# ELLIPTIC CURVES WITH COMPLEX MULTIPLICATION

YIFENG HUANG

Abstract. This is a note for the Student Arithmetic learning seminar at the University of Michigan, aimed at presenting the important properties of CM elliptic curves and fixing a gap in the proof of [AEC2, Chapter II, Theorem 4.1]. This note can be used as a supplementary to [AEC2, Chapter II] for readers familiar with the basics of elliptic curves [AEC1, Chapter III] and algebraic number theory.

## 1. References

(a) [AEC1] *Arithmetic of Elliptic Curves* by J. Silverman
(b) [AEC2] *Advanced Topics in the Arithmetic of Elliptic Curves* by J. Silverman
(c) [CFT] *Class Field Theory* by J. Milne

## 2. Introduction

Recall div $f$ that for an elliptic curve $E$ over $\mathbb{C}$, the endomorphism group $R = \mathrm{End}(E)$ is either $\mathbb{Z}$ or an order of an imaginary quadratic field. Say $E$ has **CM** if the latter holds, i.e. the curve has extra "multiplications" apart from multiplication by integers. Focus on the case $R = \mathcal{O}_K$ where $K$ is an imaginary quadratic field.

Any elliptic curve over $\mathbb{C}$ is of the form $E_\Lambda := \mathbb{C}/\Lambda$ (analytic picture), where $\Lambda$ is a lattice in $\mathbb{C}$. The equation of $E_\Lambda$ is

$$E_\Lambda : y^2 = 4x^3 - g_2(\Lambda) - g_3(\Lambda) \text{ (algebraic picture)}$$

where $g_2, g_3$ are given by infinite series. So it is hard in general to go between analytic and algebraic picture.

**Example 2.1.** Let $\mathfrak{a}$ be a fractional ideal of $R = \mathcal{O}_K$, then $\mathfrak{a}$ is a lattice in $\mathbb{C}$. Consider $E = \mathbb{C}/\mathfrak{a}$, then $\mathrm{End}(E) = \{\alpha \in \mathbb{C} : \alpha\mathfrak{a} \subseteq \mathfrak{a}\}$ (true for any lattice). Multiply by $\mathfrak{a}^{-1}$ at both sides, we get $\alpha \in R$,

*Date*: Mar. 23, 2017.

so $\mathrm{End}(E) = R$. Any $\alpha \in R$ gives a canonical "multiplication-by-$\alpha$" endomorphism

$$[\alpha] : \mathbb{C}/\mathfrak{a} \to \mathbb{C}/\mathfrak{a}$$
$$z \mapsto \alpha z$$

For the invariant differential $\omega = dz$, we have

$$[\alpha]^*(dz) = d([\alpha] \circ z) = d(\alpha z) = \alpha dz$$

So $[\alpha]^*\omega = \alpha\omega$ (*).

Note that the multiplication map by $\alpha$ is constructed analytically. However, (*) gives a purely algebraic characterization of the action of $R$ on $E$: for an abstract CM curve $E$ by $R$ and $\alpha \in R$, the **normalized multiplication-by-$\alpha$** map is the unique endomorphism $[\alpha]$ of $E$ such that (*) holds for one (and all) invariant differential $\omega \in \Gamma(E, \Omega^1_{E/\mathbb{C}})$. Normalized multiplication commutes with isogeny (the proof is formal using (*)).

**Example 2.2.** Consider $E : y^2 = x^3 + 1$, $j = 0$. It has an endomorphism

$$\rho : (x, y) \mapsto (\zeta_3 x, y)$$

Check: $(\zeta_3 x)^3 + 1 = x^3 + 1 = y^2$

Is it an integer multiplication? Look at the effect of $\rho$ on invariant differential $\omega = \dfrac{dx}{y}$

$$\rho^* \frac{dx}{y} = \frac{d(x \circ \rho)}{y \circ \rho} = \frac{d(\zeta_3 x)}{y} = \zeta_3 \frac{dx}{y}$$

Thus $\rho$ is the mutiplication map by $\zeta_3$, and in particular it is complex! Thus the endomorphism ring of $E$ contains $\mathbb{Z}[\zeta_3]$, which is already a maximal order of $\mathbb{Q}(\sqrt{-3})$, so $\mathrm{End}(E)$ is exactly $R = \mathbb{Z}[\zeta_3]$.

Upshot: I computed the endomorphism ring and give the normalized multiplication map without rewriting $E$ analytically.

**Example 2.3.** $E : y^2 = x^3 + x, j = 1728$, $\rho(x, y) = (-x, iy)$.

$$\rho^* \frac{dx}{y} = \frac{d(-x)}{iy} = i\frac{dx}{y}$$

**Proposition 2.4.** *Any CM curve by $R = \mathcal{O}_K$ is isomorphic to $\mathbb{C}/\mathfrak{a}$ for some fractional ideal $\mathfrak{a}$ of $K$.*

*Proof.* WLOG $E = \mathbb{C}/\Lambda$, $\Lambda = \mathbb{Z} \oplus \mathbb{Z}\tau$, $\tau \in \mathbb{C} - \mathbb{R}$. Choose $\alpha \in R - \mathbb{Z}$, then

$$\alpha\Lambda \subseteq \Lambda \implies a\tau \in \Lambda \implies \alpha\tau = a + b\tau, a, b \in \mathbb{Z} \implies \tau = \frac{a}{\alpha - b}$$

Note that $\alpha - b \neq 0$ since $\alpha \notin \mathbb{Z}$. So $\tau \in K$, and $\Lambda$ is itself a fractional ideal of $K$. □

Upshot: the number of isomorphic classes of CM curves by $R$ is finite. In fact it equals to $h_K$ = class number of $K$.

**Corollary 2.5.** *If $E$ has CM, then the $j$-invariant $j(E) \in \overline{\mathbb{Q}}$. Moreover, $[\mathbb{Q}(j(E)) : \mathbb{Q}] \leq h_K$. (In fact we will show that equality holds.)*

*Proof.* Recall for an elliptic curve $E : y^2 = x^3 + Ax + B$, the $j$-invariant is $j = 1728 \dfrac{4A^3}{4A^3 + 27B^2}$, and two elliptic curves defined over any algebraically closed field $L$ are isomorphic over $L$ iff they have the same $j$-invariant.

Now consider an arbitrary field automorphism $\sigma \in \mathrm{Aut}(\mathbb{C})$. For an elliptic curve $E : y^2 = x^3 + Ax + B$, consider $E^\sigma : y^2 = x^3 + \sigma(A)x + \sigma(B)$. We have an isomorphism $\mathrm{End}(E) \to \mathrm{End}(E^\sigma) : f \mapsto f^\sigma$, so $\mathrm{End}(E^\sigma) = R$. By finiteness result, the isomorphic classes of $\mathrm{End}(E^\sigma)$ have at most $h_K$ choices. Note $\sigma(j(E)) = j(E^\sigma)$ because it is a rational function of $A, B$ with rational coefficient. So $\sigma(j(E))$ has at most $h_K$ choices. □

For example, if $K = \mathbb{Q}(\sqrt{-163})$, then $h_K = 1$, so $j(\mathbb{C}/\mathcal{O}_K)$ is rational. In fact it will be an integer (see the last section).

*Remark* 2.6. I concluded the finiteness using analytic picture, but I applied this result in algebraic picture.

Upshot: when studying CM curves, can assume they are all defined on a number field $L$. Moreover, given two elliptic curves $E_1, E_2$ defined over $L$, any given isogeny $E_1 \to E_2$ is defined over a finite field extension of $L$ (since isogeny is given by a rational formula, which involves only finitely many coefficients). As $\mathrm{Hom}(E_1, E_2)$ is finitely generated, we can enlarge $L$ to make every isogeny $E_1 \to E_2$ defined over $L$.

## 3. Analytic action vs Algebraic action

Let $\mathcal{E}\ell\ell(R) = \{\mathbb{C}\text{-isomorphic classes of CM curves by } R\}$.

We have $\mathcal{E}\ell\ell(R)$ consists of elliptic curves $E_\Lambda = \mathbb{C}/\Lambda$ such that $\alpha\Lambda \subseteq \Lambda$ iff $\alpha \in R$. Note that $\Lambda$ is determined up to $\mathbb{C}^*$ scaling.

Equip $\mathcal{E}\ell\ell(R)$ with $\mathcal{C}\ell(K)$ action

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

Since $\Lambda$ is determined up to $\mathbb{C}^*$, the choice of $\Lambda$ does not matter. Also principal ideals act on $\Lambda$ by scaling, so the action is well-defined on the class group. Finally, $\mathrm{End}(E_{\mathfrak{a}^{-1}\Lambda}) = R$ as well: $\alpha\mathfrak{a}^{-1}\Lambda \subseteq \mathfrak{a}^{-1}\Lambda \implies \alpha\Lambda \subseteq \Lambda$ by multiplying by $\mathfrak{a}$ at both sides.

Since every EC with CM by $R$ has the form $\mathbb{C}/\mathfrak{a}$, $\mathfrak{a}$ a fractional ideal, we have

**Proposition 3.1.** *There is an isomorphism of $\mathcal{C}\ell(K)$-sets*

$$\mathcal{C}\ell(K) \to \mathcal{E}\ell\ell(R)$$
$$\overline{\mathfrak{a}} \mapsto \mathbb{C}/\mathfrak{a}^{-1}$$

In other words, $\mathcal{C}\ell(K)$ acts on $\mathcal{E}\ell\ell(R)$ freely and transitively. To write down this action for an abstract elliptic curve, we need its analytic picture.

Recall from the proof of rationality that $\mathrm{Aut}(\mathbb{C})$ also acts on $\mathcal{E}\ell\ell(R)$. To write down this action for an abstract elliptic curve, we need to find its equation (algebraic picture).

**Proposition 3.2.** *Let $\overline{\mathfrak{a}} \in \mathcal{C}\ell(K), \sigma \in \mathrm{Aut}(\mathbb{C}), E \in \mathcal{E}\ell\ell(R)$. Then*

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

*(Note $\sigma(\mathfrak{a})$ is in $\sigma(K)$, which is $K$ since $K$ is normal over $\mathbb{Q}$.)*

This statement sounds vacuous, but it is not trivial. Start with an abstract elliptic curve $E \in \mathcal{E}\ell\ell(R)$, to check the statement, compute

LHS: Find a lattice for $E$, compute $\overline{\mathfrak{a}} * E$, find the equation, apply $\sigma$ to its coefficients, get an algebraic representation;

RHS: Find an equation for $E$, apply $\sigma$ to coefficients, find the lattice, apply $\sigma(\overline{\mathfrak{a}})$ action, get an analytic representation

and finally compare the algebraic picture in LHS and analytic picture in RHS.

*Proof.* The key is to find an algebraic description of the analytic action.

Claim: $\overline{\mathfrak{a}} * E = \mathrm{Hom}_R(\mathfrak{a}, E)$. Write $E = \mathbb{C}/\Lambda$. Recall that $\mathfrak{a}$ is an invertible sheaf over $R$, thus

$$\mathrm{Hom}_R(\mathfrak{a}, E) = \mathfrak{a}^{-1} \otimes_R \mathbb{C}/\Lambda = \mathfrak{a}^{-1} \otimes_R \mathbb{C}/\mathfrak{a}^{-1}\Lambda$$

Now $\mathbb{C}$ is flat over $K$ flat over $R$, so the $\mathbb{C}$ vector space $\mathfrak{a}^{-1} \otimes_R \mathbb{C} \hookrightarrow K \otimes_R \mathbb{C} = K \otimes_K \mathbb{C} = \mathbb{C}$. Thus $\mathfrak{a}^{-1} \otimes_R \mathbb{C} \cong \mathbb{C}$, and

$$\mathrm{Hom}_R(\mathfrak{a}, E) = \mathbb{C}/\mathfrak{a}^{-1}\Lambda = \overline{\mathfrak{a}} * E$$

Now fix a finite presentation of $\mathfrak{a}$ as $R$-module:

$$R^n \xrightarrow{A} R^n \to \mathfrak{a} \to 0$$

Apply $\mathrm{Hom}_R(-, E)$, we get

$$0 \to \mathrm{Hom}_R(\mathfrak{a}, E) \to \mathrm{Hom}_R(R^m, E) = E^n \xrightarrow{A^T} \mathrm{Hom}_R(R^n, E)$$

Therefore

$$\overline{\mathfrak{a}} * E \cong \ker(E^n \xrightarrow{A^T} E^m),$$

the kernel of a homomorphism of abelian varieties.

Now everything is algebraic, so it is routine to check that everything commutes with field automorphisms of $\mathbb{C}$. □

**Corollary 3.3.** *The subgroup* $\mathrm{Aut}(\mathbb{C}/K)$ *acts on* $\mathcal{E}\ell\ell(R)$ *as a* $\mathcal{C}\ell(K)$*-sets.*

*Proof.* When $\sigma$ fixes $K$, $(\overline{\mathfrak{a}} * E)^\sigma = \sigma(\overline{\mathfrak{a}}) * E^\sigma = \overline{\mathfrak{a}} * E^\sigma$. □

Hence from now on, we only study the action of $\mathrm{Aut}(\mathbb{C}/K)$ (instead of the whole $\mathrm{Aut}(\mathbb{C}/\mathbb{Q})$ on $\mathcal{E}\ell\ell(R)$. We have a striking formula to compute the analytic action in terms of algebraic action:

Let $E, \overline{\mathfrak{a}}$ be as above, and $\sigma$ is any automorphism of $\mathbb{C}$ that extends the Frobenius element $(\mathfrak{a}, K^{\mathrm{nr}}/K)$ on the maximal unramified extensions $K^{\mathrm{nr}}$ of $K$, then

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

We will give a much stronger form of this statement and prove it using class field theory.

Note the definition of $E^\sigma$ is independent of the equation: if $E_1, E_2$ are two isomorphic models over $\mathbb{C}$, we have isomorphism $\varphi : E_1 \to E_2$, then there is isomorphism $\varphi^\sigma : E_1^\sigma \to E_2^\sigma$. Therefore, if $E$ has a model defined over $L$ (Galois over $K$), and $\sigma$ fixes $L$, then $E^\sigma = E$. We get

**Proposition 3.4.** *If $L$ is a Galois extension of $K$ that contains $j(E)$, then the algebraic action factors through*

$$F : \mathrm{Gal}(L/K) \to \mathrm{Aut}_{\mathcal{C}\ell(K)}\mathcal{E}\ell\ell(R) \cong \mathcal{C}\ell(K)$$

*Since RHS is abelian, it further factors through*

$$F : \mathrm{Gal}(L_{\mathrm{ab}}/K) \to \mathcal{C}\ell(K)$$

*where $L_{\mathrm{ab}}$ is the maximal abelian subextension of $L/K$.*

From now on, we can talk about $E^\sigma$ for $\sigma \in \mathrm{Gal}(L/K)$ where $L$ is as above.

## 4. Hilbert Class Field

**Theorem 4.1** (Main Theorem, AEC2 II.4.1)**.** *] Define $H = K(j(E))$ where $E \in \mathcal{E}\ell\ell(R)$. Then $H$ is Galois, abelian and unramified over $K$ (so the Frobenius map $I \to \mathrm{Gal}(H/K), \mathfrak{a} \mapsto (\mathfrak{a}, H/K)$ is defined) and we have*

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

*Moreover $H$ is the maximal abelian unramified extension over $K$, i.e. the Hilbert class field of $K$. In particular $[K(j(E)) : K] = [H : K] = h_K$.*

*Remark* 4.2. This explains the $\mathfrak{a}^{-1}$ in the definition of analytic action.

We start with proving (*) for a density one set of primes in $K$, then use Dirichlet theorem saying that every ideal class contains a prime in the set. The following relation between analytic and algebraic actions is the starting point of class field theory of CM curves.

**Theorem 4.3** (Key Lemma, AEC2 II.4.2)**.** *For all but finitely degree one primes $\mathfrak{p}$ in $K$, we have*

$$\overline{\mathfrak{p}} * E = E^{\sigma_{\mathfrak{p}}}$$

*where $E$ is any elliptic curve in $\mathcal{E}\ell\ell(\mathcal{O}_K)$, and $\sigma_{\mathfrak{p}}$ is the Frobenius element of $\mathfrak{p}$ (which has ambiguity that does not matter).*

*Proof.* Idea: For elliptic curves $E_1, E_2$ over a finite field of characteristic $p$, any nonseparable map $E_1 \to E_2$ of degree $p$ is the Frobenius map $E_1 \to E_1^{(p)}$ up to automorphism. But degree and nonseparability can be obtained from analytic picture.

Now pick a finite Galois field extension $L/K$ and a model $E_i$ over $L$ for each isomorphic class in $\mathcal{E}\ell\ell(R)$, and assume that all isogenies between these $E_i$'s are defined onver $L$. Define $\varphi : E \to \overline{\mathfrak{p}} * E$ analytically by $E/\Lambda \to E/\mathfrak{p}\Lambda, z \mapsto z$. Let $\mathfrak{P}$ is a prime of $L$ lying over $\mathfrak{p}$. For $p$ large enough, $p$ is unramified in $L$ and all $E_i$ have good reduction mod $\mathfrak{P}$.

<u>Claim</u>: the mod-$\mathfrak{P}$ reduction $\widetilde{\varphi} : \widetilde{E} \to \widetilde{\overline{\mathfrak{p}} * E}$ has degree $p$ and is nonseparable, so it is essentially the Frobenius.

Given the claim,

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

and

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

Now $E^{\sigma_{\mathfrak{p}}}$ only depends on $\sigma_{\mathfrak{p}}|_{L_{\mathrm{ab}}}$, which has no ambiguity since $L_{\mathrm{ab}}$ is abelian and unramified at $\mathfrak{p}$ over $K$. So we can as well choose $\sigma_{\mathfrak{p}} = (\mathfrak{P}, L/K)$, and

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

If we pick $p$ large enough so that $\{j(E) \mod \mathfrak{P} : E \in \mathcal{E}\ell\ell(R)\}$ has no repetition, we conclude that $\overline{\mathfrak{p}} * E = E^{\sigma_p}$.

<u>To prove the claim</u>, we need two facts:

(a) For fractional ideals $\mathfrak{a} \subseteq \mathfrak{b}$ and $\mathfrak{c}$, we have $(\mathfrak{bc} : \mathfrak{ac}) = (\mathfrak{b} : \mathfrak{a})$.

For a proof, note $\mathfrak{ab} \cong \mathfrak{a} \otimes_R \mathfrak{b}$ as $R$-modules, so

$$\frac{\mathfrak{bc}}{\mathfrak{ac}} = \frac{\mathfrak{b}}{\mathfrak{a}} \otimes_R \mathfrak{c}$$

Since $\mathfrak{c}$ is an invertible sheaf over $R$, tensoring with $\mathfrak{c}$ does not change the stalks. As $\frac{\mathfrak{b}}{\mathfrak{a}}$ is supported at finitely many points, $\frac{\mathfrak{b}}{\mathfrak{a}} \otimes_R \mathfrak{c} \cong \frac{\mathfrak{b}}{\mathfrak{a}}$ as $R$-modules.

(b) For two elliptic curves $E_1, E_2$ defined over a local field $(L, \mathfrak{P})$ with good reduction, the reduction is functorial:

$$\begin{array}{ccc} E_1 & \xrightarrow{\varphi} & E_2 \\ \downarrow & & \downarrow \\ \widetilde{E_1} & \xrightarrow{\widetilde{\varphi}} & \widetilde{E_2} \end{array}$$

Moreover, the degree is preserved: $\deg \widetilde{\varphi} = \deg \varphi$.

For the proof of degree preserving, pick a prime $\ell \neq \operatorname{char}(L/\mathfrak{P})$, take Tate modules for the diagram above, we get

$$\begin{array}{ccc} T_\ell E_1 & \xrightarrow{\varphi_\ell} & T_\ell E_2 \\ \downarrow \cong & & \downarrow \cong \\ T_\ell \widetilde{E_1} & \xrightarrow{\widetilde{\varphi}_\ell} & T_\ell \widetilde{E_2} \end{array}$$

Thus $\deg \varphi = \det \phi_\ell = \det \widetilde{\phi_\ell} = \deg \widetilde{\varphi}_\ell$.

Now write $E = \mathbb{C}/\mathfrak{a}$ for a fractional ideal $\mathfrak{a}$ of $K$, and consider

$$E = \mathbb{C}/\mathfrak{a} \xrightarrow{\varphi: z \mapsto z} \mathbb{C}/\mathfrak{p}^{-1}\mathfrak{a} \xrightarrow{z \mapsto \alpha z} \mathbb{C}/\mathfrak{a} = E$$

where $\alpha \in \mathfrak{p}$.

Check: Well-defined, and find the kernel and degree. ($\deg \varphi = N\mathfrak{p} = p$ since $\mathfrak{p}$ is a degree one prime over $\mathbb{Q}$. )

The composition is $[\alpha]$, so after reduction mod $\mathfrak{P}$, we have

$$\widetilde{[\alpha]}^* \widetilde{\omega} = \widetilde{[\alpha]^* \omega} = \widetilde{\alpha \omega} = 0$$

since $\alpha \in \mathfrak{p} \subseteq \mathfrak{P}$. So $\widetilde{[\alpha]}$ is not separable.

Write $\mathfrak{b} = \alpha \mathfrak{p}^{-1}$, an integral ideal. Choose $\alpha$ such that $\mathfrak{b}$ is coprime to $b$. Hence the second map, having degree $N\alpha$, is separable, so $\widetilde{\varphi}$ is not separable.

□

*Proof of Main Theorem.* Write $H = K(j(E))$. Recall the action $F : \mathrm{Gal}(\overline{K}/K) \to \mathcal{C}\ell(K)$. Then

$$\ker F = \{\sigma : E^\sigma = E\} = \{\sigma \text{ fixing } j(E)\} = \mathrm{Gal}(\overline{K}/H)$$

In particular $H$ is normal over $K$ and we have $F : \mathrm{Gal}(H/K) \hookrightarrow \mathcal{C}\ell(K)$, so $H$ is abelian over $K$. Claim $F$ is surjective. For any $\overline{\mathfrak{a}} \in \mathcal{C}\ell(K)$, we shall construct an element of $\mathrm{Gal}(H/K)$, using Frobenius, that is mapped to $\mathfrak{a}$. Recall class field theory:

**Theorem 4.4** (Reciprocity law, CFT V.3.5)**.** *Let $L/K$ be any abelian extension of number fields, then there is a modulus $\mathfrak{m}$ (which is just an integral ideal when $K$ is totally complex) such that $L/K$ is unramified outside $\mathfrak{m}$ and the Artin map $I^{\mathfrak{m}} \to \mathrm{Gal}(L/K)$ vanishes at $K_{\mathfrak{m},1} = \langle(\alpha) : \alpha \equiv 1 \mod \mathfrak{m}\rangle$. Here $I^{\mathfrak{m}}$ is the group of fractional ideals coprime to $\mathfrak{m}$. Moreover, there is a smallest such $\mathfrak{m}$, called the conductor of $L/K$.*

Back to the proof of of the main theorem. Now let $\mathfrak{m}$ be the conductor of $H/K$. By moving lemma , we can assume $\mathfrak{a}$ is coprime to $\mathfrak{m}$. By Dirichlet theorem, every ray class (cosets of $K_{\mathfrak{m},1}$ in $I^{\mathfrak{m}}$) contains a positive density of primes. Since only degree one primes contribute to density, every ray class contains infinitely many degree one primes, and we may pick one $\mathfrak{p}$ as in Key Lemma that has the same ray class as $\mathfrak{a}$. By the definition of $\mathfrak{m}$, $(\mathfrak{a}, H/K) = (\mathfrak{p}, H/K)$, thus

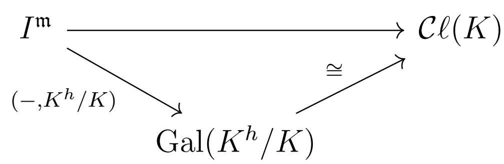
$$F(\mathfrak{a}, H/K) = F(\mathfrak{p}, H/K) = \overline{\mathfrak{p}} = \overline{\mathfrak{a}}$$

finishing the proof of surjectivity and (*) for certain choice of representative $\mathfrak{a}$. Thus we have $F : \mathrm{Gal}(H/K) \xrightarrow{\cong} \mathcal{C}\ell(K)$ and $[H : K] = h_K$. More importantly, we have a commutative diagram

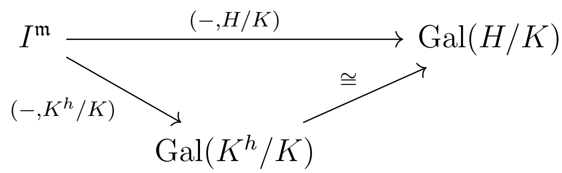
$$\begin{array}{ccc} I^{\mathfrak{m}} & \longrightarrow & \mathcal{C}\ell(K) \\ & {\scriptstyle (-,H/K)} \searrow \quad \nearrow {\scriptstyle F,\ \cong} & \\ & \mathrm{Gal}(H/K) & \end{array}$$

Since the Hilbert class field of $K$ also has degree $h_K$, it suffices to show that $H$ contains in it, that is, $H$ is unramified over $K$. Silverman says that for any $\alpha \in K^*$, $(\alpha, H) = F^{-1}\overline{(\alpha)} = 1$, so the Artin map vanishes at $K_{\mathfrak{m},1}$ even when $\mathfrak{m} = (1)$, thus the conductor has to be $(1)$. But we don't know $H/K$ is unramified yet, so the argument is cyclic (as the conductor is smallest $\mathfrak{m}$ divided by all ramified primes such that Artin map vanishes on $K_{\mathfrak{m},1}$). **How to fix Silverman's gap**? Tell me if you have a direct way, but I came up with a solution to get around this:

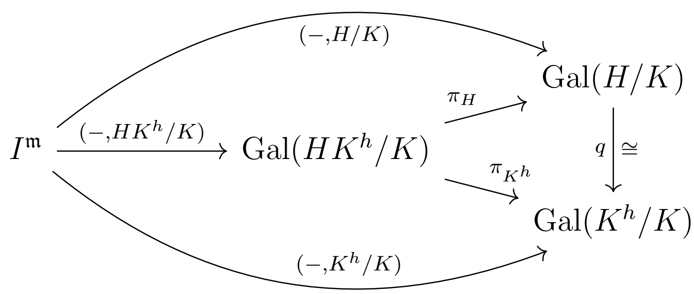
Let $K^h$ be the Hilbert class field of $K$, then we have an isomorphism $\mathcal{C}\ell(K) \to \mathrm{Gal}(K^h/K)$ given by Artin map. Thus we have




Combining the two diagrams above, we get




Since $K^h, H$ are both unramified outside $\mathfrak{m}$, so is $HK^h$ and we can insert $\mathrm{Gal}(HK^h/K)$ into the diagram:




The top left and bottom left triangles commute because they are all Artin maps. By previous diagram, the outer triangle commutes, i.e. $q \circ (-, H/K) = (-, K^h/K)$. Now we have $q \circ \pi_H \circ (-, HK^h/K) = \pi_{K^h} \circ (-, HK^h/K)$. Class field theory says Artin map $(-, HK^h)$ is surjective, so we can cancel $(-, HK^h/K)$ and the right hand side triangle commutes! As $q$ is an isomorphism,

$$\ker \pi_H = \ker \pi_{K^h}$$

and thus

$$\mathrm{Gal}(HK^h/H) = \mathrm{Gal}(HK^h/K^h)$$

as subgroups of $\mathrm{Gal}(HK^h/K)$. Hence $H = K^h$ is the Hilbert class field of $K$. $\square$

## 5. Maximal Abelian Extension

See [AEC2, Chapter II, §5], especially Corollary 5.7

Quick summary:

| Cyclomotic Theory | CM theory |
| --- | --- |
| $\mathbb{G}_m(\mathbb{C})$ | $E(\mathbb{C})$ |
| $\mathrm{End} = \mathbb{Z}$, study the field $\mathbb{Q}$ | $\mathrm{End} = \mathcal{O}_K$, study the field $K$ |
| $\mathbb{Q}^{\mathrm{ab}} = \mathbb{Q}(\zeta_n)_n = \mathbb{Q}(\mathbb{G}_m(\mathbb{C})_{\mathrm{tor}})$ | $K^{\mathrm{ab}} = K(j(E), h(E_{\mathrm{tor}}))$ |

Here $h(x, y) = x$ in usual except $h(x, y) = x^2$ when $j = 1728$ and $h(x, y) = x^3$ when $j = 0$. The key property is that $h$ must commute with automorphisms of $E$ and for these special $j$'s, $E$ has more symmetry.

## 6. Integrality of $j$

See [AEC2, II.6.4]. The proof uses local class field theory, Neron–Ogg–Shafaverich criterion, and the fact that having potential good reduction implies $j$-invariant is integral.

Application:

Now there are nine integers (Heegner numbers) $n$ such that $\mathbb{Q}(\sqrt{-n})$ has class number one. The largest three are $n = 43, 67, 163$, all having $n \equiv 3 \mod 4$. Now $j(\mathcal{O}_{\mathbb{Q}(\sqrt{-n})})$ is integer for $n = 43, 67, 163$. On the other hand,

$$j = \frac{1}{q} + 744 + 196884q + \cdots$$

where $q = \exp(2\pi i\tau)$.

Let $\tau = \dfrac{1+\sqrt{n}i}{2}$, then $q = \exp(\pi i - \pi\sqrt{n}) = -\exp(-\pi\sqrt{n})$, which is a negative number very close to 0.

Thus $j \approx \dfrac{1}{q} + 744$, so $1/q = -\exp(\pi\sqrt{n})$ is almost an integer.