Complex Multiplication of Elliptic Curves

Caleb Ji

The theory of complex multiplication began with Kronecker's *Jugendtraum*, which aimed to construct abelian extensions of a number field through adjoining special values of special functions. Apart from $\mathbb{Q}$ itself, this goal has only been fully achieved for imaginary quadratic fields. This is done through constructing an elliptic curve with a given imaginary quadratic field as its endomorphism ring and adjoining its j-invariant and torsion point coordinates.

The primary goal of this paper is to provide an expository account of the classical picture just described. In Section 1 we state some relevant features of class field theory. In Section 2 we provide some background on elliptic curves. In Section 3 we prove the main theorems of complex multiplication for elliptic curves, discuss examples, and mention an extension to abelian varieties. Finally, in Section 4 we investigate the Hasse-Weil L-function of an elliptic curve with complex multiplication and show how it can be expressed via Hecke L-functions.

Contents

1 Background from class field theory

In this section, we begin by reviewing relevant key features of class field theory. First we give the statements of class field theory, which will be used extensively throughout this paper. Then we discuss the Hilbert class field and the Kronecker-Weber theorem, which set up the primary goal of complex multiplication of elliptic curves.

1.1 Statements

Here we give both the idelic and ideal-theoretic versions of class field theory. The idelic version will be more useful when we discuss characters and the ideal-theoretic version will be more useful in the determination of class fields.

Idelic class field theory

Let K be a number field and let $\mathbb{I}_K$ denote the ideles of K.

Theorem 1.1 (Artin reciprocity). *There exists a global Artin map $\phi_K : \mathbb{I}_K \to \operatorname{Gal}(K^{\mathrm{ab}}/K)$ satisfying the following properties.*

(a) The global Artin map satisfies $\phi_K(K^\times) = 1$.

(b) For every finite abelian extension L/K, ϕ_K induces an isomorphism

$$\phi_{L/K} \xrightarrow{\cong} \mathbb{I}_K/(K^\times \cdot \operatorname{Nm}(\mathbb{I}_L)) \to \operatorname{Gal}(L/K).$$

Theorem 1.2 (existence theorem). *Let $C_K = \mathbb{I}_K/K^\times$ be the idele class group. For every open subgroup $N \subset C_K$ of finite index, there exists a unique finite abelian extension L/K such that $\operatorname{Nm}(L/K) = N$.*

Ideal-theoretic class field theory

In this portion we mainly follow the presentation of [9].

Let K be a number field any let $\mathfrak{m} = \mathfrak{m}_0\mathfrak{m}_\infty$ be a modulus of K. We let $I_K^{\mathfrak{m}}$ denote the fractional ideals of K relatively prime to $\mathfrak{m}$. For any finite abelian Galois extension L/K where L is unramified outside of the places dividing $\mathfrak{m}$, one defines the Artin map

$$\psi_{L/K}^{\mathfrak{m}} : I_K^{\mathfrak{m}} \to \operatorname{Gal}(L/K)$$

by $\mathfrak{p} \mapsto \sigma_p$ (the Frobenius element) and extending linearly.

Part of the ideal theoretic theorems states that the Artin map $\psi_{L/K}^{\mathfrak{m}}$ is always surjective. We are therefore interested in the kernel. First, fixing $\mathfrak{m}$, we define

- the **ray group** of $\mathfrak{m}$: $R_K^{\mathfrak{m}} := \{(\alpha) | \nu_{\mathfrak{p}}(\alpha) \geq \nu_{\mathfrak{p}}(\mathfrak{m}_0), \alpha_v > 0 \text{ for } v | m_\infty\}$
- the **ray class group** of $\mathfrak{m}$: $\operatorname{Cl}_K^{\mathfrak{m}} := I_K^{\mathfrak{m}}/R_K^{\mathfrak{m}}$
- the **ray class field** of $\mathfrak{m}$: $K(\mathfrak{m})$ is the unique finite abelian extension of K, unramified at all $\mathfrak{p} \nmid \mathfrak{m}$, such that $\ker \psi_{L/K}^{\mathfrak{m}} = R_K^{\mathfrak{m}}$.

One of the statements of class field theory is that the ray class field of $\mathfrak{m}$ does indeed exist and is unique. Generally speaking, the kernel of $\psi_{L/K}^{\mathfrak{m}}$ will not even contain the ray group $R_K^{\mathfrak{m}}$. We call the subgroups of $I_K^{\mathfrak{m}}$ which contain $R_K^{\mathfrak{m}}$ **congruence subgroups**. If the kernel of $\psi_{L/K}^{\mathfrak{m}}$ is a congruence subgroup, then we say that L **admits** the modulus $\mathfrak{m}$. Note that this is equivalent to L being contained in the ray class field $K(\mathfrak{m})$.

As we are interested in all finite abelian extensions of K, we would like to know if any given one L is contained in a ray class field – or equivalently, if it admits a modulus. Another theorem of class field theory guarantees this to be the case. In fact, one can check that if L admits $\mathfrak{m}_1$ and $\mathfrak{m}_1|\mathfrak{m}_2$, then L admits $\mathfrak{m}_2$. This implies that there is a minimal modulus which L admits, and we call it the **conductor** of L, denoted $\mathfrak{c}(L/K)$. We know a priori that the ramifying primes of K divide $\mathfrak{c}(L/K)$, and it turns out that no other ones do. To summarize, $\mathfrak{c}(L/K)$ is a modulus divisible by precisely the primes of K ramifying in L satisfying

$$L \subseteq K(\mathfrak{m}) \Leftrightarrow \mathfrak{c}(L/K)|\mathfrak{m}.$$

Finally, another part of class field theory states that as L ranges over the abelian extensions contained in $K(\mathfrak{m})$, then $\ker \psi^{\mathfrak{m}}_{L/K} = R^{\mathfrak{m}}_K \operatorname{Nm}_{L/K}(I^{\mathfrak{m}}_L)$ and ranges over all congruence subgroups of $\mathfrak{m}$.

Having made these explanations, we now state the theorems of class field theory in terms of ideals.

Theorem 1.3 (Class field theory in terms of ideals)**.** *Let L be a finite abelian extension of K, and let S be the set of primes of K ramifying in L. (a) (Artin reciprocity) The Artin map $\psi^S_{L/K} \to$ $\operatorname{Gal}(L/K)$ admits a modulus $\mathfrak{m}$ divisible by precisely the primes in S, and defines an isomorphism*

$$I^S_K/R^{\mathfrak{m}}_K \operatorname{Nm}_{L/K}(I^{\mathfrak{m}}_L) \xrightarrow{\cong} \operatorname{Gal}(L/K).$$

(b) (completeness) If L admits a modulus $\mathfrak{m}$, then it admits every modulus divisible by $\mathfrak{m}$. Thus it admits a minimal modulus, known as its conductor.

(c) (existence theorem) For every congruence subgroup H modulo $\mathfrak{m}$, there exists a finite abelian extension L/K such that $H = R^{\mathfrak{m}}_K \operatorname{Nm}_{L/K}(I^{\mathfrak{m}}_L)$.

1.2 The Hilbert class field

Historically, one of the primary goals of class field theory was to determine the *Hilbert class field* of a number field, defined as follows.

Definition 1.4 (Hilbert class field)*.* Let K be a number field. The **Hilbert class field** of K is the maximal unramified abelian extension of K.

Remark. Unramified here means unramified not only at finite primes but also at infinite primes. Concretely, this means that all extensions of real embeddings $K \hookrightarrow \mathbb{R} \subset \mathbb{C}$ to $L \hookrightarrow \mathbb{C}$ remain real.

Let H be the Hilbert class field of K. Then H is a number field which satisfies several remarkable properties.

- Let $\operatorname{Cl}(K)$ be the class group of K. Then $\operatorname{Cl}(K) \cong \operatorname{Gal}(H/K)$.
- The prime ideals $\mathfrak{p} \in \operatorname{Spec} K$ split in L are precisely the principal ones.
- Let $I \subset \mathcal{O}_K$ be an ideal. Then $I\mathcal{O}_H$ is principal.

Let us briefly recall how these statements are proved. Full details may be found in (e.g.) [10].

Sketch.

- We apply the ideal-theoretic version of global class field theory to the modulus $\mathfrak{m} = 1$. The corresponding ray class field is a finite abelian extension H'/K unramified everywhere, and the kernel of the Artin map is simply the congruence subgroup of principal fractional ideals of K. Then the Artin map induces an isomorphism between $\mathrm{Cl}(K)$ and $\mathrm{Gal}(H'/K)$. Furthermore, one shows through properties of the conductor that any unramified abelian extension must be contained in H', so in fact $H' = H$ as desired.

- Note that $\mathfrak{p} \in \operatorname{Spec} K$ splitting completely in H is equivalent to the corresponding residue field extensions being trivial. This is equivalent to the Frobenius element $\sigma_{\mathfrak{p}}$ being trivial. But in the case of the Hilbert class field, the kernel of the Artin map is precisely the congruence subgroup of principal fractional ideals, as desired.

- Consider the extension of Hilbert class fields $H_1/H/K$. Then setting $G = \mathrm{Gal}(H_1/K)$, we have $\mathrm{Gal}(H_1/H) = [G, G]$ and $\mathrm{Gal}(H/K) = G^{\mathrm{ab}}$. One shows through a group-theoretic argument that the image of the Artin map applied to $I\mathcal{O}_H$ is trivial in $\mathrm{Gal}(H'/H)$, which as above implies that $I\mathcal{O}_H$ is principal.

□

Example 1.5. *If $\mathcal{O}_K$ is a unique factorization domain, e.g. when $K = \mathbb{Q}$, then the Hilbert class field of K is K itself.*

Example 1.6. *The Hilbert class field of $\mathbb{Q}(\sqrt{-5})$ is $\mathbb{Q}(\sqrt{-5}, i)$.*

In general, it is a difficult problem to explicitly compute the Hilbert class field of a given number field. However, by viewing an imaginary quadratic field as the endormophism ring of some elliptic curve, the theory of complex multiplication gives a construction for such fields.

1.3 The Kronecker-Weber Theorem

Understanding the maximal abelian extension of a number field may be thought of as the primary goal of class field theory. The first result in this direction is known as the Kronecker-Weber theorem, which applies to the case of $K = \mathbb{Q}$.

Theorem 1.7. *Every abelian extension of $\mathbb{Q}$ is contained in a cyclotomic extension.*

One ought to expect the main theorems of global class field theory to imply this theorem as a special case. This is indeed true.

Sketch. By global class field theory, every abelian extension $K/\mathbb{Q}$ admits a conductor $\mathfrak{m}$. This means that K is contained in the ray class field of $\mathfrak{m}$. Over $\mathbb{Q}$, every modulus divides some modulus of the form $(m)\infty$, which has ray class field $\mathbb{Q}(\zeta_m)$. Thus $K \subset \mathbb{Q}(\zeta_m)$, as desired. □

One can consider the roots of unity as the values of the function $e^{2\pi i z}$, evaluated at points of finite order on S^1. This paradigm of adjoining special functions evaluated at torsion points will reappear in the construction of the maximal abelian extension of an imaginary quadratic field.

2 Background on elliptic curves

In this section we recall some basic facts about elliptic curves and prove some basic facts about elliptic curves with complex multiplication. We also cover some results on good reduction of elliptic curves which will be needed for later proofs.

In all that follows, unless otherwise specified E is an elliptic curve over $\mathbb{C}$, K is an imaginary quadratic field, and $\mathcal{O}_K$ is its ring of integers.

2.1 j-invariant

First, we define the j-invariant using Weierstrass equations.

Definition 2.1. Let E be an elliptic curve with a Weierstrass equation

$$y^2 = x^3 + Ax + B.$$

Then the j-invariant of E is given by

$$j_E = -1728\frac{(4A)^3}{-16(4A^3+27B^2)}.$$

The significance of the j-invariant lies in the fact that two elliptic curves are isomorphic if and only if they have the same j-invariant. For a proof, see [5], III.1.4. The rational coefficients of this expression make it clear that for any $\sigma \in \mathrm{Aut}(\mathbb{C})$, we have $\sigma(j_E) = j_{\sigma(E)}$.

Another perspective involves treating elliptic curves as $SL_2(\mathbb{Z})$ orbits on the upper-half plane $\mathbb{H}$. We recall that to make this identification, one fixes the origin $O = [0:1:0]$ on E and integrates the invariant differential along any paths from O to every point of E. This is well-defined up to the periods of E, and thus identifies E with a lattice $\mathbb{C}/\Lambda$. Normalizing this lattice to be generated by $1, \tau$, we can ask about the j-invariant in terms of τ. It turns out that

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

where $g_2(\tau)$ and $g_3(\tau)$ are the Eisenstein series defined by

$$g_2(\tau) = 60\sum_{(m,n)\neq(0,0)}\frac{1}{(m+n\tau)^4} \qquad g_3(\tau) = 140\sum_{(m,n)\neq(0,0)}\frac{1}{(m+n\tau)^6}.$$

Using the expansions of the Eisenstein series, we can compute the j-function as a series in terms of $q = e^{2\pi i\tau}$:

$$j(q) = \frac{1}{q} + 744 + 196884q + 21493760q^2 + \cdots.$$

Furthermore, the curve

$$y^2 = 4x^3 - g_2(\tau)x - g_3(\tau)$$

recovers the Weierstrass form from $g_2(\tau)$ and $g_3(\tau)$. For more details and proofs, see [6], chapter 1.

2.2 Complex multiplication

The term complex multiplication refers to an elliptic curve having an endomorphism ring given by a lattice in $\mathbb{C}$, rather than just by $\mathbb{Z}$.

Proposition 2.2. *Let E be an elliptic curve. Then $\mathrm{End}(E)$ is congruent to either $\mathbb{Z}$ or an order in an imaginary quadratic field.*

Proof. We view E as a lattice $\mathbb{C}/\Lambda$ with $\Lambda = \langle 1, \tau\rangle$. Any endomorphism of E as a complex manifold induces multiplication by some α on the tangent space at the origin. Because an endomorphism of E must preserve the group structure, we easily deduce that it must in fact be multiplication by α. We thus have $\alpha, \alpha\tau \in \langle 1, \tau\rangle$. Writing $\alpha = a + b\tau$, this gives $a\tau + b\tau^2 \in \langle 1, \tau\rangle$, so τ is quadratic. Furthermore, τ must be imaginary. Then if $\mathbb{Q}(\tau) = \mathbb{Q}(\sqrt{-d})$, we obtain that $\mathrm{End}(E) = \mathbb{Z} + n\mathcal{O}_{\mathbb{Q}(\sqrt{-d})}$ for some integer n, which is indeed either $\mathbb{Z}$ or an order in $\mathbb{Q}(\sqrt{-d})$. □

Remark. Notice that if $End(E) = R$, then there may be multiple isomorphisms $f : R \xrightarrow{\cong} \operatorname{End}(E)$. When identifying the two, we naturally pick the unique one whereby $(f(\alpha))^*\omega = \alpha\omega$, where ω is the invariant differential of E.

Now fix an imaginary quadratic field $K = \mathbb{Q}[\sqrt{-d}]$ and let $\mathcal{O}_K$ be its ring of integers. We define

$$\operatorname{Ell}(R) := \{\text{elliptic curves } E/\mathbb{C} | \operatorname{End}(E) \cong R\}/\text{isomorphism over } \mathbb{C}.$$

Remark. When E has complex multiplication, one can show (using the fact that $j(E)$ is algebraic, Proposition 2.4) that we can replace isomorphism over $\mathbb{C}$ with isomorphism over $\overline{\mathbb{Q}}$.

While we may be interested in all elliptic curves with complex multiplication, it simplifies things to consider only those whose endomorphism ring is in fact a ring of integers. This will suffice to prove the classical theorems of complex multiplication.

We will now describe $\operatorname{Ell}(\mathcal{O}_K)$ in terms of the ideal class group of K. First, note that given any nonzero fractional ideal $\mathfrak{a} \in \mathcal{O}_K$, we can form the lattice $\mathfrak{a}\mathcal{O}_k$. The isomorphism class of $\mathfrak{a}\mathcal{O}_K$ clearly is the same up to scaling. Furthermore, the endomorphism ring of this lattice consists of multiplication by α where $\alpha\mathcal{O}_K \subset \alpha$. Since $\mathfrak{a}$ is a fractional ideal of a Dedekind domain, we see that its corresponding endomorphism ring is $\mathcal{O}_K$.

More generally, if Λ is a lattice with endomorphism ring $\mathcal{O}_K$, we see that $\mathfrak{a}\Lambda$ is one too. We thus obtain an action $*$ of $\operatorname{Cl}(\mathcal{O}_K)$ on $\operatorname{Ell}(\mathcal{O}_K)$ defined by

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

Proposition 2.3. *The action (1) of* $\operatorname{Cl}(\mathcal{O}_K)$ *on* $\operatorname{Ell}(\mathcal{O}_K)$ *is simply transitive.*

Proof. Because two elliptic curves are isomorphic if and only if their lattices are homothetic, it follows that the action of $\operatorname{Cl}(\mathcal{O}_K)$ is free. To show transitivity, we must show that if $E_{\Lambda_1}, E_{\Lambda_2} \in \operatorname{Ell}(\mathcal{O}_K)$, then we can find some fractional ideal $\mathfrak{a}$ such that $E_{\mathfrak{a}\Lambda_1} \cong E_{\Lambda_2}$. We may assume Λ_1, Λ_2 are of the form $\langle 1, \tau \rangle$, and thus themselves form fractional ideals $\mathfrak{a}_1, \mathfrak{a}_2$ of K. Then taking $\mathfrak{a} = \mathfrak{a}_2/\mathfrak{a}_1$ gives the desired result. □

We end this section with an important property of the j-invariant of elliptic curves with complex multiplication.

Proposition 2.4. *Take* $E \in \operatorname{Ell}(\mathcal{O}_K)$. *Then* $j(E) \in \overline{\mathbb{Q}}$.

Proof. We use the fact (noted at the beginning of Section 2.1) that for all $\sigma \in \operatorname{Aut}(\mathbb{C})$, we have $\sigma(j(E)) = j(\sigma(E))$. Moreover, it is clear that $\sigma(E) \in \operatorname{Ell}(\mathcal{O}_K)$, and from the previous proposition we have $|\operatorname{Ell}(\mathcal{O}_K)| = h_K$. Thus $j(E)$ takes on finitely many values under the action of $\operatorname{Aut}(\mathbb{C})$, which implies it must be an algebraic number. □

In fact, this argument shows that $[\mathbb{Q}(j(E)) : \mathbb{Q}] \leq h_K$. In Section 3.1 we will show equality and in Section 3.3 we will prove that $j(E)$ is in fact an algebraic integer.

2.3 The action of the absolute Galois group

As the j-invariant is an analytic entity, some work must be done to give it the algebraic significance given by the Hilbert class field. We do this by showing the compatibility of the action of the class group (which is analytic, in the sense that it is multiplication of a lattice by an ideal) with the action of the absolute Galois group.

Fix an elliptic curve $E \in \mathrm{Ell}(\mathcal{O}_K)$. We have both an action of $\mathrm{Cl}(\mathcal{O}_K)$ and an action of $\mathrm{Gal}(\overline{K}/K)$ on $\mathrm{Ell}(\mathcal{O}_K)$, where the second action is given by the action on the coefficients of the Weierstrass equations of the elliptic curves. Because the action of $\mathrm{Cl}(\mathcal{O}_K)$ is simply transitive, we may define a map

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

prescribed by the equation

$$\sigma(E) = F(\sigma) * E. \tag{2}$$

Here, the $*$ action is given by (1). One checks immediaely that F is a homomorphism. Less straightforward is the following proposition.

Proposition 2.5. *The homomorphism $F : \mathrm{Gal}(\overline{K}/K) \to \mathrm{Cl}(\mathcal{O}_K)$ given by (2) is independent of the choice of E.*

Proof. It suffices to show that for $E/\overline{\mathbb{Q}} \in \mathrm{Ell}(\mathcal{O}_K)$, $\mathfrak{a} \in \mathrm{Cl}(\mathcal{O}_K)$, and $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$, we have

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

To show this, we will use the fact that $\mathrm{Hom}_{\mathcal{O}_K}(\mathfrak{a}, M) \cong \mathfrak{a}^{-1}M$ where M is a torsion-free $\mathcal{O}_K$-module. Thus, to describe $\mathbb{C}/\mathfrak{a}^{-1}\Lambda$ it suffices to describe $\mathrm{Hom}(\mathfrak{a}, \mathbb{C})/\mathrm{Hom}(\mathfrak{a}, \Lambda)$. To do this, we construct a free resolution of $\mathfrak{a}$:

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

Now taking the $\mathcal{O}_K$-homomorphisms from these to the exact sequence of $\mathcal{O}_K$-modules

$$0 \to \Lambda \to \mathbb{C} \to E \to 0,$$

we obtain the following commutative diagram.

$$\begin{tikzcd}
 & 0 \arrow[d] & 0 \arrow[d] & 0 \arrow[d] & \\
0 \arrow[r] & \mathfrak{a}^{-1}\Lambda \arrow[r] \arrow[d] & \mathbb{C} \arrow[r] \arrow[d] & \mathrm{Hom}(\mathfrak{a}, E) \arrow[d] & \\
0 \arrow[r] & \Lambda^n \arrow[r] \arrow[d, "A^T"'] & \mathbb{C}^n \arrow[r] \arrow[d, "A^T"'] & E^n \arrow[r] \arrow[d, dashed, "A^T"'] & 0 \\
0 \arrow[r] & \Lambda^m \arrow[r] & \mathbb{C}^m \arrow[r] & E^m \arrow[r] & 0
\end{tikzcd}$$

The snake lemma gives an exact sequence

$$0 \to \mathbb{A}^{-1}\Lambda \to \mathbb{C} \to [\ker A^T : E^n \to E^m] \to \Lambda^m/A^T\Lambda^n.$$

Because $\Lambda^m/A^T\Lambda^n$ is discrete and $\mathbb{C}/\mathfrak{a}^{-1}\Lambda$ is connected, we get that $\mathbb{C}/\mathfrak{a}^{-1}\Lambda$ is the identity component of $[\ker A^T : E^n \to E^m]$. Note that $A^T : E^n \to E^m$ is a morphism of algebraic varieties, and applying $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ to the identity component of its kernel gives the identity component of $[\ker \sigma(A^T) : (\sigma(E))^n \to (\sigma(E))^m]$. Thus

$$\sigma(\mathfrak{a} * E) = \mathbb{C}/\mathfrak{a}^{-1}\Lambda = \text{identity component of } [\ker \sigma(A^T) : (\sigma(E))^n \to (\sigma(E))^m] = \sigma(\mathfrak{a}) * \sigma(E),$$

as desired.

□

2.4 Good reduction of elliptic curves

In this section, we consider elliptic curves E defined over a field K where $\mathrm{char}(K)$ may be positive. We will define and state various results regarding good reduction, which will be used in the proof that the j-invariant is an algebraic integer in Section 3.3.

Definition 2.6 (Tate module). Let E/K be an elliptic curve and let $l \in \mathbb{Z}$ be a prime. The l-adic Tate module of E is the group

$$T_l(E) = \varprojlim_n E[l^n],$$

Where the maps $E[l^{n+1}] \xrightarrow{\cdot l} E[l^n]$ are multiplication by l.

Remark. This definition generalizes word-for-word to abelian varieties.

We are interested in the case where $l \neq \mathrm{char}(K)$. In this case, it is not hard to see that $T_l(E) \cong \mathbb{Z}_l \times \mathbb{Z}_l$ as a $\mathbb{Z}_l$ module. Because the action of $\mathrm{Gal}(\overline{K}/K)$ on $E[l^n]$ commutes with multiplication by l, we obtain an l-adic representation of dimension 2:

$$\mathrm{Gal}(\overline{K}/K) \to \mathrm{Aut}(T_l(E)) \hookrightarrow \mathrm{Aut}(T_l(E)) \otimes_{\mathbb{Z}_l} \mathbb{Q}_l.$$

We will now define good and bad reduction and state the Neron-Ogg-Shafarevich criterion. In the rest of this section, we change our notation.

- K is a local field complete with respect to a discrete valuation v.
- $(A, \mathfrak{m}, k)$ is the corresponding local ring (where $v(x) \geq 0$).
- π is a uniformizer of A with $v(\pi) = 1$.

A minimal Weierstrass equation for an elliptic curve E is one that minimizes $v(\Delta)$ subject to the condition that $v(\Delta) \geq 0$. One can always find a minimal Weierstrass equation with coefficients in R. Given such an equation, the reduction of E modulo $\mathfrak{m}$ is the base change of E by the morphism $\mathrm{Spec}\, k \to \mathrm{Spec}\, A$, which of course just amounts to reducing coefficients modulo $\mathfrak{m}$.

Definition 2.7 (good and bad reduction). Let E/K be an elliptic curve and let $\tilde{E}$ be the reduction modulo $\mathfrak{m}$ of a minimal Weierstrass equation for E.
(a) E has good (or stable) redution if $\tilde{E}$ is nonsingular.
(b) E has multiplicative (or semistable) reduction if $\tilde{E}$ has a node.
(c) E has additive (or unstable) reduction if $\tilde{E}$ has a cusp.

In cases (b) and (c), we also say that E has bad reduction. If K is instead a number field, we can define these same notions of reduction at v by the embedding $K \hookrightarrow K_v$.

Let K^{unr} be the maximal unramified extension of K. Then we have an exact sequence

$$1 \to \mathrm{Gal}(\overline{K}/K^{\mathrm{unr}}) \to \mathrm{Gal}(\overline{K}/K) \to \mathrm{Gal}(K^{\mathrm{unr}}/K) \cong \mathrm{Gal}(\overline{k}/k) \to 1.$$

We define the inertia subgroup

$$I_v := \mathrm{Gal}(\overline{K}/K^{\mathrm{unr}}) \subset \mathrm{Gal}(\overline{K}/K).$$

If $\mathrm{Gal}(\overline{K})/K)$ acts on some set S, we say that S is **unramified at** v if the action of I_v on S is trivial. We can now state the Neron-Ogg-Shafarevich criterion, which relates good reduction to whether the Tate module is unramified.

Theorem 2.8. *[Neron-Ogg-Shafarevich criterion] Let E/K be an elliptic curve. Then the folloing are equivalent.*

(a) E has good reduction at v.

(b) $E[m]$ is unramified at v for all integers $m \geq 1$ that are relatively prime to $\mathrm{char}(k)$.

(c) The Tate module $T_l(E)$ is unramified at v for all primes $l \neq \mathrm{char}(k)$.

(d) $E[m]$ is unramified at v for infinitely many integers $m \geq 1$ that are relatively prime to $\mathrm{char}(k)$.

For a proof, see [5], Section VII.7.

Remark. This crietrion has been generalized to abelian varieties in the article [7] by Serre and Tate.

Reduction type depends on the field over which E is defined. This motivates the following definition.

Definition 2.9 (potential good reduction). We say that an elliptic curve E/K has *potential good reduction* if there is a finite extension K'/K such that E has good reduction over K'.

Remark. While we will not need it directly, we note that the semistable reduction theorem states that an elliptic curve has either good or multiplicative reduction over some finite extension. Grothendieck generalized this statement to abelian varieties and Deligne and Mumford generalized it to all curves.

Proposition 2.10. *Let E/K be an elliptic curve. Then E has potential good reduction if and only if its j-invariant is integral.*

The proof of this proposition is a relatively straightforward computation and can be found in [5] VII.5. Finally, we have the following corollary of Theorem 2.8.

Corollary 2.11. *Let E/K be an elliptic curve. Then E has potential good reduction if and only if the inertia group I_v acts on the Tate module $T_l(E)$ through a finite quotient for some (all) prime(s) $l \neq \mathrm{char}(k)$.*

This corollary will be directly used in the proof that the j-invariant is an algebraic integer. Its proof is also relatively straightforward and can be found in [5] VII.7.

3 The main theorems of complex multiplication

3.1 The j-invariant generates the Hilbert class field

The goal of this section is show that for any $E \in \mathrm{Ell}(\mathcal{O}_K)$, the Hilbert class field of K is given by $K(j(E))$. We will assume the following proposition.

Proposition 3.1. *There is a finite set of rational primes $S \subset \mathbb{Z}$ such that if $p \in S$ is a prime which splits in K, say as $p\mathcal{O}_K = \mathfrak{p}\mathfrak{p}'$, then*

$$F(\sigma_{\mathfrak{p}}) = \overline{\mathfrak{p}} \in \mathrm{Cl}(\mathcal{O}_K).$$

For the proof, see Proposition 4.2 of [6]. It involves analyzing the structure of the isogenies between E and $\mathfrak{p} * E$, reducing them modulo certain primes and using the fact that maps between smooth curves in characteristic p can be factored as a Frobenius map followed by a separable map.

Theorem 3.2. *Take $E \in \mathrm{Ell}(\mathcal{O}_K)$. Then $K(j(E))$ is the Hilbert class field H of K.*

Proof. First we show that $K(j(E))$ is the fixed field of $\ker F$ (defined in 2). Indeed,

$$\begin{aligned}\ker F &= \{\sigma \in \mathrm{Gal}(\overline{K}/K) | F(\sigma) * E = E\} \\ &= \{\sigma \in \mathrm{Gal}(\overline{K}/K) | \sigma(E) = E\} \\ &= \{\sigma \in \mathrm{Gal}(\overline{K}/K) | j(\sigma(E)) = j(E)\} \\ &= \{\sigma \in \mathrm{Gal}(\overline{K}/K) | \sigma(j(E)) = j(E)\} \\ &= \mathrm{Gal}(K/K(j(E))).\end{aligned}$$

Moreover $\mathrm{Gal}(K/K(j(E))$ is a normal subgroup of $\mathrm{Gal}(\overline{K}/K)$, because if $\sigma(j(E)) = j(E)$, then $F(\tau\sigma\tau^{-1})(E) = E \Rightarrow \tau\sigma\tau^{-1}(j(E)) = j(E)$. Therefore, F maps the quotient $\mathrm{Gal}(K(j(E)/K)$ injectively into $\mathrm{Cl}(\mathcal{O}_K)$, so $K(j(E))/K$ is an abelian extension.

Now we show that $K(j(E))/K$ is unramified, or equivalently, that the conductor $\mathfrak{c}(K(j(E))/K) = 1$. For convenience, we will denote $\mathfrak{c}(K(j(E))/K)$ by just $\mathfrak{c}$. We claim that the composition with the Artin map

$$I_K^{\mathfrak{c}} \xrightarrow{\psi^{\mathfrak{c}}_{K(j(E))/K}} \mathrm{Gal}(K(j(E)/K) \xrightarrow{F} \mathrm{Cl}(\mathcal{O}_K)$$

is simply projection on the integral ideals $\mathfrak{a} \in I_K^{\mathfrak{c}}$. Indeed, from Proposition 3.1 and the Chebotarev density theorem, there is some degree 1 $\mathfrak{p} \in I_K^{\mathfrak{c}}$ in the same $P(\mathfrak{c})$ class as $\mathfrak{a}$ which does not lie over a prime in S. Then

$$F(\psi^{\mathfrak{c}}_{K(j(E))/K}(a)) = F(\mathfrak{p}) = \overline{\mathfrak{p}} = \overline{\mathfrak{a}},$$

as desired. In particular, the image of all principal ideals of $I_K^{\mathfrak{c}}$ are in the kernel of

$$F : \mathrm{Gal}(K(j(E)/K) \xrightarrow{F} \mathrm{Cl}(\mathcal{O}_K),$$

which is itself injective. This means that all principal ideals of $I_K^{\mathfrak{c}}$ are in the kernel of $\psi^{\mathfrak{c}}_{K(j(E))/K}$. But by class field theory, $\mathfrak{c}$ is the smallest integral ideal where (α) is in the kernel of the Artin map for all $\alpha \equiv 1 \pmod{\mathfrak{c}}$. This implies that $\mathfrak{c} = 1$.

Thus $K(j(E))/K$ is unramified, so $K(j(E)) \subset H$. On the other hand, the composition of F with the Artin map is surjective, so $F : \mathrm{Gal}(K(j(E)/K) \xrightarrow{F} \mathrm{Cl}(\mathcal{O}_K)$ is bijective. Since $[H : K] = |\mathrm{Cl}(\mathcal{O}_K)|$, it follows that $K(j(E)) = H$ as desired. □

Recall that we showed in a previous section that $[\mathbb{Q}(j(E)) : \mathbb{Q}] \leq h_K$. This proof shows that $[K(j(E)) : K] = h_K$, so since $[K(j) : \mathbb{Q}(j)] \leq 2$, we get the equality $[\mathbb{Q}(j(E)) : \mathbb{Q}] \leq h_K$.

Remark. This proof in fact shows that as E_i ranges over all representatives of $\mathrm{Ell}(\mathcal{O}_K)$, then $j(E_i)$ gives a complete set of $\mathrm{Gal}(\overline{K}/K)$-conjugates of $j(E)$. Moreover, the action of any nonzero $\mathfrak{a} \in I_K$ on $j(E)$ vis the Artin map is given by

$$\psi^{1}_{H/K}(\mathfrak{a})j(E) = j(\mathfrak{a} * E).$$

3.2 Torsion points and the maximal abelian extension

The goal of this section is to compute the abelian extensions of an imaginary quadratic field K by adjoining torsion points of some $E \in \mathrm{Ell}(\mathcal{O}_K)$. As we will see, adjoining them all along with $j(E)$ will give an abelian extension of the Hilbert class field H. The maximal abelian extension is instead obtained by evaluating the torsion points on a Weber function, which essentially gives their x-coordinates.

We begin with a preliminary result.

Proposition 3.3. *Take $E \in \mathrm{Ell}(\mathcal{O}_K)$ and let*

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

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

Proof. Let $L_m = H(E[m]) \subset L$ be the field obtained by adjoining the m-torsion points of E for some m. It suffices to show that L_m is an abelian extension of H. By the addition formula in terms of the Weierstrass $\wp$-function, we see that automorphisms of $\mathbb{C}/K$ act on $E[m]$, and thus K_m is indeed a finite Galois extension of K. Moreover, we immediately obtain an injection

$$\rho : \mathrm{Gal}(L_m/H) \hookrightarrow \mathrm{GL}_2(\mathbb{Z}/m\mathbb{Z})$$

from the action on $E[m]$.

Next, we claim that this action of $\mathrm{Gal}(L_m/H)$ commutes with the action of $\mathcal{O}_K$ on $E[m]$. Indeed, take a model of E defined over H. Then it is not hard to show that every endomorphism of E is defined over H (for complete details, see [6], Theorem 2.2.2). The claim follows from applying this to the action of $\mathcal{O}_K$. Thus the image of ρ lies in $\mathrm{Aut}_{\mathcal{O}_K/m\mathcal{O}_K}(E[m])$. But it is easy to see that $E[m] \cong \mathcal{O}_K/m\mathcal{O}_K$ as $\mathcal{O}_K/m\mathcal{O}_K$-modules, so the image is abelian as desired. □

Next, we determine the ray class fields of K. First, we define the following Weber function $h : E \to \mathbb{P}^1$, where we pick some model $y^2 = x^3 + Ax + B$ for E.

$$h(f(z)) = \begin{cases} x & j(E) \neq 0, 1728, \\ x^2 & j(E) = 0, \\ x^3 & j(E) = 1728. \end{cases}$$

Remark. One may define a Weber function of an elliptic curve to be independent of the choice of model in the following way. Fix an isomorphism $f : \mathbb{C}/\Lambda \xrightarrow{\cong} E$ and define

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

As usual, g_2 and g_3 are Eisenstein series, $\Delta = g_2^2 - 27g_3^3$ is the discriminant, and $\wp$ is the Weierstrass $\wp$-function.

Theorem 3.4. *Let K be a quadratic imaginary field, take $E \in \mathrm{Ell}(\mathcal{O}_K)$, and let h be the Weber function defined above. 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 $\mathfrak{c}$.

This theorem implies the following corollary, which is what we were after in the first place.

Corollary 3.5. *We have*

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

Moreover, for $j(E) \neq 0, 1728$, we have that K^{ab} is generated over K by $j(E)$ and the x-coordinates of the torsion points of E.

Indeed, this follows from the fact from class field theory that every abelian extension is contained in a ray class field.

We will now give a rough idea of a proof of Theorem 3.4.

Idea of proof of Theorem 3.4. We would like to show that

$$\psi_{L/K}(\mathfrak{p}) = 1 \Leftrightarrow \mathfrak{p} \in R_K^{\mathfrak{c}};$$

it suffices to do so for all but finitely many primes in K which split completely. If we take such a $\mathfrak{p} \in R_K^{\mathfrak{c}}$, then one can show that $\mathfrak{p} = (\pi)$ for some $\pi \in \mathcal{O}_K$ such that multiplication by π and reducing $\pmod{\mathfrak{p}}$ is equivalent to reducing first and taking the Frobenius. The fact that $\mathfrak{p}$ is principal implies that $\psi_{L/K}(\mathfrak{p})$ fixes H, and we use the commutative diagram described to show that it fixes $h(E[\mathfrak{c}])$. This proves one direction, and the other direction follows a similar paradigm. □

3.3 Integrality of the j-invariant

We have already seen in Proposition 2.4 that $j(E)$ is rational for curves with complex multiplication. In this section, we will prove that it is in fact an algebraic integer. As a particularly nice consequence, $e^{\pi\sqrt{163}}$ is almost an integer, a fact we explain in Section 3.4.

There are three proofs of these in [6]: a complex analytic proof, an l-adic proof, and a p-adic proof. Here we will present the l-adic proof, which may be generalized to abelian varieties. We will deduce the result from the following theorem, whose proof is due to Serre and Tate.

Theorem 3.6. *Let L be a number field and let E/L be a curve with complex multiplication. Then E has potential good reduction at every prime of L.*

Before discussing the proof, let us see how it implies the integrality of the j-invariant of a CM elliptic curve.

Corollary 3.7. *Let $E/\mathbb{C}$ be an elliptic curve with complex multiplication. Then $j(E)$ is an algebraic integer.*

Proof. We showed in Proposition 2.4 that $j(E)$ is an algebraic number. Take an equation for E with coefficients in $L = \mathbb{Q}(j(E))$. By Theorem 3.6, E has potential good reduction at every prime of L. By Proposition 2.10, $j(E)$ is integral at every prime of L, which implies that $j(E) \in \overline{\mathbb{Z}}$ as desired. □

We now give a proof of Theorem 3.6 that is a bit light on details; full details may be found in [6], Theorem II.6.4.

Proof of Theorem 3.6. We may replace L with a finite extension and assume $\operatorname{End}_{L_v}(E)$ is an order of an imaginary quadratic field. Fix a prime $v \in \operatorname{Spec} \mathcal{O}_L$ and let I_v be the inertia subgroup of $\operatorname{Gal}(\overline{L}_v/L_v)$. Let $p = \operatorname{char}((\mathcal{O}_L)_v/\mathfrak{m}_v)$ and let l be a prime not equal to 2 or p. By Corollary 2.11, it suffices to show that the image of I_v in $\operatorname{Aut} T_l(E)$ (under the implied representation of $\operatorname{Gal}(\overline{L_v}/L_v)$) is finite.

By Proposition 3.3, the action of $\operatorname{Gal}(\overline{L_v}/L_v)$ on $T_l(E)$ is abelian, so the action of I_v factors through I_v^{ab}. By local class field theory, $I_v^{\mathrm{ab}} \cong (\mathcal{O}_L)_v^*$. Let $(\mathcal{O}_L)_{v,1}^*$ be the group of 1-units; that is, the subgroup of $(\mathcal{O}_L)_v$ with $u \equiv 1 \pmod{\mathfrak{m}_v}$. One can show $(\mathcal{O}_L)_{v,1}^*$ is a pro-p group. Furthermore, we get an exact sequence

$$1 \to (\mathcal{O}_L)_{v,1}^* \to I_v^{\mathrm{ab}} \to ((\mathcal{O}_L)_v/\mathfrak{m}_v)^* \to 1.$$

On the other hand, choosing a basis for the Tate module gives an exact sequence

$$1 \to \mathrm{GL}_2(\mathbb{Z}_l)_1 \to \operatorname{Aut} T_l(E) \to \mathrm{GL}_2(\mathbb{Z}/l\mathbb{Z}) \to 1,$$

where $\mathrm{GL}_2(\mathbb{Z}_l)_1$ is the group of matrices congruent to the identity modulo l, and is pro-l group. There are no non-trivial homomorphisms from a pro-p group to a pro-l group. This fact implies that the representation

$$I_v^{\mathrm{ab}} \to \operatorname{Aut} T_l(E)$$

defines an embedding $(\mathcal{O}_L)_{v,1}^* \hookrightarrow \mathrm{GL}_2(\mathbb{Z}/l\mathbb{Z})$. The residue field $((\mathcal{O}_L)_v/\mathfrak{m}_v)^*$ is also finite, so it follows that the image of I_v^{ab} in $\operatorname{Aut} T_l(E)$ is finite, as desired. □

3.4 Examples and applications

Let us list some concrete illustrations of the theorems above. We begin with the following observation.

Observation 3.8. $e^{\pi\sqrt{163}} = 262537412640768743.99999999999250072597\ldots$

The fact that this number is almost an integer can be explained through the integrality of the j-invariant. Set

$$K = \mathbb{Q}[\sqrt{-163}], \mathcal{O}_K = \mathbb{Z}\left[\frac{1+\sqrt{-163}}{2}\right].$$

Then $\mathcal{O}_K$ is one of the nine imaginary quadratic fields with class number 1. Take the elliptic curve E corresponding to the lattice $\langle 1, \frac{1+\sqrt{-163}}{2}\rangle$. Recall that at the end of Section 3.1, we showed that for $E \in \mathrm{Ell}(\mathcal{O}_K)$, we have $[\mathbb{Q}(j(E)) : \mathbb{Q}] = h_K$. In this case, we therefore have $j(E) \in \mathbb{Q}$. Furthermore, the integrality of the j-invariant implies that $j(E) \in \mathbb{Z}$.

Here, E corresponds to the value $\tau = \frac{1+\sqrt{-163}}{2}$ and we have $q = e^{2\pi i\tau} = -e^{-\pi\sqrt{163}}$, which is numerically very close to 0. Using the q-expansion for the j-invariant:

$$j(q) = \frac{1}{q} + 744 + 196884q + 21493760q^2 + \cdots,$$

the fact that $j(q)$ is an integer implies that $\frac{1}{q} = -e^{\pi\sqrt{163}}$ is almost an integer, as desired.

To compute the Weierstrass equation for this elliptic curve, one needs a computer (or to be extremely adept at computation...). One finds ([6], Appendix 3) that a minimal Weierstrass equation for the elliptic curve corresponding to the lattice $\langle 1, \frac{1+\sqrt{-163}}{2}\rangle$ is

$$y^2 + y = x^3 - 2174420x + 1234136692.$$

There are at least a few simple cases, however, which can be easily computed by hand. For example, consider the elliptic curve E_Λ corresponding to the lattice $\Lambda = \langle 1, i\rangle$. As this corresponds to the unique factorization domain $\mathbb{Z}[i]$, we expect its j-invariant to be an integer. To calculate it, we not that the fact that $i\Lambda = \Lambda$ implies that $g_3(\tau) = g_3(i\tau) = i^6 g_3(\tau) \Rightarrow g_3(\tau) = 0$. Thus we have

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

which is indeed an integer. Furthermore, a Weierstrass equation for E_Λ is given by

$$y^2 = 4x^3 - g_2(\Lambda)x,$$

and since we can scale $A \mapsto u^2 A, B \mapsto u^3 B$, we get isomorphic elliptic curves

$$y^2 = x^3 + x \text{ and } y^2 = x^3 - nx^2.$$

Elliptic curves of the second kind are used to study the congruent number problem; for more details see [4].

Similarly, one can begin with the lattice $\Lambda = \langle 1, \frac{1+\sqrt{-3}}{2} \rangle$, corresponding to the unique factorization domain $\mathbb{Z}[e^{2\pi i/3}]$. We get $j(\tau) = 0$ and a Weierstrass equation $y^2 = 4x^3 - g_3(\Lambda)$, which is isomorphic to (e.g.) the curve $y^2 = x^3 + 1$.

3.5 The main theorem of complex multiplication

While the previous theorems in this section may be regarded as the classical main theorems of complex multiplication, there is another theorem that goes by the "main theorem of complex multiplication." With some work, one can deduce the previous theorems from this one. Moreover, this statement may be generalized to abelian varieties. This was done by Shimura and Taniyama in [8]. Here we will simply give the statement, both in the case of elliptic curves and in the general case, and add some light commentary.

Elliptic curve case

As usual, 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 $\mathrm{End}(E) \cong \mathcal{O}_K$.

Theorem 3.9 (The main theorem of complex multiplication for elliptic curves)**.** *Take $\sigma \in \mathrm{Aut}(\mathbb{C})$ and let $s \in \mathbb{I}_K$ be an idele satisfying $\phi_K(s) = \sigma|_{K^{\mathrm{ab}}} \in \mathrm{Gal}(K^{\mathrm{ab}}/K)$. Fix a complex analytic isomorphism*

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

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

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

(depending of f and σ) so that the following diagram commutes.

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

A proof may be found in [6], II.8.

Remark. As with previous results, this theorem can be extended to deal with elliptic curves whose endormorphism ring is any order in an imaginary quadratic field.

The significance of this theorem lies in how it relates the analytic action of multiplication by s^{-1} to the algebraic action of σ. This idea was present in the background of the proof that $j(E)$ generates the Hilbert class field, and this result can indeed be derived along the same lines from this theorem. However, as far as the author knows, the other classical statements would still require some substantial outside input to prove.

General case of abelian varieties

Theorem 3.10 (The main theorem of complex multiplication)**.** *Let (K, Φ) be a CM-type and $\mathcal{P} = (A, \iota, \mathcal{C})$ a polarized abelian variety of type $(K, \Phi, \mathfrak{a}, \tau)$ with respect to an isomorphism ξ :*

$\mathbb{C}^n/u(a) \to A$. *Fix* $\sigma \in \operatorname{Aut}(\mathbb{C}/K')$ *and choose* $s \in \mathbb{I}_K$ *such that* $\sigma_{|}K'^{\mathrm{ab}} = [s, K']$. *Then there is a unique complex analytic isomorphism*

$$\xi' : \mathbb{C}^n/u(N_\Phi(s)^{-1}\mathfrak{a}) \to \sigma(A)$$

satisfying the following properties.

1. $\sigma(\mathcal{P})$ *is of type* $(K, \Phi, N_\Phi(s)^{-1}\mathfrak{a}, N((s))\tau)$ *with respect to* ξ'.

2. *The following diagram commutes.*

$$\begin{tikzcd}
K/\mathfrak{a} \arrow[r, "N_\Phi(s)^{-1}"] \arrow[d, "\xi\circ u"] & K/N_\Phi(s)^{-1}\mathfrak{a} \arrow[d, "\xi'\circ u"] \\
A \arrow[r, "\sigma"] & \sigma(A)
\end{tikzcd}$$

While the structure of this theorem is similar to the case of elliptic curves, there are clearly a lot of new notions involved. Also, the original work by Shimura and Taniyama is difficult to read because it used the now-obsolete language of Weil's *Foundations*. However, modern expository accounts exist; for instance we refer the reader to [1].

4 The L-function of a CM elliptic curve

4.1 Hecke L-functions

L-functions are not necessarily strictly part of class field theory *per se*, but they are intimately linked to the study of various topics of central importance in class field theory, such as the distribution of primes. Moreover, they were historically essential to the proofs of class field theory ([2]), and one can state an important part of Artin reciprocity as an equality between certain Hecke L-functions and Artin L-functions. We begin by defining Hecke L-functions.

Definition 4.1 (Hecke character). Let K be a number field. A **Hecke character** (or **Grössencharacter**) is a continuous homomorphism

$$\chi : \mathbb{I}_K/K^\times \to \mathbb{C}^\times$$

with image in the unit circle.

For some finite set of primes S containing the infinite primes, a Hecke character will be 1 on $\prod_{v\notin S} U_v$. Given a Hecke character, we can naturally construct an L-function along the same lines of Dirichlet L-functions.

Definition 4.2 (Hecke L-function). Let χ be a Hecke character. Define the corresponding Hecke L-function by

$$L_S(s,\chi) = \sum_{(\mathfrak{a},S)=1} \chi(\mathfrak{a}) \operatorname{Nm}(\mathfrak{a})^{-s} = \prod_{v\notin S} \frac{1}{1-\chi(\pi_v)\operatorname{Nm}(\mathfrak{p}_v)^{-s}}$$

where π_v is an idele that is a uniformizer in the v-position and 1 elsewhere.

If we take S to be the primes ramified in K (along with the infinite primes), then we will denote the resulting Hecke L-function by simply $L(s,\chi)$.

In general, L-functions coming from number theory are expected to admit some analytic continuation and satisfy some functional equation. Hecke proved this using theta functions, and Tate's thesis reproves these statements for Hecke L-functions essentially through Fourier analysis on the adeles.

While Hecke L-functions can be viewed as 'beginning' from the Dirichlet series, one can also arrive at L-functions by beginning with the Euler product. In this way we obtain **Artin L-functions**.

Definition 4.3 (Artin L-function). Let $\rho : \mathrm{Gal}(L/K) \to GL_n(\mathbb{C})$ be an n-dimensional representation of $\mathrm{Gal}(L/K)$. Then we define

$$L(s,\rho) = \prod_{\mathfrak{p} \nmid \Delta_{L/K}} \frac{1}{\det(I_n - \rho(\sigma_{\mathfrak{p}}) \,\mathrm{Nm}(\mathfrak{p})^{-s})}.$$

Artin's conjecture is that the Artin L-finctions have an analytic continuation to the entire complex plane. By Hecke's result, this is true when an Artin L-function coincides with a Hecke L-function. When ρ is a 1-dimensional representation, this occurs because of Artin reciprocity. Indeed, the Artin map gives an isomorphism $C_K/\mathrm{Nm}(C_L) \xrightarrow{\cong} \mathrm{Gal}(L/K)$, so a character of $\mathrm{Gal}(L/K)$ is given by a character of C_K. All the terms in the two expressions match.

The generalization of this equality of L-functions comprises an important part of the Langlands program. One on side, the Artin L-functions can be generalized to motivic L-functions, which come from algebraic geometry, and on the other side, the Hecke L-functions can be generalized to automorphic L-functions, which come from analysis. Obviously, this topic is far outside of the scope of this paper.

4.2 The Hasse-Weil L-function of an elliptic curve

Let K be a number field and let E/K be an elliptic curve. We define the L-function of E by piecing together local L-functions into an Euler product.

Take $\mathfrak{p} \in \mathrm{Spec}\,\mathcal{O}_K$ such that E has good reduction at $\mathfrak{p}$. Let the residue field $\mathcal{O}_K/\mathfrak{p}$ be the finite field $\mathbb{F}_q$. We will define the local L-factor at $\mathfrak{p}$ through the action of Frobenius on the Tate module. Let l be a prime relatively prime to q and consider the map

$$\phi_{\mathfrak{p},l} : T_l(\tilde{E}) \to T_l(\tilde{E})$$

defined by the q-th power Frobenius on $\tilde{E}$. We set the local L-factor at $\mathfrak{p}$ to be the characteristic polynomial of $\phi_{\mathfrak{p},l}$. Because $T_l(\tilde{E}) \cong \mathbb{Z}_l \times \mathbb{Z}_l$, this a degree two polynomial in $\mathbb{Z}_l[T]$. In fact, one can calculate it to be

$$L_{\mathfrak{p}}(E/K,T) = \det(1 - \phi_{\mathfrak{p},l}T) = 1 - a_{\mathfrak{p}}T + qT^2,$$

where $a_{\mathfrak{p}} = q + 1 - \#\tilde{E}(\mathbb{F}_q)$.

For the primes of bad reduction, we set

$$L_{\mathfrak{p}}(E/K,T) = \begin{cases} 1-T & \text{split multiplicative reduction at } \mathfrak{p}, \\ 1+T & \text{non-split multiplicative reduction } at \mathfrak{p}, \\ 1 \quad \text{additive reduction } at \mathfrak{p}. \end{cases}$$

Definition 4.4. The Hasse-Weil L-function of E/K is defined by the Euler product

$$L(E/K,s) = \prod_{\mathfrak{p} \in \mathrm{Spec}\,\mathcal{O}_K} L_{\mathfrak{p}}(E/K, q^{-s})^{-1}.$$

The Hasse bound states that $|a_{\mathfrak{p}}| \leq 2\sqrt{q}$, and can be used to show that the Hasse-Weil L-function converges and gives an analytic function for all s with $\Re(s) > \frac{3}{2}$. In fact, as a consequence of the modularity theorem, we know that the Hasse-Weil L-function as an analytic continuation to the entire complex plane and satisfies an expected functional equation relating its values at s and $2-s$. In the next section, we will sketch a proof of this fact for elliptic curves with complex multiplication by interpreting their L-functions as products of Hecke L-functions. As noted earlier, then Hecke's result on the analytic continuation and functional equation will apply to the Hasse-Weil L-functions.

4.3 The Hecke character associated to a CM elliptic curve

Take $E/L \in \mathrm{Ell}(\mathcal{O}_K)$. We will describe the construction of a Hecke character $\psi_{E/L} : \mathbb{I}_L \to \mathbb{C}^*$ satisfying the following property.

- If $K \subset L$, then
$$L(E/L, s) = L(s, \psi_{E/L}) L(s, \overline{\psi_{E/L}}).$$
- If $K \not\subset L$, then let $L' = LK$. Then
$$L(E/L, s) = L(s, \psi_{E/L'}).$$

Note that here, L denotes the field of definition as well as the L-function!

The proof of the claim above can be found in [6], II.10. We now construct the desired Hecke character attached to E/L as follows.

Let $x \in \mathbb{I}_L$ be an idele and let $s = \mathrm{Nm}_{L/K}(x) \in \mathbb{I}_K$. Then we claim there is a unique element $\alpha \in K^\times$ with the following two properties:

- $\alpha\mathcal{O}_K = (s) \subset K$.
- For any fractional ideal $\mathfrak{a} \subset K$ and any analytic isomorphism
$$f : \mathbb{C}/\mathfrak{a} \to E(\mathbb{C}),$$
the following diagram commutes.

$$\begin{tikzcd} K/\mathfrak{a} \arrow[r, "\alpha s^{-1}"] \arrow[d, "f"] & K/\mathfrak{a} \arrow[d, "f"] \\ E(L^{\mathrm{ab}}) \arrow[r, "\phi_L(x)"] & \sigma(E(L^{\mathrm{ab}})) \end{tikzcd}$$

Remark. We recall that the fractional ideal of an idele s is defined as
$$(s) = \prod_{\mathfrak{p}} \mathfrak{p}^{\nu_{\mathfrak{p}}(s_{\mathfrak{p}})}.$$

The proof of this claim primarily uses the main theorem of complex multiplication (for elliptic curves). The significance of this assignment $\alpha_{E/L} : x \mapsto \alpha$ is that we have defined a homomorphism $\mathbb{I}_L \to K^\times$ that encodes the action of x via Artin reciprocity on relevant points of E. This is not a Hecke character, though, because we do not have $\alpha_{E/L}(L^\times) = 1$. We make the following modification:

$$\psi_{E/L} : \mathbb{I}_L \to \mathbb{C}^\times, \qquad x \mapsto \alpha_{E/L}(x)\,\mathrm{Nm}_{L/K}(x^{-1})_\infty.$$

Then $\psi_{E/L}$ is the desired Hecke character associated to E/L.

References

[1] Margaret Bilu. *Complex multiplication of abelian varieties*. Expository paper.
https://pub.ist.ac.at/~mbilu/Complexmultiplication.pdf

[2] James Cogdell. *On Artin L-functions*. Expository paper.
https://people.math.osu.edu/cogdell.1/artin-www.pdf.

[3] David Cox. *Primes of the form* $x^2 + ny^2$. Published by John Wiley & Sons, Inc. 2nd edition, 2013.

[4] Neal Koblitz. *Introduction to Elliptic curves and modular forms*. Published by Springer-Verlag New York, Inc. 1984.

[5] Joseph Silverman. *The Arithmetic of Elliptic Curves*. Publishedby Springer Science+Business Media, LLC. 2nd edition, 2009.

[6] Joseph Silverman. *Advanced Topics in the Arithmetic of Elliptic Curves*. Publishedby Springer Science+Business Media New York, Inc. 1994.

[7] Jean-Pierre Serre, John Tate. *Good Reduction of Abelian Varieties*. *The Annals of Mathematics*, Second Series, Volume 68, Issue 3. Nov. 1968. Pages 492-517.

[8] Goro Shimura and Yutaka Taniyama. *Complex multiplication of abelian varieties and its applications to number theory*. The Mathematical Society of Japan, 1961.

[9] Andrew Sutherland, *Number Theory 1*. Online course notes.
https://math.mit.edu/classes/18.785/2019fa/

[10] James Milne, *Class Field Theory*. Online course notes.
https://www.jmilne.org/math/CourseNotes/cft.html