can use the Weber values of the $\mathfrak{m}$-torsion points of an elliptic curve with CM by $\mathcal{O}_K$ to generate the ray class field modulo $\mathfrak{m}$ of K where $\mathfrak{m} \subset \mathcal{O}_K$ is an arbitrary modulus. We start with the following observation.

Proposition 8.1. *Let E be an elliptic curve with CM by $\mathcal{O}_K$ defined over H. Then*

$$K(j(E), E_{\text{tors}})$$

is an abelian extension of $H = K(j(E))$.

Proof. Let $\mathfrak{m} \subset \mathcal{O}_K$ be an ideal. It suffices to show that $L = K(j(E), E[\mathfrak{m}])$ is an abelian extension of H. Note that every element of $\text{End}(E)$ is defined over H. So if $\sigma \in \text{Gal}(L/H)$, $P \in E[\mathfrak{m}]$ and $\alpha \in \mathcal{O}_K$, then

$$([\alpha]P)^\sigma = [\alpha]^\sigma(P^\sigma) = [\alpha](P^\sigma). \tag{8.2}$$

In particular we have a Galois representation

$$\rho : \text{Gal}(L/H) \hookrightarrow \text{Aut}(E[\mathfrak{m}]).$$

Moreover (8.2) shows that the image of ρ lies in the ring of $\mathcal{O}_K/\mathfrak{m}$-linear endomorphisms of $E[\mathfrak{m}]$. Since $E[\mathfrak{m}] \cong \mathfrak{m}^{-1}\mathcal{O}_K/\mathcal{O}_K$ is a free $\mathcal{O}_K/\mathfrak{m}$-module of rank one, $\text{End}_{\mathcal{O}_K/\mathfrak{m}}(E[\mathfrak{m}]) = \mathcal{O}_K/\mathfrak{m}$. Thus

$$\rho : \text{Gal}(L/H) \hookrightarrow (\mathcal{O}_K/\mathfrak{m})^*$$

which shows that $\text{Gal}(L/H)$ is abelian. □

Let E be an elliptic curve with CM by $\mathcal{O}_K$ defined over H. It is not true in general that $K(j(E), E_{\text{tors}})$ is an abelian extension of K. However if we let

$$h : E \to \mathbb{P}^1$$

be the Weber function defined in Section 7 (note that h is now defined over H as well) then we have the following theorem.

Theorem 8.3. *Let E be an elliptic curve defined over H with CM by $\mathcal{O}_K$. Let $\mathfrak{m} \subset \mathcal{O}_K$ be an ideal, and let $E[\mathfrak{m}]$ denote the $\mathfrak{m}$-torsion points of E. Then*

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

is the ray class field of K modulo $\mathfrak{m}$.

We first prove the following proposition. Let $\mathfrak{p}$ be a prime of K. Let Let M and $\mathfrak{P}$ be as in the proof of Theorem 6.3. So $\mathfrak{P}$ is a prime of M lying above $\mathfrak{p}$. Let $\tilde{}$ denotes reduction modulo $\mathfrak{P}$. We have:

Proposition 8.4. *Let E be an elliptic curve defined over H with CM by $\mathcal{O}_K$. For all but finitely many prime ideals $\mathfrak{p}$ of K of degree 1 satisfying $(\mathfrak{p}, H/K) = 1$ there is an element $\pi_{\mathfrak{p}} \in \mathcal{O}_K$ such that $\mathfrak{p} = (\pi_{\mathfrak{p}})$ and the diagram*

$$\begin{array}{ccc} E & \xrightarrow{[\pi_{\mathfrak{p}}]} & E \\ \downarrow & & \downarrow \\ \tilde{E} & \xrightarrow{\text{Frob}_p} & \tilde{E} \end{array} \tag{8.5}$$

commutes.

Proof. Let $\sigma = (\mathfrak{p}, H/K)$. Assume that $\mathfrak{p}$ does not lie above the finite set S of primes defined in the proof of Theorem 6.3 and that $\mathrm{N}_{K/\mathbb{Q}} = p$. Then the proof of Theorem 6.3 shows that there is an isogeny $\phi : E \to E^\sigma$ and an isomorphism $\epsilon : \tilde{E}^{(p)} \to \widetilde{E^\sigma}$ making the following diagram commute

$$\begin{array}{ccccc} E & & \xrightarrow{\phi} & & E^\sigma \\ \downarrow & & & & \downarrow \\ \tilde{E} & \xrightarrow{\text{Frob}_p} & \tilde{E}^{(p)} & \xrightarrow{\epsilon} & \widetilde{E^\sigma}. \end{array}$$

Note that $\tilde{E}^{(p)} = \widetilde{E^\sigma}$ so that ϵ is an automorphism of $\widetilde{E^\sigma}$. There is a natural injection (see [3], Chapter 2, Proposition 4.4)

$$\mathrm{End}(E^\sigma) \hookrightarrow \mathrm{End}(\widetilde{E^\sigma}), \tag{8.6}$$

which in the present situation is surjective as well. Indeed a result of Deuring shows that the $\mathbb{Q}$-span of the endomorphism algebra of an elliptic curve defined over a finite field of characteristic p is either a quadratic field or the quaternion algebra D over $\mathbb{Q}$ ramified at p and ∞. If $\mathrm{End}_{\mathbb{Q}}(\widetilde{E^\sigma}) = D$ then $D \otimes \mathbb{Q}_p$ would contain $K \otimes \mathbb{Q}_p = \mathbb{Q}_p \times \mathbb{Q}_p$ which contains zero divisors, a contradiction. Thus $\mathrm{End}_{\mathbb{Q}}(\widetilde{E^\sigma}) = K$. In other words (8.6) is an isomorphism after tensoring with $\mathbb{Q}$. Since $\mathrm{End}(E^\sigma)$ is the maximal order (8.6) is itself an isomorphism. This means that one can pick $\epsilon_0 \in \mathrm{End}(E^\sigma)$ with $\tilde{\epsilon}_0 = \epsilon$. Clearly $\epsilon_0 \in \mathrm{Aut}(E^\sigma)$. Replacing ϕ in the diagram above with $\epsilon_0^{-1} \circ \phi$ we obtain a commutative diagram

$$\begin{array}{ccc} E & \xrightarrow{\phi} & E^\sigma \\ \downarrow & & \downarrow \\ \tilde{E} & \xrightarrow{\mathrm{Frob}_p} & \tilde{E}^{(p)}. \end{array}$$

(S. Kobayashi has pointed out an alternative way to see that ϵ lifts to characteristic 0 which avoids Deuring's result but at the cost of throwing away finitely many primes. We wish to show that

$$\mathrm{Aut}(E^\sigma) \hookrightarrow \mathrm{Aut}(\widetilde{E^\sigma}) \tag{8.7}$$

is an isomorphism. Let us assume that $p \neq 2, 3$. Then it is well known that

$$|\mathrm{Aut}(\widetilde{E^\sigma})| = \begin{cases} 2 & \text{if } j(\widetilde{E^\sigma}) \neq 0, 1728, \\ 4 & \text{if } j(\widetilde{E^\sigma}) = 1728, \\ 6 & \text{if } j(\widetilde{E^\sigma}) = 0. \end{cases}$$

If $j(E^\sigma) = 1728$, respectively 0, then $|\mathrm{Aut}(E^\sigma)| = 4$, respectively 6, forcing (8.7) to be an isomorphism. So we may assume that $j(E^\sigma) \neq 0, 1728$. Then if $p \nmid 1728 \cdot j(E) \cdot (1728 - j(E))$, one has $|\mathrm{Aut}(\widetilde{E^\sigma})| = 2$, so that (8.7) is again an isomorphism.)

We now use the additional hypothesis $\sigma = (\mathfrak{p}, H/K) = 1$ to get $E^\sigma = E$ and $\tilde{E}^{(p)} = \tilde{E}$. This means that $\phi \in \mathrm{End}(E)$ and so $\phi = [\pi_{\mathfrak{p}}]$, for some $\pi_{\mathfrak{p}} \in \mathcal{O}_K$. Note that

$$\mathrm{N}_{K/\mathbb{Q}}(\pi_{\mathfrak{p}}) = \deg([\pi_{\mathfrak{p}}]) = \deg(\mathrm{Frob}_p) = p,$$

and since $\mathfrak{p}$ is principal, $\mathfrak{p} = (\pi_\mathfrak{p})$ or $\mathfrak{p} = (\bar{\pi}_\mathfrak{p})$. To see that it is the former note that

$$\widetilde{\pi_\mathfrak{p}}\tilde{\omega} = \widetilde{\pi_\mathfrak{p}\omega} = \widetilde{[\pi_\mathfrak{p}]^*\omega} = \widetilde{[\pi_\mathfrak{p}]}^*\tilde{\omega} = \mathrm{Frob}_p^*\tilde{\omega} = 0,$$

where the last equality follows from the fact that Frob_p is inseparable. This shows that $\tilde{\pi}_\mathfrak{p} = 0$ and so $\pi_\mathfrak{p} \in \mathfrak{P} \cap K = \mathfrak{p}$. □

Proof of Theorem 8.3. Let

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

To show that L is the the ray class field modulo $\mathfrak{m}$ it suffices to show that

$$(\mathfrak{p}, L/K) = 1 \iff \mathfrak{p} \in K_{\mathfrak{m},1}, \tag{8.8}$$

since (8.8) characterizes the ray class field modulo $\mathfrak{m}$ (see the discussion in Section 5). As we have seen in the proof of Theorem 6.3, it suffices to prove (8.8) for all but finitely many primes $\mathfrak{p}$ of residue degree one.

So suppose that $\mathfrak{p}$ is a prime of residue degree one and that $(\mathfrak{p}, L/K) = 1$. Then $(\mathfrak{p}, H/K) = 1$ since it is the restriction of $(\mathfrak{p}, L/K)$ to H. So by Proposition 8.4, after eliminating from consideration finitely many $\mathfrak{p}$, there is an element $\pi_\mathfrak{p} \in \mathcal{O}_K$ such that $\mathfrak{p} = (\pi_\mathfrak{p})$ and such that the diagram (8.5) commutes.

Let $F = K(j(E), E[\mathfrak{m}])$. This is a (not necessarily abelian) Galois extension of K. Fix a prime $\mathfrak{Q}$ of F lying above $\mathfrak{p}$ and let $\sigma \in \mathrm{Gal}(F/K)$ denote the corresponding Frobenius element. Note that σ restricted to L is just $(\mathfrak{p}, L/K) = 1$.

Denote by $\tilde{}$ reduction modulo $\mathfrak{Q}$. Reducing $h : E \to E/\mathrm{Aut}(E) = \mathbb{P}^1$ modulo $\mathfrak{Q}$, we get a map

$$\tilde{h} : \tilde{E} \to \tilde{E}/\widetilde{\mathrm{Aut}E}.$$

Let $P \in E[\mathfrak{m}]$ be an $\mathfrak{m}$-torsion point of E. We compute

$$\tilde{h}(\tilde{[\pi_\mathfrak{p}]}\tilde{P}) = \tilde{h}(\widetilde{[\pi_\mathfrak{p}]P}) = \tilde{h}(\mathrm{Frob}_p(\tilde{P})) \quad \text{by (8.5)},$$

so that

$$\begin{aligned}
\tilde{h}(\tilde{[\pi_{\mathfrak{p}}]}\tilde{P}) &= \tilde{h}(\widetilde{P^{\sigma}}) \\
&= \widetilde{h(P^{\sigma})} \\
&= \widetilde{h(P)^{\sigma}} \quad \text{since } \sigma = 1 \text{ on } H \text{ and } h \text{ is defined over } H \\
&= \widetilde{h(P)} \quad \text{since } \sigma = 1 \text{ on } L \\
&= \tilde{h}(\tilde{P}).
\end{aligned}$$

Thus there exists an element $[\xi] \in \mathrm{Aut}(E)$ such that

$$\tilde{[\pi]}\tilde{P} = \tilde{[\xi]}\tilde{P}.$$

Now the reduction map $E \to \tilde{E}$ is injective on $\mathfrak{m}$-torsion points whose order is prime to p (see [2], Chapter 7, Proposition 3.1(b)). So if we discard the primes p that divide $N_{K/\mathbb{Q}}(\mathfrak{m})$ then

$$E[\mathfrak{m}] \hookrightarrow \tilde{E}[\mathfrak{m}] \tag{8.9}$$

is injective. Thus we get that

$$[\pi_{\mathfrak{p}} - \xi]P = 0.$$

The same ξ works for all $P \in E[\mathfrak{m}]$ since we may assume that P is a generator of the free rank one $\mathcal{O}_K/\mathfrak{m}$-module $E[\mathfrak{m}]$. This shows that

$$\pi_{\mathfrak{p}} \equiv \xi \bmod \mathfrak{m},$$

and $\mathfrak{p} = (\xi^{-1}\pi_{\mathfrak{p}}) \in K_{\mathfrak{m},1}$ as desired.

Conversely suppose that $\mathfrak{p}$ is a degree one prime of K and that $\mathfrak{p} \in K_{\mathfrak{m},1}$. Say $\mathfrak{p} = (\alpha)$ with $\alpha \equiv 1 \bmod \mathfrak{m}$. Since $\mathfrak{p}$ is principal we have $(\mathfrak{p}, H/K) = 1$. By Proposition 8.4 again, after discarding finitely many $\mathfrak{p}$, we may assume that there is a $\pi_{\mathfrak{p}} \in \mathcal{O}_K$ such that $\mathfrak{p} = (\pi_{\mathfrak{p}})$ and such that (8.5) commutes. Note that since $(\pi_{\mathfrak{p}}) = (\alpha)$ there is a unit $\xi \in \mathcal{O}_K^{\times}$ such that $\pi_{\mathfrak{p}} = \xi\alpha$.

Let F, $\mathfrak{Q}$ and σ be as above and denote reduction modulo $\mathfrak{Q}$ by $\tilde{\ }$. Let $P \in E[\mathfrak{m}]$. We have

$$\widetilde{P^{\sigma}} = \mathrm{Frob}_p(\tilde{P}) = \widetilde{[\pi_{\mathfrak{p}}]P} \quad \text{by (8.5)}.$$

Again by discarding finitely many $\mathfrak{p}$ and using (8.9) we get $P^\sigma = [\pi]P$. Hence

$$\begin{aligned} h(P)^{(\mathfrak{p},L/K)} &= h(P^\sigma) && \text{since } (\mathfrak{p}, H/K) = 1 \text{ and } h \text{ is defined over } H \\ &= h([\pi_\mathfrak{p}]P) && \text{by the remarks above} \\ &= h([\xi] \circ [\alpha]P) && \text{since } \pi_\mathfrak{p} = \xi\alpha \\ &= h([\alpha]P) && \text{by Lemma 7.2 and since } [\xi] \in \mathrm{Aut}(E) \\ &= h(P) && \text{since } \alpha = 1 + m,\ m \in \mathfrak{m}, \text{ and } [1+m]P = P. \end{aligned}$$

This shows that $(\mathfrak{p}, L/K) = 1$ since it fixes both $j(E)$ and $h(P)$ for all $P \in E[\mathfrak{m}]$, proving the converse. □

9 Main theorem of complex multiplication

We now state the main theorem of complex multiplication. It is stated using the idelic formulation of class field theory. We do not explain this here nor do we give the proof of the main theorem as we do not need it. On the other hand, after the arguments of the previous sections the proof of the main theorem is not difficult. In fact in Shimura [1] the main theorem is proved first, and then Theorems 6.3 and 8.3 are derived as corollaries of it.

Theorem 9.1. *Let E be an elliptic curve with CM by $\mathcal{O}_K$. Let $f : \mathbb{C}/\mathfrak{a} \to E$ be a fixed isomorphism. Let $\sigma \in \mathrm{Aut}(\mathbb{C})$, and say $s \in \mathbb{A}_K^\times$ is such that the restriction of σ to K^{ab} is $(s, K^{\mathrm{ab}}/K)$. Then there is a unique isomorphism*

$$f : \mathbb{C}/s^{-1}\mathfrak{a} \to E^\sigma$$

such that the following diagram is commutative:

$$\begin{array}{ccc} K/\mathfrak{a} & \xrightarrow{\quad f \quad} & E \\ \downarrow{\scriptstyle s^{-1}} & & \downarrow{\scriptstyle \sigma} \\ K/s^{-1}\mathfrak{a} & \xrightarrow{\quad f' \quad} & E^\sigma. \end{array}$$

Proof. See [1], Theorem 5.4.

10 Integrality of $j(E)$

In Lemma 4.1 we showed that the j-invariant of an elliptic curve E with CM by $\mathcal{O}_K$ is an algebraic number of degree at most h_K. More is true:

Theorem 10.1. *Let E be an elliptic curve with CM. Then $j(E)$ is an algebraic integer.*

Proof. An elementary but slightly involved proof of this fact can be found in [1], Chapter 4.6. Here we briefly sketch a more conceptual proof (see [3], Chapter 2 for further details). It is a fact that the CM elliptic curve E has potentially good reduction (not just potentially semi-stable reduction) at ALL primes. Since $j(E)$ is integral at a prime of (potentially) good reduction, we are done. □

Let us give an amusing consequence of the above theorem: we will explain why the transcendental number

$$e^{\pi\sqrt{163}} = 262537412640768743.99999999999925007....$$

is almost an integer. Note that $K = \mathbb{Q}(\sqrt{-163})$ is the 'largest' imaginary quadratic field of class number 1. By the above theorem we get

$$j\left(\frac{1+\sqrt{-163}}{2}\right) \in \mathbb{Z}.$$

The leading term in the q-expansion of j is

$$\frac{1}{q} = -e^{\pi\sqrt{163}}.$$

We now leave it to the reader to check that the remaining terms in the q-expansion of $j(\frac{1+\sqrt{-163}}{2})$ other than the constant term 744 are very small, explaining why $e^{\pi\sqrt{163}}$ is almost an integer.

References

[1] G. Shimura. *Introduction to the arithmetic theory of automorphic functions.* Princeton Univ. Press, Princeton, 1971.

[2] J. Silverman. *Arithmetic of elliptic curves, GTM 106.* Springer-Verlag, New York, 1986.

[3] J. Silverman. *Advanced topics in the arithmetic of elliptic curves, GTM 151.* Springer-Verlag, New York, 1994.