Explicit Class Field Theory: Elliptic Curves with Complex Multiplication

Eliot Hodges

Math 223b: Algebraic Number Theory
Final Paper
May 2024
Salim Tayou

1. Introduction

For some number field K, understanding the Galois group $\mathrm{Gal}(L/K)$ of an extension L/K is a fundamental problem in algebraic number theory. For general extensions, this problem can be quite difficult. However, by restricting our attention to abelian extensions, it turns out that we can give a complete description of the abelian extensions in terms of the arithmetic of the base field. Class field theory makes this description precise by eliciting a surjective homomorphism between $\mathrm{Gal}(L/K)$ for a finite abelian extension L/K and the group of fractional ideals modulo the conductor $\mathfrak{c}_{L/K}$ of the extension L/K. The kernel of this map can be described explicitly. The main results of class field theory will be stated in greater detail in Section 2

Recall the Kronecker–Weber theorem, which states that every finite abelian extension of $\mathbb{Q}$ is contained in a cyclotomic field $\mathbb{Q}(\mu_n)$ for some n, where μ_n denotes the group of complex nth roots of unity. This result allows us to arrive at an analytic realization of the class field theory of $\mathbb{Q}$ in terms of the values of the exponential function at the torsion points of $\mathbb{C}/\mathbb{Z}$, which we will discuss in greater detail briefly in Section 3. It is thus natural to ask whether there exist realizations of class field theory for other number fields. Enter the theory of complex multiplication.

The group law on an elliptic curve E gives us a well-defined ring of endomorphisms $\mathrm{End}(E)$ of E. For an elliptic curve defined over $\mathbb{C}$, each integer m gives us a multiplication-by-m endomorphism taking a point x in E to $[m]x = x + \ldots + x$, where there are m summands. It is a standard fact from the theory of elliptic curves that an elliptic curve over $\mathbb{C}$ has either $\mathrm{End}(E) \simeq \mathbb{Z}$ or $\mathrm{End}(E) \simeq R$, where R is an order in a quadratic imaginary field [5]. If $\mathrm{End}(E)$ is larger than $\mathbb{Z}$, then E is said to have *complex multiplication*, or CM for short.

Elliptic curves with complex multiplication provide an explicit realization of class field theory for quadratic imaginary fields. In particular, for such a field K, we will see the intricate relationship between elliptic curves with complex multiplication by $\mathcal{O}_K$ with the arithmetic of K. We will prove that the Hilbert class field of K is given by adjoining the j-invariant of an elliptic curve E with complex multiplication by $\mathcal{O}_K$, and we will see the way in which the torsion points of E generate abelian extensions of K, just as roots of unity (the torsion points of $\mathbb{C}/\mathbb{Z}$) generate abelian extensions of $\mathbb{Q}$. The theory culminates with an analytic description of the (algebraic) action of $\mathrm{Gal}(K^{ab}/K)$ on the torsion points of E. Finally, in the last section, to a CM-elliptic curve E we will associate a Grössencharacter and describe how the Hecke L-series of the Grössencharacter is related to the Hasse-Weil L-series of E. While there exist generalizations of these results to abelian varieties (of higher genus) with complex multiplication (see [3]), little is known otherwise. In fact, analogous results are for real quadratic fields are still elusive.

In the following, which is adapted from Chapter 2 of Silverman's *Advanced Topics in the Arithmetic of Elliptic Curves* [4] and Chapter 8 of Cassels' and Frölich's *Algebraic Number Theory* [1], we assume basic familiarity with the theory of elliptic curves and the statements of class field theory (both the ideal-theoretic and idèle-theoretic formulations). The goal of this paper is not to give a complete treatment of this theory. For this, we refer the reader to Silverman [4]. Rather, its purpose is to give an overview of the main ideas at play while providing enough detail to (hopefully) be comprehensible.

2. Class Field Theory, a Review

We give a brief overview of the ideal-theoretic formulation of class field theory, followed by an even more succinct summary of the idèle-theoretic formulation (we will need this when

discussing L-series and the Grössencharacter of an elliptic curve). For our purposes, it will be enough to state these results for totally imaginary fields.

Given a totally imaginary field K, let L/K be a finite abelian extension. Consider an unramified prime $\mathfrak{p}$ of K, and let $\mathfrak{P}$ be a prime of L lying over $\mathfrak{p}$. Let κ and λ denote the respective residue fields. Because $\mathfrak{p}$ is unramified, the decomposition group $D(\mathfrak{P}/\mathfrak{p})$ is isomorphic to $\mathrm{Gal}(\lambda/\kappa)$. Thus, there is a unique element $\sigma_\mathfrak{p}$ of $D(\mathfrak{P}/\mathfrak{p})$ mapping to Frobenius. Since L/K is abelian, this element does not depend on the chosen prime $\mathfrak{P}$ lying above $\mathfrak{p}$ (for a generic extension L/K, note that $\mathfrak{p}$ determines only the conjugacy class of $\sigma_\mathfrak{p}$; for abelian extensions this class is the singleton $\{\sigma_\mathfrak{p}\}$). Hence, to each unramified prime $\mathfrak{p}$ of K, we may associate an element of $\mathrm{Gal}(L/K)$ that is uniquely determined by the property

$$\sigma_\mathfrak{p}(x) \equiv x^{|\mathfrak{p}|} \mod \mathfrak{P}$$

for all $x \in O_K$.

For an integral ideal $\mathfrak{c}$ of K, let $J(\mathfrak{c})$ be the group of fractional ideals relatively prime to $\mathfrak{c}$. Let J_K denote $J((1))$. We also let the group of principal ideals congruent to 1 modulo $\mathfrak{c}$ be denoted by

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

Let $\mathfrak{c}$ be an integral ideal of K divisible by the primes ramified in L/K, and define the *Artin map* $(\cdot, L/K) : J(\mathfrak{c}) \to \mathrm{Gal}(L/K)$ by setting $(\mathfrak{p}, L/K) = \sigma_\mathfrak{p}$ and extending multiplicatively.

Theorem 2.1. *Let L/K be a finite abelian extension of number fields. Then the kernel of the Artin map contains $P(\mathfrak{c})$ for some integral ideal $\mathfrak{c}$ of K divisible by precisely the primes of K that ramify in L. There is some largest ideal for which this is true, called the conductor of L/K and denoted $\mathfrak{c}_{L/K}$. The Artin map*

$$(\cdot, L/K) : I(\mathfrak{c}_{L/K}) \to \mathrm{Gal}(L/K)$$

is a surjective homomorphism with kernel $N_K^L(J_L)P(\mathfrak{c}_{L/K})$.

The idèlic formulation of class field theory that we need can be packaged into the following theorem. Let $\mathbb{A}_K^*$ denote the idèle group of the number field K.

Theorem 2.2. *For a number field K, there is a unique continuous homomorphism*

$$[\cdot, K] : \mathbb{A}_K^* \to \mathrm{Gal}(K^{ab}/K)$$

such that the following holds: for any finite abelian extension L/K and idèle $s \in \mathbb{A}_K^*$ whose ideal (s) is coprime to the primes that ramify in L, we have that

$$[s, K]|_L = ((s), L/K).$$

Finally, we will state the following version of Dirichlet's theorem on primes in arithmetic progressions.

Theorem 2.3. *For a number field K and integral ideal $\mathfrak{c}$ of K, every ideal class in $J(\mathfrak{c})/P(\mathfrak{c})$, the ray class group of K modulo $\mathfrak{c}$, contains infinitely many degree-1 primes of K.*

3. Cyclotomic Fields

Before understanding class field theory for quadratic imaginary fields, we first formulate the analogous statements for $\mathbb{Q}$. The approach in this simpler case will serve as a rough guideline for the rest of the paper.

Since $\mathbb{Q}$ has trivial class group, its Hilbert class field is trivial as well. We already know from Kronecker–Weber that the complex roots of unity generate abelian extensions of $\mathbb{Q}$. We can take the following viewpoint on the cyclotomic theory, which will inform our approach in the sequel, where an elliptic curve $E(\mathbb{C})$ will take the place of the multiplicative group $\mathbb{C}^*$. Let μ_n denote the nth roots of unity, i.e., the kernel of the map $\mathbb{C}^* \to \mathbb{C}^*$ given by $z \mapsto z^n$. Recall that $\mathbb{Q}(\mu_n)/\mathbb{Q}$ is an abelian extension ramified precisely at the primes dividing n. Let ζ be a generator of μ_n. For a prime p coprime to n, consider the Frobenius element $\sigma_p \in \mathrm{Gal}(\mathbb{Q}(\mu_n)/\mathbb{Q})$ associated to p. Now, if $\wp$ is a prime of $\mathbb{Q}(\mu_n)$ lying over p, then recall that σ_p is uniquely characterized by the property

$$\zeta^{\sigma_p} \equiv \zeta^p \mod \wp.$$

Because $(p, n) = 1$, it follows that $x^n - 1$ is separable modulo $\wp$, and hence its roots are distinct modulo $\wp$. Therefore, the above can be strengthened to an equality $\zeta^{\sigma_p} = \zeta^p$, and we have that $\sigma_p = 1$ if and only if $p \equiv 1 \bmod n$. Hence, $\mathbb{Q}(\mu_n)$ is the ray class field of $\mathbb{Q}$.

Now, recall that the exponential map $f : \mathbb{C}/\mathbb{Z} \to \mathbb{C}^*$ taking $t \mapsto e^{2\pi i t}$ gives an analytic parametrization of $\mathbb{C}^*$. By Kronecker–Weber, the torsion points $\mathbb{C}^*_{\mathrm{tors}} = f(\mathbb{Q}/\mathbb{Z})$ generate abelian extensions of $\mathbb{Q}$. Class field theory gives us an analytic description of the action of $\mathrm{Gal}(\mathbb{Q}^{ab}/\mathbb{Q})$ on $\mathbb{C}^*_{\mathrm{tors}}$:

Theorem 3.1. *Let $\sigma \in \mathrm{Aut}(\mathbb{C})$ and $s \in \mathbb{A}^*_{\mathbb{Q}}$ be such that $[s, \mathbb{Q}] = \sigma|_{\mathbb{Q}^{ab}}$. There exists a unique complex-analytic isomorphism $f' : \mathbb{C}/s^{-1}\mathbb{Z} \to \mathbb{C}^*$ such that the following diagram commutes*

$$\begin{array}{ccc} \mathbb{Q}/\mathbb{Z} & \xrightarrow{s^{-1}} & \mathbb{Q}/s^{-1}\mathbb{Z} \\ \downarrow f & & \downarrow f' \\ \mathbb{C}^* & \xrightarrow{\sigma} & \mathbb{C}^*. \end{array}$$

Note that Theorem 3.1 repackages the algebraic information of the action of $\mathrm{Gal}(\mathbb{Q}^{ab}/\mathbb{Q})$ into an analytic action by multiplication. In particular, we see that

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

for all $t \in \mathbb{Q}/\mathbb{Z}$ (multiplication in $\mathbb{Q}/\mathbb{Z}$ by an idèle is defined componentwise using the decomposition $\mathbb{Q}/\mathbb{Z} \simeq \bigoplus_p \mathbb{Q}_p/\mathbb{Z}_p$). Moreover, it follows from Theorem 3.1 that $f'(t) = e^{2\pi i N_s t}$, where N_s is some rational number depending on s. Hence, the above can be translated as

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

for $t \in \mathbb{Q}/\mathbb{Z}$, which elucidates the way in which the Galois action is realized as the analytic multiplication-by-$(N_s s^{-1})$ action.

4. Elliptic Curves and Class Groups

Let $E/\mathbb{C}$ be an elliptic curve with complex multiplication. Then $\mathrm{End}(E) \otimes \mathbb{Q} \simeq K$ for K a quadratic imaginary field, and $\mathrm{End}(E)$ is an order in K. We say that *E has complex multiplication by R* if $\mathrm{End}(E) \simeq \mathbb{R} \subset \mathbb{C}$; if $K = R \otimes \mathbb{Q}$, then we say that *E has complex multiplication by K*. In the sequel, unless stated otherwise, we assume that we are dealing with elliptic curves with complex multiplication by $\mathcal{O}_K$ for K a quadratic imaginary field. Let $\mathcal{E}(\mathcal{O}_K)$ denote the set of elliptic curves over $\mathbb{C}$ with $\mathrm{End}(E) \simeq \mathcal{O}_K$, up to isomorphism. With this setup out of the way, we state and sketch the proof of the main theorem of this section:

Theorem 4.1. *Let K be a quadratic imaginary field. Then $\#\mathcal{E}(\mathcal{O}_K) = \#\mathrm{Cl}(K)$.*

In order to better understand this bijection, we first recall some facts about elliptic curves over $\mathbb{C}$. In particular, it is a standard complex-analytic result that there is a bijection between the set of isomorphism classes of elliptic curves over $\mathbb{C}$ and the set of homothety classes of lattices in $\mathbb{C}$ (recall that two lattices $\Lambda, \Lambda' \subset \mathbb{C}$ are said to be *homothetic* if $\Lambda = \alpha\Lambda'$ for some $\alpha \in \mathbb{C}$). For an elliptic curve E defined over $\mathbb{C}$ with corresponding lattice $\Lambda \subset \mathbb{C}$, we have an isomorphism $\mathbb{C}/\Lambda \to E(\mathbb{C})$ given by taking $z \mapsto (\wp(z), \wp'(z))$, where $\wp$ is the Weierstrass-$\wp$ function for the lattice Λ (we will not make further mention of such complex analytic machinery; for a nice introduction to the analytic theory, we refer the reader to [5] or [2]). We thus note that $\mathcal{E}(\mathcal{O}_K)$ is equal to the set of homothety classes of lattices $\Lambda \subset \mathbb{C}$ with $\mathrm{End}(\mathbb{C}/\Lambda) \simeq \mathcal{O}_K$, where $\mathrm{End}(\mathbb{C}/\Lambda) \simeq \{\alpha \in \mathbb{C} \mid \alpha\Lambda \subset \Lambda\}$.

This bijection—between elliptic curves and lattices—is very informative. In particular, given a quadratic imaginary field K, we can use this bijection to construct an elliptic curve with complex multiplication by $\mathcal{O}_K$. Consider a nonzero fractional ideal $\mathfrak{a}$ of K. Since K is imaginary, it embeds uniquely (up to complex conjugation) into $\mathbb{C}$, and we may view $\mathfrak{a}$ as a subgroup of $\mathbb{C}$. Further, recall that $\mathfrak{a}$ is a $\mathbb{Z}$-module of rank 2, and note that $\mathfrak{a}$ is not contained in $\mathbb{R}$ since K is imaginary. Thus, we may regard each fractional ideal $\mathfrak{a}$ as a lattice in $\mathbb{C}$ and consider the associated elliptic curve $E_\mathfrak{a} = \mathbb{C}/\mathfrak{a}$. The endomorphism ring of $E_\mathfrak{a}$ is

$$\mathrm{End}(E_\mathfrak{a}) \simeq \{\alpha \in \mathbb{C} \mid \alpha\mathfrak{a} \subset \mathfrak{a}\} = \{\alpha \in K \mid \alpha\mathfrak{a} \subset \mathfrak{a}\} = \mathcal{O}_K,$$

where the first equality follows from the fact that $\mathfrak{a} \subset K$ and the second from the fact that $\mathfrak{a}$ is a fractional ideal. Hence, we have a map from the group of fractional ideals of K to $\mathcal{E}(\mathcal{O}_K)$. Furthermore, for $c \in K$, note that $\mathfrak{a}$ and $c\mathfrak{a}$ yield isomorphic elliptic curves, so this map descends to the quotient of the group of fractional ideals by the group of principal ideals, i.e., the ideal class group. To summarize, if $\bar{\mathfrak{a}}$ denotes the ideal class of $\mathfrak{a}$, we have a map $\mathrm{Cl}(K) \to \mathcal{E}(\mathcal{O}_K)$ given by $\bar{\mathfrak{a}} \mapsto E_\mathfrak{a}$.

More generally, consider a lattice Λ with $E_\Lambda \in \mathcal{E}(\mathcal{O}_K)$. For a nonzero fractional ideal $\mathfrak{a}$ of K, consider the product

$$\mathfrak{a}\Lambda = \{\alpha_1\lambda_1 + \ldots + \alpha_r\lambda_r \mid \alpha_i \in \mathfrak{a}, \lambda_i \in \Lambda\}.$$

This is again a lattice in $\mathbb{C}$, and we have that $\mathrm{End}(E_{\mathfrak{a}\lambda}) = \mathcal{O}_K$. Moreover, $E_{\mathfrak{a}\Lambda} \simeq E_{\mathfrak{b}\Lambda}$ if and only if $\bar{\mathfrak{a}} = \bar{\mathfrak{b}}$ in $\mathrm{Cl}(K)$. Using these facts, we define a $\mathrm{Cl}(K)$-action on $\mathcal{E}(\mathcal{O}_K)$ given by

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

(The reason for taking $\mathfrak{a}^{-1}$ will become apparent in the following section.) This $\mathrm{Cl}(K)$-action is transitive, and it is simply so by the above. Note that Theorem 4.1 follows immediately. All of the facts stated in this paragraph are nontrivial, but we omit their proofs for the sake of brevity.

5. The j-invariant and the Hilbert Class Field

Recall that to each elliptic curve E we may associate a quantity called the *j-invariant* of the curve, which is so named because it only depends on the isomorphism class of the curve. If E is modeled by the Weierstrass equation $E : y^2 = x^3 + Ax + B$, then $j(E) = -1728(4A)^3/\Delta$, where $\Delta = -16(4A^3 + 27B^2)$ is the discriminant of elliptic curve. The j-invariant can also be realized analytically as a bijection between moduli spaces of elliptic curves $j : \mathcal{M}_1 \to \mathcal{M}_{0,4}$ that is an isomorphism of orbifolds (see [2] for more details). From this analytic picture, we have that, over $\mathbb{C}$, two elliptic curves are isomorphic if and only if they have the same j-invariant.

Proposition 5.1. *Let E be an elliptic curve with complex multiplication by $\mathcal{O}_K$, where K is a quadratic imaginary field. Then $j(E)$ is algebraic. (In fact, $j(E)$ is an algebraic integer, but we will not need this fact.)*

Proof. By Theorem 4.1, we may associate $h_K = \#\mathrm{Cl}(K)$ j-invariants to $\mathcal{O}_K$—one for each curve in $\mathcal{E}(\mathcal{O}_K)$. For $\sigma \in \mathrm{Aut}(\mathbb{C})$, we have that $\mathrm{End}(E^\sigma) \simeq \mathrm{End}(E)$ (where E^σ is given by applying σ to the coefficients of the Weierstrass equation). This follows from noting that if $\phi : E \to E$ is in $\mathrm{End}(E)$, then $\phi^\sigma \in \mathrm{End}(E^\sigma)$. Thus, E^σ represents one of the finitely many isomorphism classes in $\mathcal{E}(\mathcal{O}_K)$. Since the j-invariant is a rational combination of the coefficients of the Weierstrass equation, we have that $j(E^\sigma) = j(E)^\sigma$. It follows that there are only finitely many possible values $j(E)^\sigma$ for $\sigma \in \mathrm{Aut}(\mathbb{C})$, which forces $[\mathbb{Q}(j(E)) : \mathbb{Q}] < \infty$, as desired. □

One consequence of the above proposition is that $\mathcal{E}(\mathcal{O}_K)$ is in bijection with the set of isomorphism classes of elliptic curves over $\overline{\mathbb{Q}}$. In the sequel, this identification will allow us to work arithmetically, so from here on out, identify $\mathcal{E}(\mathcal{O}_K)$ with the isomorphism classes of elliptic curves defined over $\overline{\mathbb{Q}}$. The goal of this section is to prove the following theorem, but along the way we will actually show much more.

Theorem 5.2. *Let K be a quadratic imaginary field; let $E \in \mathcal{E}(\mathcal{O}_K)$. Then $K(j(E))$ is the Hilbert class field of K.*

Since the elements of $\mathcal{E}(\mathcal{O}_K)$ is defined over $\overline{\mathbb{Q}}$, there is a natural action of absolute Galois group $\mathrm{Gal}(\overline{K}/K)$ on $\mathcal{E}(\mathcal{O}_K)$ given by $E \mapsto E^\sigma$ for $\sigma \in \mathrm{Gal}(\overline{K}/K)$. Recall from Section 4 that $\mathrm{Cl}(K)$ acts simply transitively on $\mathcal{E}(\mathcal{O}_K)$. Therefore, for $\sigma \in \mathrm{Gal}(\overline{K}/K)$, there is a unique $\bar{\mathfrak{a}} \in \mathrm{Cl}(K)$ for which $E^\sigma = \bar{\mathfrak{a}} * E$. This gives us a well-defined map

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

characterized by the property $E^\sigma = F(\sigma) * E$. It is not shocking (nor hard to verify) that F is a homomorphism. More surprising, however, is that this map does not depend on the choice of elliptic curve E. The proof of this statement highly nontrivial; as a result we take it for granted. Thus, the homomorphism F is characterized by the property that $E^\sigma = F(\sigma) * E$ for all $\sigma \in \mathrm{Gal}(\overline{K}/K)$ and all $E \in \mathcal{E}(\mathcal{O}_K)$.

Now, $\mathrm{Cl}(K)$ is abelian, so F factors through $\mathrm{Gal}(K^{ab}/K)$. Using class field theory, it turns out that we can actually understand F explicitly through the following proposition.

Proposition 5.3. *There is a finite set $S \subset \mathbb{Z}$ of primes such that the following holds. For a prime $p \notin S$ that splits in K, say as $p\mathcal{O}_K = \mathfrak{p}\mathfrak{p}'$, we have that*

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

Although this proposition only describes F for the Frobenius elements whose corresponding primes split in K, it is deceptively powerful. One of its consequences is the following theorem, which we assume using Proposition 5.3.

Theorem 5.4. *Let E be an elliptic curve representing an isomorphism class in $\mathcal{E}(\mathcal{O}_K)$. Then $K(j(E))$ is the Hilbert class field H of K. Moreover, for every prime ideal of K, we have*

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

hence, for any fractional ideal $\mathfrak{a}$ of K, we have

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

Remark 5.5. We remark here that had we taken the action of $\mathrm{Cl}(K)$ on $\mathcal{E}(\mathcal{O}_K)$ to be $\mathfrak{a} * E_\Lambda = E_{\mathfrak{a}\Lambda}$, then the Artin symbol $(\mathfrak{a}, H/K)$ would act by $\bar{\mathfrak{a}}^{-1}$ rather than $\bar{\mathfrak{a}}$.

Proof of Theorem 5.4. Let L be the field fixed by $\ker(F)$. We have that

$$\mathrm{Gal}(\overline{K}/L) = \{\sigma \in \mathrm{Gal}(\overline{K}/K) \mid F(\sigma) = 1\} = \{\sigma \in \mathrm{Gal}(\overline{K}/K) \mid F(\sigma) * E = E^\sigma = E\},$$

since $\mathrm{Cl}(K)$ acts simply transitively on $\mathcal{E}(\mathcal{O}_K)$. If $E^\sigma = E$, then $j(E)^\sigma = j(E^\sigma) = j(E)$, so the above is equal to

$$\{\sigma \in \mathrm{Gal}(\overline{K}/K) \mid j(E^\sigma) = j(E)^\sigma = j(E)\} = \mathrm{Gal}(\overline{K}/K(j(E))).$$

By Galois theory, it follows that $K(j(E)) = L$. Thus, F factors through the quotient of $\mathrm{Gal}(\overline{K}/K)$ by $\mathrm{Gal}(\overline{K}/L) = \ker(F)$ to give an injective map $F : \mathrm{Gal}(L/K) \to \mathrm{Cl}(K)$. It follows that $\mathrm{Gal}(L/K)$ is abelian.

Composing F with the Artin map $(\cdot, L/K) : J(\mathfrak{c}_{L/K}) \to \mathrm{Gal}(L/K)$, we have a map $J(\mathfrak{c}_{L/K}) \to \mathrm{Cl}(K)$ given by

$$J(\mathfrak{c}_{L/K}) \xrightarrow{(\cdot,L/K)} \mathrm{Gal}(L/K) \xhookrightarrow{F} \mathrm{Cl}(K)\ ,$$

where $\mathfrak{c}_{L/K}$ is the conductor of L/K. We claim that this map is simply map $J(\mathfrak{c}_{L/K}) \to \mathrm{Cl}(K)$ taking an ideal to its ideal class. In other words, for all $\mathfrak{a} \in J(\mathfrak{c}_{L/K})$, we have $F((\mathfrak{a}, L/K)) = \bar{\mathfrak{a}} \in \mathrm{Cl}(K)$. Let S be the finite set of rational primes described in Proposition 5.3. By Dirichlet's theorem on primes in arithmetic progressions (Theorem 2.3), there must exist a degree-1 prime $\mathfrak{p} \in J(\mathfrak{c}_{L/K})$ in the same $P(\mathfrak{c}_{L/K})$-class as $\mathfrak{a}$ such that $\mathfrak{p}$ does not lie over a prime in S. In symbols, there exists $\alpha \in K^*$ with $\alpha \equiv 1 \bmod \mathfrak{c}_{L/K}$ and $\mathfrak{a} = (\alpha)\mathfrak{p}$. It follows that

$$F((\mathfrak{a}, L/K)) = F(((\alpha)\mathfrak{p}, L/K)) = F((\mathfrak{p}, L/K)) = F(\sigma_{\mathfrak{p}}) = \bar{\mathfrak{p}} = \bar{\mathfrak{a}},$$

where the second equality follows from the fact that $\alpha \equiv 1 \bmod \mathfrak{c}_{L/K}$ and the third equality follows from Proposition 5.3. Thus, $F(((\alpha), L/K)) = 1$ for all principal ideals $(\alpha) \in J(\mathfrak{c}_{L/K})$, not simply the ideals $(\alpha) \in P(\mathfrak{c}_{L/K})$. Since $F : \mathrm{Gal}(L/K) \to \mathrm{Cl}(K)$ is injective, it follows that $((\alpha), L/K) = 1$ for all $(\alpha) \in J(\mathfrak{c}_{L/K})$. Now, recall that the conductor $\mathfrak{c}_{L/K}$ is the smallest integral ideal $\mathfrak{c}$ of K such that $\alpha \equiv 1 \bmod \mathfrak{c}$ implies $((\alpha), L/K) = 1$. This forces $\mathfrak{c}_{L/K} = \mathcal{O}_K$. Because the conductor is divisible by every prime of K that ramifies in L, it follows that L/K must be

everywhere unramified. Therefore, L is contained in the Hilbert class field H of K (we need not concern ourselves with the prime at infinity, as our field is totally imaginary).

Lastly, since $\mathfrak{c}_{L/K} = (1)$, we have $J(\mathfrak{c}_{L/K}) = J_K$, and the composition of F with the Artin map is just the natural quotient $J_K \twoheadrightarrow \mathrm{Cl}(K)$. It follows that F must be surjective and, therefore, an isomorphism. It follows that

$$[L : K] = \#\mathrm{Gal}(L/K) = \#\mathrm{Cl}(K) = \#\mathrm{Gal}(H/K) = [H : K],$$

where the third equality follows from class field theory. This forces $L = K(j(E)) = H$, as desired. Note that, along the way, we showed the second statement of the theorem. □

As we have seen, Proposition 5.3 is quite powerful. It not only allows us to determine the Hilbert class field of K, but it also determines the Galois action on the j-invariant. However, the proof of Proposition 5.3 is quite complicated, and thus we omit it. We briefly illustrate the main ideas below.

Sketch of the Proof of Proposition 5.3. The first step is to replace $\overline{\mathbb{Q}}$ by a finite extension L/K such that the elements of $\mathcal{E}(\mathcal{O}_K)$ and the isogenies between them are all defined over L. This step is fairly nontrivial, but, assuming that it is possible, we proceed as follows. Let S be the finite set of primes p in $\mathbb{Z}$ satisfying one of the following:

(1) p ramifies in L;

(2) some E in $\mathcal{E}(\mathcal{O}_K)$ has bad reduction at p;

(3) p is such that $v_p(N_{\mathbb{Q}}^L(j(E) - j(E'))) \neq 0$ for some $E, E' \in \mathcal{E}(\mathcal{O}_K)$.

The last condition can be reinterpreted as follows: if $p \notin S$ and $\mathfrak{P}$ divides $p\mathcal{O}_L$, then $j(E) \equiv j(E') \bmod \mathfrak{P}$ if and only if $E \simeq E'$.

Then, for $\mathfrak{P}|\mathfrak{p}$ in L, we reduce modulo $\mathfrak{P}$ and compute that

$$j(\bar{\mathfrak{p}} * E) = j(F(\sigma_{\mathfrak{p}}) * E) \mod \mathfrak{P}.$$

This computation implies the proposition by our choice of S, but it is nontrivial. Roughly, it is done by considering a reduction of the invariant differential on E and using this to show that the reduction of some maps is inseparable. This allows us to compute things explicitly downstairs using Frobenius, from which the congruence of j-invariants follows. □

6. Generating Abelian Extensions

Having determined the Hilbert class field of K, we now turn to generating abelian extensions of K. Recall that, in the cyclotomic case, abelian extensions of $\mathbb{Q}$ were obtained by adjoining the torsion points of $\mathbb{C}/\mathbb{Z}$ to its Hilbert class field. In particular, we adjoin the values given by evaluating the exponential map—an analytic parameterization of $\mathbb{C}/\mathbb{Z}$—at the torsion points of $\mathbb{C}/\mathbb{Z}$.

We proceed similarly in the case of elliptic curves. The idea is that the torsion points of an elliptic curve with complex multiplication by $\mathcal{O}_K$ will generate abelian extensions of the Hilbert class field $H = K(j(E))$. To make this precise, we choose a model for E that is defined over H and let $h : E \to E/\mathrm{Aut}(E) \simeq \mathbb{P}^1$ be a *Weber function* (i.e., a finite map $h : E \to E/\mathrm{Aut}(E)$) that is defined over H. We remark that as long as $j(E) \neq 0, 1728$, we can take h to be the Weber function

given by $h(x, y) = x$, where E has Weierstrass equation $y^2 = x^3 + Ax + B$ for $A, B \in H$. The Weber function gives us a well-defined way to adjoin the torsion points of E to $\mathbb{C}$.

Now, for an integral ideal $\mathfrak{c}$ of K, let

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

where $[\gamma]$ is the multiplication-by-γ map. We refer to $E[\mathfrak{c}]$ as the set of $\mathfrak{c}$-torsion points of E.

Theorem 6.1. *Let E be an elliptic curve representing an isomorphism class in $\mathcal{E}(\mathcal{O}_K)$. Fix a Weber function $h : E \to \mathbb{P}^1$, and let $\mathfrak{c}$ be an integral ideal of K. Then $K(j(E), h(E[\mathfrak{c}]))$ is the ray class field of K modulo $\mathfrak{c}$. Moreover,*

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

Therefore, just as in the cyclotomic case, the abelian extensions of the Hilbert class field of K are generated by the torsion points of E.

7. The Main Theorem

The following describes the analog of Theorem 3.1 for elliptic curves with complex multiplication. In particular, it translates the algebraic action of an element of $\mathrm{Gal}(K^{ab}/K)$ on $E_{\text{tors}} = f(K/\mathfrak{a})$ into an analytic action given by multiplication by an idéle.

Theorem 7.1 (The Main Theorem of Complex Multiplication)**.** *Let $E/\mathbb{C}$ be an elliptic curve representing an isomorphism class in $\mathcal{E}(\mathcal{O}_K)$. Let $\sigma \in \mathrm{Aut}(\mathbb{C})$ and $s \in \mathbb{A}_K^*$ an idèle of K such that $[s, K] = \sigma|_{K^{ab}}$. For a fractional ideal $\mathfrak{a}$ of K, let $f : \mathbb{C}/\mathfrak{a} \to E(\mathbb{C})$ be a complex-analytic isomorphism. Then there is a unique complex-analytic isomorphism $f' : \mathbb{C}/s^{-1}\mathfrak{a} \to E^\sigma(\mathbb{C})$ such that the following diagram commutes:*

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

The multiplication-by-s^{-1} map is defined componentwise via $K/\mathfrak{a} \simeq \bigoplus_{\mathfrak{p}} K_{\mathfrak{p}}/\mathfrak{a}_{\mathfrak{p}}$.

8. Grössencharacters and L-series

The theorem in the preceding section leads to a beautiful connection with the analytic theory of elliptic curves. To each elliptic curve defined over a number field L we can associate its Hasse–Weil L-function, which we define below. Studying the L-function of $E(L)$ can reveal important arithmetic information about the curve. For example, the Birch–Swinnerton–Dyer conjecture—one of the seven Millennium Problems—hypothesizes that that the rank of $E(L)$ (as an abelian group) is the order of the zero of $L(E/L, s)$ at $s = 1$.

Definition 8.1. For a prime $\mathfrak{P}$ of L, let $\lambda_{\mathfrak{P}}$ denote its residue field, and let $q_{\mathfrak{P}} = \#\lambda_{\mathfrak{P}}$. If E has good reduction at $\mathfrak{P}$, then define

$$L_{\mathfrak{P}}(E/L, t) = 1 - (q_{\mathfrak{P}} + 1 - \#\tilde{E}(\lambda_{\mathfrak{P}}))T + q_{\mathfrak{P}}T^2.$$

Otherwise, set

$$L_{\mathfrak{P}}(E/L,t) = \begin{cases} t-1 & \text{if } E \text{ has split multiplicative reduction at } \mathfrak{P}; \\ 1+t & \text{if } E \text{ has nonsplit multiplicative reduction at } \mathfrak{P}; \\ 1 & \text{otherwise.} \end{cases}$$

The polynomial $L_{\mathfrak{P}}(E/L,t)$ is called the local L-series of E at $\mathfrak{P}$. We piece the local L-series into the *(global) L-series of E/L* by setting

$$L(E/L,s) = \prod_{\mathfrak{P}} L_{\mathfrak{P}}(E/L, q_{\mathfrak{p}}^{-s})^{-1}.$$

Using the basic theory of elliptic curves, one can show that the L-series of E/L converges to an analytic function for s with $\mathrm{Re}(s) > 3/2$. In fact, much more is true. As a corollary to the Taniyama–Shimura–Weil conjecture (which implies Fermat's Last Theorem), we have the following:

Theorem 8.2 (Taylor–Wiles)**.** *Let L be a number field and E an elliptic curve defined over L. Then the L-series of E/L has an analytic continuation to the entirety of $\mathbb{C}$ and a functional equation relating $L(E/L,s)$ to $L(E/L,2-s)$.*

However, assuming Tate's thesis, one can give a proof of Theorem 8.2 for an elliptic curve E with complex multiplication by relating its L-series to the Hecke L-series attached to a Grössencharacter associated to E. Recall that a Grössencharacter on a number field L is a continuous homomorphism

$$\psi : \mathbb{A}_L^* \to \mathbb{C}^*$$

whose restriction to $L^* \subset \mathbb{A}_L^*$ is trivial. Moreover, given a Grössencharacter ψ, let $L(\psi,s)$ denote its Hecke L-series.

Theorem 8.3 (Hecke; Tate)**.** *Let ψ be a Grössencharacter with Hecke L-series $L(\psi,s)$. Then $L(\psi,s)$ has an analytic continutation to all of $\mathbb{C}$, and there is some functional equation relating $L(\psi,s)$ to $L(N-s,\bar{\psi})$, where N is a real number depending on ψ.*

It is a consequence of Theorem 7.1 that we may associate a Grössencharacter to an elliptic curve with complex multiplication. We do so with the following theorem, which is a corollary of Theorem 7.1.

Theorem 8.4. *Let E/L be an elliptic curve representing a class in $\mathcal{E}(\mathcal{O}_K)$. For an idèle $x \in \mathbb{A}_L^*$, let $s = N_K^L x \in \mathbb{A}_K^*$. There exists a unique $\alpha = \alpha_{E/L}(x) \in K^*$ such that the following hold: $\alpha\mathcal{O}_K = (s)$ (here (s) denotes the ideal of s), and for any fractional ideal $\mathfrak{a}$ of K and complex-analytic isomorphism $f : \mathbb{C}/\mathfrak{a} \to E(\mathbb{C})$, the diagram*

$$\begin{array}{ccc} K/\mathfrak{a} & \xrightarrow{\alpha s^{-1}} & K/\mathfrak{a} \\ \downarrow{\scriptstyle f} & & \downarrow{\scriptstyle f} \\ E(L^{ab}) & \xrightarrow{[x,L]} & E(L^{ab}) \end{array}$$

commutes.

Thus, we have a well-defined homomorphism $\alpha_{E/L} : \mathbb{A}_L^* \to K^* \subset \mathbb{C}^*$, but this map is not a Grössencharacter. To see why, we show that the restriction of $\alpha_{E/L}$ to L is nontrivial. Let $c \in L^* \subset \mathbb{A}_L^*$, and note that $[c, L] = 1$. By the above, $\alpha_{E/L}(c)$ is the unique element of K^* such that $\alpha \mathcal{O}_K = N_K^L((c))\mathcal{O}_K = N_K^L(c)\mathcal{O}_K$ and multiplication by $\alpha N_K^L c^{-1}$ gives the identity map on $K/\mathfrak{a}$. From this description, we see immediately that $\alpha_{E/L}(c) = N_K^L c$. Thus, $\alpha_{E/L}$ is not a Grössencharacter. However, we can correct for this in the following way. Let $\psi_{E/L} : \mathbb{A}_L^* \to \mathbb{C}^*$ be given by

$$\psi_{E/L}(x) = \alpha_{E/L}(x) N_K^L(x^{-1})_\infty.$$

Using the computation from the above, it is straightforward to verify that $\psi_{E/L}$ is indeed a Grössencharacter of L.

It turns out that we can express the L-series of an elliptic curve with complex multiplication in terms of the Hecke L-series attached to the Grössencharacter of the curve.

Theorem 8.5 (Deuring)**.** *Consider an elliptic curve E/L with complex multiplication by $\mathcal{O}_K$. If $K \subset L$, then*

$$L(E/L, s) = L(\psi_{E/L}, s) L(\overline{\psi_{E/L}}, s),$$

where $\psi_{E/L} : \mathbb{A}_L^* \to \mathbb{C}^*$ is the Grössencharacter associated to E/L. If $K \not\subset L$, then let M denote the compositum $M = LK$. If $\psi_{E/M} : \mathbb{A}_M^* \to \mathbb{C}^*$ is the Grössencharacter attached to E/M, then

$$L(E/L, s) = L(\psi_{E/M}, s).$$

The above, in conjunction with Theorem 8.3, immediately implies Theorem 8.2 for E/L elliptic curves with complex multiplication.

Acknowledgments

In addition to Melanie Matchett Wood, who suggested this project, I am very grateful to Salim Tayou and Elia Gorokhovsky for their patient and steadfast support throughout the course of this project and the semester at large.

References

[1] Cassels, J., and Frölich, A. *Algebraic Number Theory: Proceedings of an Instructional Conference*. London Mathematical Society, 1976.

[2] McMullen, C. Math 213a: Advanced complex analysis lecture notes, Fall 2023.

[3] Shimura, G. *Abelian varieties with complex multiplication and modular functions*, vol. 46 of *Princeton Mathematical Series*. Princeton University Press, Princeton, NJ, 1998.

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

[5] Silverman, J. H. *The arithmetic of elliptic curves*, second ed., vol. 106 of *Graduate Texts in Mathematics*. Springer, Dordrecht, 2009.