Elliptic curves with complex multiplication (CM) and class field theory

Asimina S. Hamakiotes

University of Connecticut

Oct. 16 2023

Introduction

How do we build abelian extensions of number fields? Our goal:

Theorem

Let K be an imaginary quadratic field with ring of integers $\mathcal{O}_K$. Let E be an elliptic curve with $\mathrm{End}(E) \cong \mathcal{O}_K$ and let $\mathfrak{c} \subset \mathcal{O}_K$ be a nonzero ideal. Let h be a Weber function for $E/K(j(E))$. Then

(1) $K(j(E))$ *is the Hilbert class field of* K,

(2) $K(j(E), E_{tors})$ *is an abelian extension of* $K(j(E))$,

(3) $K(j(E), h(E[\mathfrak{c}]))$ *is the ray class field of* K *modulo* $\mathfrak{c}$,

(4) $K(j(E), h(E_{tors}))$ *is the maximal abelian extension of* K.

Background

Let K be a totally complex number field and let L be a finite abelian extension of K, i.e., L/K is Galois with abelian Galois group.

Let $\mathcal{O}_K$ and $\mathcal{O}_L$ be the rings of integers of K and L.

Let $\mathfrak{p}$ be a prime of K unramified in L and $\mathfrak{P}$ be a prime of L over $\mathfrak{p}$.

$$\begin{array}{ccccc} L & \qquad & \mathfrak{P} & \qquad & \mathcal{O}_L/\mathfrak{P} \\ \Big| & & \Big| & & \Big| \\ K & & \mathfrak{p} & & \mathcal{O}_K/\mathfrak{p} \end{array}$$

We have the homomorphism

$$\{\sigma \in \mathrm{Gal}(L/K) : \sigma(\mathfrak{P}) = \mathfrak{P}\} \to \mathrm{Gal}((\mathcal{O}_L/\mathfrak{P})/(\mathcal{O}_K/\mathfrak{p})),$$
$$\sigma \mapsto (\overline{x} \mapsto \overline{\sigma(x)})$$

where the Galois group of residue fields is cyclic, generated by the Frobenius automorphism $x \mapsto x^{N(\mathfrak{p})}$ for $x \in \mathcal{O}_L/\mathfrak{P}$.

Artin map

When $\mathfrak{p}$ in K is unramified in L, there is a unique $\sigma_{\mathfrak{p}} \in \mathrm{Gal}(L/K)$ which maps to the Frobenius of $\mathfrak{P}$ over $\mathfrak{p}$, determined by the condition

$$\sigma_{\mathfrak{p}}(x) \equiv x^{N(\mathfrak{p})} \bmod \mathfrak{P} \quad \text{for all } x \in \mathcal{O}_L.$$

Let $\mathfrak{c}$ be an integral ideal of K divisible by all primes that ramify in L/K and $I(\mathfrak{c})$ be the group of fractional ideals of K relatively prime to $\mathfrak{c}$.

The *Artin map* $(\cdot, L/K) : I(\mathfrak{c}) \to \mathrm{Gal}(L/K)$, sends each $\mathfrak{a} \in I(\mathfrak{c})$ to

$$(\mathfrak{a}, L/K) = \left(\prod_{\mathfrak{p}} \mathfrak{p}^{n_{\mathfrak{p}}}, L/K\right) := \prod_{\mathfrak{p}} \sigma_{\mathfrak{p}}^{n_{\mathfrak{p}}}.$$

In other words, each prime $\mathfrak{p} \nmid \mathfrak{c}$ goes to $\sigma_{\mathfrak{p}}$ and extend this multiplicatively.

<u>Note:</u> the Artin map is surjective.

Artin reciprocity and conductor

Theorem (Artin Reciprocity)

Let L/K be a finite abelian extension of number fields. If an ideal $\mathfrak{c} \subset \mathcal{O}_K$ is sufficiently divisible by the primes of K that ramify in L, then

$$((\alpha), L/K) = 1 \quad \textit{for all } \alpha \in K^* \textit{ satisfying } \alpha \equiv 1 \bmod \mathfrak{c}.$$

When $\mathfrak{c} = \prod_{\mathfrak{p}} \mathfrak{p}^{e_{\mathfrak{p}}}$, the condition "$\alpha \equiv 1 \bmod \mathfrak{c}$" means for each $\mathfrak{p} \mid \mathfrak{c}$ that

$$\mathrm{ord}_{\mathfrak{p}}(\alpha - 1) \geq e_{\mathfrak{p}}.$$

If the above is true for integral ideals $\mathfrak{c}_1$ and $\mathfrak{c}_2$, then it also true for $\mathfrak{c}_1 + \mathfrak{c}_2$. Therefore, there is a largest ideal $\mathfrak{c}_{L/K}$ for which the above is true, and we call this ideal the *conductor* of the abelian extension L/K.

Note: all primes in K ramifying in L divide $\mathfrak{c}_{L/K}$.

Principal fractional ideals

We define the group of principal fractional ideals that are 1 modulo $\mathfrak{c}$ as

$$P(\mathfrak{c}) = \{(\alpha) : \alpha \in K^*, \alpha \equiv 1 \bmod \mathfrak{c}\}.$$

<u>Note:</u> an ideal (α) may be in $P(\mathfrak{c})$ even if $\alpha \not\equiv 1 \bmod \mathfrak{c}$, as long as there exists some unit $u \in \mathcal{O}_K^*$ such that $u\alpha \equiv 1 \bmod \mathfrak{c}$.

Example

Let $K = \mathbb{Q}$, so $\mathcal{O}_K = \mathbb{Z}$. Consider

$$P((6)) = \{(\alpha) : \alpha \in \mathbb{Q}^*, \alpha \equiv 1 \bmod 6\}.$$

Observe that

$$5 \not\equiv 1 \bmod 6,$$

but $(5) \in P((6))$, because $(5) = (-5)$ as ideals and

$$-5 \equiv 1 \bmod 6.$$

Kernel of the Artin map

Artin reciprocity tells us that for appropriate $\mathfrak{c}$, the kernel of the Artin map contains $P(\mathfrak{c})$:

$$(\alpha) \in P(\mathfrak{c}_{L/K}) \Rightarrow ((\alpha), L/K) = 1.$$

Let $\mathfrak{p}$ be a prime of K which is unramified in L. Then

$$\begin{aligned} \mathfrak{p} \text{ splits completely in } L &\Leftrightarrow \text{ the extension of residue fields has degree } 1, \\ &\Leftrightarrow (\mathfrak{p}, L/K) = 1. \end{aligned}$$

Thus, when $\mathfrak{c} = \mathfrak{c}_{L/K}$, the unramified prime ideals in the kernel of the Artin map on $I(\mathfrak{c})$ are precisely the primes of K that split completely in L.

The kernel of the Artin map is $N_{\mathfrak{c}}(L/K)P(\mathfrak{c})$, where

$$N_{\mathfrak{c}}(L/K) = \{\mathfrak{a} \subset K : \mathfrak{a} = N_{L/K}(\mathfrak{A}) \text{ for some frac. ideal } \mathfrak{A} \text{ in } L,\ \mathfrak{a} \in I(\mathfrak{c})\}.$$

When $\mathfrak{c} = (1)$, the kernel of the Artin map is $N_{(1)}(L/K)P((1)) = P((1))$, which is all principal fractional ideals.

Ray class field definition

Definition

Let $\mathfrak{c}$ be an integral ideal of K. The *ray class field of K modulo* $\mathfrak{c}$ is a finite abelian extension $K_{\mathfrak{c}}/K$ with the property that for any finite abelian extension L/K,

$$\mathfrak{c}_{L/K} \mid \mathfrak{c} \Rightarrow L \subset K_{\mathfrak{c}}.$$

Intuitively, the ray class field $K_{\mathfrak{c}}$ is the "largest" abelian extension of conductor dividing $\mathfrak{c}$ (the conductor need not be $\mathfrak{c}$).

Ray class field definition

When L/K is Galois, the set $\mathrm{Spl}(L/K)$ of primes in K that split in L has density $1/[L:K]$.

Theorem (Bauer)

Let L_1 and L_2 be finite Galois extensions of a number field K. Then

$$L_1 \subset L_2 \quad \Longleftrightarrow \quad \mathrm{Spl}(L_2/K) \subset \mathrm{Spl}(L_1/K).$$

In particular, $L_1 = L_2$ if and only if $\mathrm{Spl}(L_1/K) = \mathrm{Spl}(L_2/K)$.

Proposition

The ray class field of K modulo $\mathfrak{c}$, denoted $K_{\mathfrak{c}}$, is the finite abelian extension of K such that

$$\mathrm{Spl}(K_{\mathfrak{c}}/K) \;=\; \{\mathfrak{p} = (\alpha) : \alpha \equiv 1 \bmod \mathfrak{c}\},$$

where $\mathrm{Spl}(K_{\mathfrak{c}}/K)$ is the set of primes in K that split completely in $K_{\mathfrak{c}}$.

Ray class field example

Example

Let $K = \mathbb{Q}(i)$, so $\mathcal{O}_K = \mathbb{Z}[i]$. We will show the ray class field of $\mathbb{Q}(i)$ modulo $(4) = (1+i)^4$ is $\mathbb{Q}(i, \sqrt{2}) = \mathbb{Q}(\zeta_8)$.

To prove this, we will check that for $\mathfrak{p} \subset \mathcal{O}_K$ such that $\mathfrak{p} \nmid (1+i)^4$,

$$\mathfrak{p} \in \mathrm{Spl}(\mathbb{Q}(i)_{(4)}/\mathbb{Q}(i)) \iff \mathfrak{p} = (\pi) \text{ such that } \pi \equiv 1 \bmod (1+i)^4.$$

$\mathrm{Spl}(\mathbb{Q}(i)_{(4)}/\mathbb{Q}(i))$ includes all ideals (p) for prime $p \in \mathbb{Z}^+$ such that $p \equiv 3 \bmod 4$, since $(p) = (-p)$ and $-p \equiv 1 \bmod 4$.

A Gaussian prime (π) lying over a prime number that's 1 mod 4 might not have a generator that is 1 mod 4. For example, $(\pi) = (1+2i)$.

Note $\left(\mathbb{Z}[i]/(1+i)^4\right)^* = \{\pm 1, \pm i, \pm 1 + 2i, 2 \pm i \bmod (1+i)^4\}$. Of these, only $\{\pm 1, \pm i \bmod (1+i)^4\}$ can contain generators of prime ideals that are 1 mod 4, so only $4/8 = 1/2$ of Gaussian primes split in $\mathbb{Q}(i, \sqrt{2})$.

Ray class field example

Example (cont'd)

Since half the prime ideals in $\mathbb{Z}[i]$ split completely in $\mathbb{Q}(i)_{(4)}$, the set of Gaussian primes that split in $\mathbb{Q}(i)_{(4)}$ has density $1/2$, so

$$\frac{1}{[\mathbb{Q}(i)_{(4)} : \mathbb{Q}(i)]} = \frac{1}{2} \quad \Longrightarrow \quad [\mathbb{Q}(i)_{(4)} : \mathbb{Q}(i)] = 2.$$

We want to show $\mathbb{Q}(i)_{(4)} = \mathbb{Q}(i, \sqrt{2})$ is the correct quadratic extension.

Since $\mathbb{Q}(i, \sqrt{2}) = \mathbb{Q}(i, \sqrt{i})$, for odd prime (π) in $\mathbb{Z}[i]$, one can show

$$\begin{aligned} \pi \equiv 1 \bmod (4) &\implies (\pi) \text{ splits in } \mathbb{Q}(i, \sqrt{2}), \\ &\iff x^2 - i \bmod \pi \text{ splits}, \\ &\iff N(\pi) \equiv 1 \bmod 8. \end{aligned}$$

Thus, by Bauer's theorem, $\mathbb{Q}(i, \sqrt{2})$ is the ray class field of $\mathbb{Q}(i)_{(4)}$.

Hilbert class field definition

Definition

The ray class field of K modulo (1) is the maximal abelian extension of K unramified at all primes in K. We call it the *Hilbert class field of* K and denote it by $H = K_{(1)}$.

Observe that

$$I((1)) = \{\text{all nonzero fractional ideals of } K\},$$
$$P((1)) = \{\text{all nonzero principal ideals of } K\},$$

and $I((1))/P((1)) \cong \mathcal{CL}(\mathcal{O}_K)$ by definition. Thus, the Artin map on $I((1))$ induces the following isomorphism

$$(\cdot, H/K) : \mathcal{CL}(\mathcal{O}_K) \to \mathrm{Gal}(H/K).$$

Theorem (Dirichlet's Theorem on primes in arithmetic progression)

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

Hilbert class field example

Example (Hilbert class field of $K = \mathbb{Q}(\sqrt{-5})$)

Observe that $K = \mathbb{Q}(\sqrt{-5})$ has class number 2, so the Hilbert class field H of K must be a degree 2 extension of K. In fact, $H = \mathbb{Q}(\sqrt{-5}, i)$.

$$\begin{tikzcd} & \mathbb{Q}(\sqrt{-5}, i) \arrow[dl, dash, "2"'] \arrow[d, dash] \arrow[dr, dash] & \\ \mathbb{Q}(\sqrt{-5}) \arrow[dr, dash, "2"'] & \mathbb{Q}(\sqrt{5}) \arrow[d, dash] & \mathbb{Q}(i) \arrow[dl, dash] \\ & \mathbb{Q} & \end{tikzcd}$$

- Only 2 and 5 ramify in $\mathbb{Q}(\sqrt{-5})$ (disc $= -20$)
- Only 5 ramifies in $\mathbb{Q}(\sqrt{5})$ (disc $= 5$)
- Only 2 ramifies in $\mathbb{Q}(i)$ (disc $= -4$)

Hilbert class field example

Example (cont'd)

Since $[\mathbb{Q}(\sqrt{-5}, i) : \mathbb{Q}] = 4$, we have that $4 = efg$, where e is the ramification index, f is the degree of the residue field, and g is the number of distinct prime factors.

$$\begin{tikzcd}
& \mathfrak{p}^2 \arrow[dl, dash] \arrow[d, dash] \arrow[dr, dash] & \\
(2, 1+\sqrt{-5})^2 \arrow[dr, dash, "{e_1 = 2,\ f_1 = 1}"'] & (2) \arrow[d, dash, "{e_1 = 1,\ f_1 = 2}"] & (1+i)^2 \arrow[dl, dash, "{e_1 = 2,\ f_1 = 1}"] \\
& 2 &
\end{tikzcd}
\qquad
\begin{tikzcd}
& \mathfrak{p}^2\mathfrak{q}^2 \arrow[dl, dash] \arrow[d, dash] \arrow[dr, dash] & \\
(\sqrt{-5})^2 \arrow[dr, dash, "{e_1 = 2,\ f_1 = 1}"'] & (\sqrt{5})^2 \arrow[d, dash, "{e_1 = 2,\ f_1 = 1}"] & (1+2i)(1-2i) \arrow[dl, dash, "{e_1 = 1,\ f_1 = 1}"] \\
& 5 &
\end{tikzcd}$$

$2 \mid e,\ 2 \mid f \Rightarrow e = 2,\ f = 2,\ g = 1.$ $\quad 2 \mid e,\ g \geq 2 \Rightarrow e = 2,\ f = 1,\ g = 2.$

Therefore, we conclude that the primes $(2, 1+\sqrt{-5})$ and $(\sqrt{-5})$ are unramified in $\mathbb{Q}(\sqrt{-5}, i)$. Thus, it is the Hilbert class field of $\mathbb{Q}(\sqrt{-5})$.

Hilbert class field

Theorem (1)

Let $K/\mathbb{Q}$ be an imaginary quadratic field with ring of integers $\mathcal{O}_K$, and let $E/\mathbb{C}$ be an elliptic curve with $\mathrm{End}(E) \cong \mathcal{O}_K$. Then $K(j(E))$ is the Hilbert class field H of K.

Example

Let $K = \mathbb{Q}(i)$, so $\mathcal{O}_K = \mathbb{Z}[i]$. The elliptic curve $E/\mathbb{Q} : y^2 = x^3 - x$ (32.a3) has CM by $\mathcal{O}_K$, with $j(E) = 1728$.

By Theorem (1), the Hilbert class field of $\mathbb{Q}(i)$ is

$$H = K(j(E)) = \mathbb{Q}(i)(1728) = \mathbb{Q}(i).$$

Also, observe that $[K(j(E)) : K] = [\mathbb{Q}(i) : \mathbb{Q}(i)] = 1$, which is the class number of K.

Hilbert class field

Example

Let $K = \mathbb{Q}(\sqrt{-5})$, so $\mathcal{O}_K = \mathbb{Z}[\sqrt{-5}]$.

Let $\phi = \frac{1+\sqrt{5}}{2}$, which has minimal polynomial $x^2 - x - 1$.

The elliptic curve $E/\mathbb{Q}(\sqrt{5})$ given by (4096.1-k1)

$$y^2 = x^3 - \phi x^2 + (-\phi - 9)x - 6\phi - 15$$

has CM by $\mathcal{O}_K$, with $j(E) = -565760\phi + 914880$.

By Theorem (1), the Hilbert class field H of K is

$$K(j(E)) = \mathbb{Q}(\sqrt{-5})(-565760\phi + 914880) = \mathbb{Q}(\sqrt{-5}, \sqrt{5}) = \mathbb{Q}(i, \sqrt{-5}).$$

Indeed, $H = \mathbb{Q}(i, \sqrt{-5})$ is the Hilbert class field of $K = \mathbb{Q}(\sqrt{-5})$.

Also, observe that $[K(j(E)) : K] = [\mathbb{Q}(i, \sqrt{-5}) : \mathbb{Q}(\sqrt{-5})] = 2$, which is the class number of K.

Elliptic curves with complex multiplication

Let K be an imaginary quadratic field and let $E/\mathbb{C}$ be an elliptic curve with complex multiplication by $\mathcal{O}_K$, i.e., $\mathrm{End}(E) \cong \mathcal{O}_K$.

Then there is a lattice $\Lambda \subset \mathbb{C}$ such that $E(\mathbb{C}) \cong \mathbb{C}/\Lambda := E_\Lambda$ and

$$\mathrm{End}(E_\Lambda) = \{\alpha \in \mathbb{C} : \alpha\Lambda \subset \Lambda\} = \mathcal{O}_K.$$

If $\mathfrak{a}$ is a fractional ideal of $\mathcal{O}_K$, then $\mathfrak{a}$ is a lattice in $\mathbb{C}$ and we can form $E_\mathfrak{a} := \mathbb{C}/\mathfrak{a}$, with

$$\mathrm{End}(E_\mathfrak{a}) \cong \{\alpha \in \mathbb{C} : \alpha\mathfrak{a} \subset \mathfrak{a}\} = \{\alpha \in K : \alpha\mathfrak{a} \subset \mathfrak{a}\} = \mathcal{O}_K.$$

Example

If E has CM by $\mathbb{Z}[\sqrt{-5}]$, then $E_\mathfrak{a} := \mathbb{C}/\mathfrak{a}$, where $\mathfrak{a}$ is an ideal in $\mathbb{Z}[\sqrt{-5}]$ are all elliptic curves with CM by $\mathbb{Z}[\sqrt{-5}]$.

It turns out that $E_{\mathfrak{a}\Lambda} \cong E_{\mathfrak{b}\Lambda} \iff \overline{\mathfrak{a}} = \overline{\mathfrak{b}}$ in $\mathcal{CL}(\mathcal{O}_K)$, so we can define

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

Background

Proposition

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

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

uniquely characterized by the condition

$$E^\sigma = F(\sigma) * E \quad \text{for all } \sigma \in \mathrm{Gal}(\bar{K}/K) \text{ and all } E \in \mathcal{ELL}_{\overline{\mathbb{Q}}}(\mathcal{O}_K),$$

where for a lattice Λ with endomorphism ring $\mathcal{O}_K$, the $*$ action is

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

The kernel of F is a finite quotient of $\mathrm{Gal}(\bar{K}/K)$, since any E will be defined over some finite extension L/K and $F(\sigma) = [1]$ for $\sigma \in \mathrm{Gal}(\bar{K}/L)$. Since $\mathcal{CL}(\mathcal{O}_K)$ is an abelian group, F factors through

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

where K^{ab} is the maximal abelian extension of K.

Proof of Theorem (1)

Proof: Let L/K be the finite extension corresponding to the homomorphism

$$F : \mathrm{Gal}(\bar{K}/K) \to \mathcal{CL}(\mathcal{O}_K),$$

by which we mean that L is the fixed field of the kernel of F. Then

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

Therefore, $L = K(j(E))$.

Since $\mathrm{Gal}(\bar{K}/K)/\ker F = \mathrm{Gal}(L/K)$ **injects** into $\mathcal{CL}(\mathcal{O}_K)$, L/K is an abelian extension. Thus, $L = K(j(E))$ is an abelian extension of K.

Proof of Theorem (1)

Proof cont'd: Let $\mathfrak{c}_{L/K}$ be the conductor of L/K, and consider the composition of the Artin map with F,

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

We want to show that this composition is just the natural projection of $I(\mathfrak{c}_{L/K})$ onto $\mathcal{CL}(\mathcal{O}_K)$, i.e.,

$$F((\mathfrak{a}, L/K)) = [\mathfrak{a}] \quad \text{for all } \mathfrak{a} \in I(\mathfrak{c}_{L/K}).$$

Proposition (1)

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 $p\mathcal{O}_K = \mathfrak{p}\mathfrak{p}'$, then

$$F(\sigma_{\mathfrak{p}}) = [\mathfrak{p}] \in \mathcal{CL}(\mathcal{O}_K).$$

Proof of Theorem (1)

Proof cont'd: Let $\mathfrak{a} \in I(\mathfrak{c}_{L/K})$, and let S be the finite set of primes described in Prop. (1).

From Dirichlet's theorem, there exists a degree 1 prime $\mathfrak{p} \in I(\mathfrak{c}_{L/K})$ in the same class of $I(\mathfrak{c}_{L/K})/P(\mathfrak{c}_{L/K})$ as $\mathfrak{a}$ and not lying over a prime in S, i.e., there is an $\alpha \in K^*$ satisfying

$$\alpha \equiv 1 \bmod \mathfrak{c}_{L/K} \quad \text{and} \quad \mathfrak{a} = (\alpha)\mathfrak{p}.$$

Using the above, we can compute the following:

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

Thus, we have shown that $F((\mathfrak{a}, L/K)) = [\mathfrak{a}]$, i.e., the composition of the Artin map and F is just the natural projection of $I(\mathfrak{c}_{L/K})$ onto $\mathcal{CL}(\mathcal{O}_K)$.

Proof of Theorem (1)

Proof cont'd: It follows that

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

not just the principal ideals with a generator congruent to 1 modulo $\mathfrak{c}_{L/K}$. Recall that $F : \mathrm{Gal}(L/K) \to \mathcal{CL}(\mathcal{O}_K)$ is injective. This implies that

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

But the conductor of L/K is the largest integral ideal $\mathfrak{c}$ such that

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

Thus, $\mathfrak{c}_{L/K} = (1)$. The conductor is divisible by every prime that ramifies, and since $\mathfrak{c}_{L/K} = (1)$, L/K is everywhere unramified.
Therefore, $L = K(j(E))$ is contained in the Hilbert class field H of K.

Proof of Theorem (1)

Proof cont'd: On the other hand, the natural map

$$I(\mathfrak{c}_{L/K}) = I((1)) \to \mathcal{CL}(\mathcal{O}_K)$$

is surjective, which implies that $F : \mathrm{Gal}(L/K) \to \mathcal{CL}(\mathcal{O}_K)$ is surjective. Therefore, F is an isomorphism. It follows that

$$[L : K] = \#\,\mathrm{Gal}(L/K) = \#\mathcal{CL}(\mathcal{O}_K) = \#\,\mathrm{Gal}(H/K) = [H : K].$$

Since we already showed that $L \subset H$, this proves that $L = H$.

Therefore, $H = K(j(E))$ is the Hilbert class field of K. $\square$

Remark: The equality above also proves that $[K(j(E)) : K] = h_K$, where $h_K = \#\mathcal{CL}(\mathcal{O}_K)$.

Abelian extension of the Hilbert class field

Theorem (2)

Let $E/\mathbb{C}$ be an elliptic curve with CM by the ring of integers $\mathcal{O}_K$ of the imaginary quadratic field K, and let

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

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

Rk 1: In general, L will not be an abelian extension of K, only $K(j(E))$.

Rk 2: The extension $\mathbb{Q}(j(E), E_{\text{tors}})/\mathbb{Q}(j(E))$ is never abelian. See "Elliptic curves with complex multiplication and abelian division fields" by H. and Lozano-Robledo.

Abelian extension of $K(j(E))$

Example

Let $K = \mathbb{Q}(i)$, so $\mathcal{O}_K = \mathbb{Z}[i]$. The elliptic curve $E/\mathbb{Q} : y^2 = x^3 - x$ (32.a3) has CM by $\mathcal{O}_K$, with $j(E) = 1728$.

The 2-torsion points of E are

$$E[2] = \{\mathcal{O}, (0,0), (1,0), (-1,0)\},$$

so the 2-division field of E is $\mathbb{Q}(E[2]) = \mathbb{Q}$. By Theorem (2), we have that

$$K(j(E), E[2])/K(j(E)) = \mathbb{Q}(i)(1728)/\mathbb{Q}(i) = \mathbb{Q}(i)/\mathbb{Q}(i)$$

is an abelian extension.

Abelian extension of $K(j(E))$

Example

Let $K = \mathbb{Q}(i)$, so $\mathcal{O}_K = \mathbb{Z}[i]$. The elliptic curve $E/\mathbb{Q} : y^2 = x^3 - x$ (32.a3) has CM by $\mathcal{O}_K$, with $j(E) = 1728$.

The 4-torsion points of E are

$$\begin{aligned} E[4] = \{&\mathcal{O}, (0,0), (\pm 1, 0), (i, \pm(1-i)), (-i, \pm(1+i)), \\ &(1+\sqrt{2}, \pm(\sqrt{2}+2)), (1-\sqrt{2}, \pm(\sqrt{2}-2)), \\ &(-1+\sqrt{2}, \pm(2i - i\sqrt{2}), (-1-\sqrt{2}, \pm(-2i - i\sqrt{2})\}, \end{aligned}$$

so the 4-division field of E is $\mathbb{Q}(E[4]) = \mathbb{Q}(i, \sqrt{2})$.

A Magma computation shows that

$$K(j(E), E[4])/K(j(E)) = \mathbb{Q}(i)(1728, i, \sqrt{2})/\mathbb{Q}(i) = \mathbb{Q}(i, \sqrt{2})/\mathbb{Q}(i)$$

is an abelian extension, as we would expect by Theorem (2).

Weber function

Definition

Let K be an imaginary quadratic field and let H be the Hilbert class field of K. Let E be an elliptic curve defined over H with CM by $\mathcal{O}_K$. Fix a (finite) map

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

also defined over H. We call h a *Weber function for* E/H.

If we take a Weierstrass equation for E of the form $y^2 = x^3 + Ax + B$ with $A, B \in H$, then the following is a Weber function for E/H:

$$h(P) = h(x, y) = \begin{cases} x & \text{if } AB \neq 0 \quad (j(E) \neq 0, 1728), \\ x^2 & \text{if } B = 0 \quad (j(E) = 1728), \\ x^3 & \text{if } A = 0 \quad (j(E) = 0). \end{cases}$$

The Weber function h is essentially just an x-coordinate of the curve.

Ray class field of K modulo $\mathfrak{c}$

Let K be an imaginary quadratic field. Recall that for any integral ideal $\mathfrak{c}$ of $\mathcal{O}_K$, we define the group of $\mathfrak{c}$-torsion points of E to be

$$E[\mathfrak{c}] = \{P \in E : [\gamma]P = 0 \text{ for all } \gamma \in \mathfrak{c}\}.$$

Theorem (3)

Let K be an imaginary quadratic field, let E be an elliptic curve with CM by $\mathcal{O}_K$, and let $h : E \to \mathbb{P}^1$ be a Weber function for E/H, where H is the Hilbert class field of K. Let $\mathfrak{c}$ be an integral ideal of $\mathcal{O}_K$. Then the field

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

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

Ray class field of K modulo $\mathfrak{c}$

Example

Let $K = \mathbb{Q}(i)$, so $\mathcal{O}_K = \mathbb{Z}[i]$. The elliptic curve $E/\mathbb{Q} : y^2 = x^3 + x$ (64.a4) has CM by $\mathcal{O}_K$, with $j(E) = 1728$.

Observe that the 2-torsion points of E are

$$E[2] = \{\mathcal{O}, (0,0), (i,0), (-i,0)\}.$$

Since $j(E) = 1728$, the Weber function gives us that $h(x,y) = x^2$, so $h(0,0) = 0$, $h(i,0) = i^2 = -1$, and $h(-i,0) = (-i)^2 = 1$. Therefore,

$$K(j(E), h(E[2])) = \mathbb{Q}(i)(1728, 0, -1, 1) = \mathbb{Q}(i),$$

which confirms that the ray class field of $\mathbb{Q}(i)$ modulo (2) is indeed $\mathbb{Q}(i)$.

Ray class field of K modulo $\mathfrak{c}$

Example (cont'd)

Let $K = \mathbb{Q}(i)$, so $\mathcal{O}_K = \mathbb{Z}[i]$. The elliptic curve $E/\mathbb{Q} : y^2 = x^3 + x$ (64.a4) has CM by $\mathcal{O}_K$, with $j(E) = 1728$.

Observe that the x-coordinates of the 4-torsion points of E are

$$x(E[4]) = \{0,\ \pm i,\ \pm 1,\ 1 \pm \sqrt{2},\ -1 \pm \sqrt{2}\}.$$

Since $j(E) = 1728$, the Weber function gives us that $h(x(E[4])) = x^2$, so the only non-rational values are $h(1-\sqrt{2}) = h(-1+\sqrt{2}) = 3 - 2\sqrt{2}$, and $h(-1-\sqrt{2}) = h(1+\sqrt{2}) = 3 + 2\sqrt{2}$. Therefore,

$$K(j(E), h(E[4])) = \mathbb{Q}(i)(1728, 3 \pm 2\sqrt{2}) = \mathbb{Q}(i, \sqrt{2}),$$

which confirms that the ray class field of $\mathbb{Q}(i)$ modulo (4) is $\mathbb{Q}(i, \sqrt{2})$.

Maximal abelian extension of K

Theorem (4)

Let K be an imaginary quadratic field and let E be an elliptic curve with CM by $\mathcal{O}_K$. Then

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

In particular, if $j(E) \neq 0, 1728$ and if we take an equation for E with coefficients in $K(j(E))$, then the maximal abelian extension of K is generated by $j(E)$ and the x-coordinates of the torsion points of E.

It is not generally true that $K(j(E), E_{\mathrm{tors}})$ is an abelian extension of K. However, if K has class number 1 (so the j-invariants of these curves will be in $\mathbb{Q}$), then

$$K^{\mathrm{ab}} = K(h(E_{\mathrm{tors}})) = K(E_{\mathrm{tors}}).$$

Maximal abelian extension of K

Corollary

Let K be an imaginary quadratic field and let E be an elliptic curve with CM by $\mathcal{O}_K$. If K has class number 1, then $K^{ab} = K(E_{tors})$.

Proof: If K has class number 1, then $j(E) \in \mathbb{Q}$, so Theorem (4) says that

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

By Theorem (2), we know that

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

is an abelian extension of $K(j(E)) = K$. By the definition of h, we know

$$K(h(E_{\text{tors}})) \subset K(E_{\text{tors}}).$$

By Theorem (4), $K^{\text{ab}} = K(h(E_{\text{tors}}))$, so it follows that

$$K(E_{\text{tors}}) \subset K(h(E_{\text{tors}})).$$

Thus, we conclude that if K has class number 1, then $K^{\text{ab}} = K(E_{\text{tors}})$. $\square$

Questions?

Existence of Weil pairing consequence

Let K be an imaginary quadratic field with ring of integers $\mathcal{O}_K$. Let E be an elliptic curve with CM by $\mathcal{O}_K$. Let ζ_N be a primitive N^{th} root of unity.

We know that $K(\zeta_N)/K$ is an abelian extension. Therefore, it must be contained in $K(j(E), h(E_{\text{tors}}))$, the maximal abelian extension.

Theorem

There exist points $S, T \in E[N]$ such that the Weil pairing $e_N(S, T)$ is a primitive N^{th} root of unity.

By the Theorem, we can pick $S, T \in E[N]$ such that $e_N(S, T) = \zeta_N$. The Weil pairing is Galois invariant, so if we act on $e_N(S, T)$ by elements of $\mathrm{Gal}(\overline{K}/K(E[N]))$, then we get

$$e_N(S, T)^\sigma = e_N(S^\sigma, T^\sigma) = e_N(S, T) = \zeta_N \quad \text{for all } \sigma \in \mathrm{Gal}(\overline{K}/K(E[N])).$$

Thus, $e_N(S, T) \in K(E[N])$, so $K(\zeta_N) \subset K(E[N])$.

Example of $K(\zeta_N) \subset K(E[N])$

Let $K = \mathbb{Q}(i)$, so $\mathcal{O}_K = \mathbb{Z}[i]$. The elliptic curve $E/\mathbb{Q} : y^2 = x^3 - x$ (32.a3) has CM by $\mathcal{O}_K$, with $j(E) = 1728$.

Since K has class number 1, $K^{\mathrm{ab}} = K(h(E_{\mathrm{tors}})) = K(E_{\mathrm{tors}})$, so all abelian extensions of K are contained in $K(E_{\mathrm{tors}})$.

The x-coordinates of the 3-torsion points of E are

$$x(E[3]) = \left\{ \frac{\pm\sqrt{3+2\sqrt{3}}}{\sqrt{3}}, \frac{\pm i\sqrt{-3+2\sqrt{3}}}{\sqrt{3}} \right\}.$$

Since $j(E) = 1728$, the Weber function gives us that $h(x(E[3])) = x^2$, so

$$h\left(\frac{\pm\sqrt{3+2\sqrt{3}}}{\sqrt{3}}\right) = \frac{3+2\sqrt{3}}{3} \quad \text{and} \quad h\left(\frac{\pm i\sqrt{-3+2\sqrt{3}}}{\sqrt{3}}\right) = \frac{3-2\sqrt{3}}{3}.$$

Therefore, $K(h(E[3])) = K(E[3]) = K(\sqrt{3}) = \mathbb{Q}(i)(\sqrt{3}) = \mathbb{Q}(i, \sqrt{-3})$, so $\zeta_3 \in \mathbb{Q}(i, \sqrt{-3})$ and of course $\zeta_3 = -\frac{1}{2} + \frac{\sqrt{-3}}{2}$.

Abelian extension of the Hilbert class field

Sketch of proof: Let $L_m = K(j(E), E[m])$. Since L is the compositum of all the L_m's, it suffices to show that L_m is an abelian extension of $K(j(E))$.

- $\rho : \mathrm{Gal}(\bar{K}/K(j(E))) \to \mathrm{Aut}(E[m])$ determined by the condition

$$\rho(\sigma)(T) = T^\sigma \text{ for all } \sigma \in \mathrm{Gal}(\bar{K}/K(j(E))) \text{ and } T \in E[m].$$

- The elements $\sigma \in \mathrm{Gal}(L_m/K(j(E)))$ commute with elements of $\mathcal{O}_K$ in their action on $E[m]$:

$$([\alpha]T)^\sigma = [\alpha](T^\sigma) \text{ for all } T \in E[m] \text{ and } \alpha \in \mathcal{O}_K.$$

- ρ is a homomorphism from $\mathrm{Gal}(\bar{K}/K(j(E)))$ to the group of $\mathcal{O}_K/m\mathcal{O}_K$-module automorphisms of $E[m]$, and hence ρ induces

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

- $E[m]$ is a free $\mathcal{O}_K/m\mathcal{O}_K$-module of rank 1, so

$$\mathrm{Aut}_{\mathcal{O}_K/m\mathcal{O}_K}(E[m]) \cong (\mathcal{O}_K/m\mathcal{O}_K)^*.$$

$\square$