COMPLEX MULTIPLICATION

YUNHAN (ALEX) SHENG

Abstract. Given an abelian extension of a number field K, what can be said about the set of algebraic numbers that generates the extension over K? This is known as Hilbert's twelfth problem. A special case of the problem, known as the theory of complex multiplication, is when K is a totally imaginary quadratic extension of a totally real field number field. We shall give some motivation in Section 1, before delving into the theory of complex multiplication of elliptic curves and abelian varieties in Sections 2 and 3, respectively.

Contents

1. Introduction

We assume that the readers are familiar with elliptic curves, although we will briskly gather the relevant concepts necessary to state the main result. A detailed exposition of the following can be found in Silverman's text [13].

By an *elliptic curve* E, we understand a one-dimensional nonsingular projective variety of genus one, together with a special point $O \in E$. An elliptic curve E is defined over a field K, and is denoted by E/K, if its homogeneous ideal

$$I(E) = \{f \in \overline{K}[X] : f \text{ is homogenous and } f(P) = 0 \text{ for all } P \in E\}$$

is generated by homogeneous polynomials in $K[X]$. Here and in what follows, $\overline{K}$ will always denote the algebraic closure of K. The absolute Galois group $\mathrm{Gal}(\overline{K}/K)$ acts on E by acting on the the homogenous coordinates of its underlying projective plane $\mathbf{P}^2_K$. The set of K-rational points of E is

$$E(K) = \left\{P \in V : P^\sigma = P \text{ for all } \sigma \in \mathrm{Gal}(\overline{K}/K)\right\}.$$

More concretely, each elliptic curve E/K can be embedded into $\mathbf{P}^2_K$ so that it is given by a so-called *Weierstrass equation*

$$Y^2Z + a_1XYZ + a_3YZ^2 = X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^6, \quad a_1, \cdots, a_6 \in K.$$

The special point O has coordinate $[0:1:0]$. Conversely, every smooth cubic curve defined by an equation as such is an elliptic curve E/K with $O = [0:1:0]$. We shall tacitly assume that $\mathrm{char}(\overline{K}) \neq 2, 3$, in which case the Weierstrass equation can be reduced via linear substitution to a simpler form:

$$Y^2Z = X^3 + AXZ^2 + BZ^3, \quad A, B \in K.$$

Two elliptic curves are isomorphic if and only if they have the same *j-invariant*, which is defined by

$$j(E) = -1728(4A)^3/\Delta, \quad \text{where } \Delta = -16(4A^3 + 27B^2).$$

An elliptic curve is endowed with a group structure with points of E as elements. Using the group law, we may define the *multiplication-by-m map* on E by

$$[m] : P \mapsto mP := \underbrace{P + P + \ldots + P}_{m \text{ times}}.$$

An *isogeny* ϕ between two elliptic curves E_1 and E_2 is a morphism of varieties satisfying $\phi(O) = O$. For instance, $[m] : E \to E$ is an isogeny. Consider the ring $\mathrm{End}(E)$ of isogenies from E to itself, such as $[m]$. A natural question to ask is:

Question. Is every element of $\mathrm{End}(E)$ of the form $[m]$ for some $m \in \mathbf{Z}$, or is $\mathrm{End}(E)$ strictly larger than $\mathbf{Z}$?

This question is answered in Theorem 1.1. We need the following definition.

Definition. Let K be a number field, i.e., a finite extension of $\mathbf{Q}$. An *order* R of K is a subring of K that is finitely generated as $\mathbf{Z}$-module and spans K over $\mathbf{Q}$.

For example, $\mathbf{Z}[i]$ and $\{a + 2bi : a, b \in \mathbf{Z}\}$ are both orders of $\mathbf{Q}(i)$. In fact, the ring of integers is the largest order of a number field.

Theorem 1.1. *Let $E/\mathbf{C}$ be an elliptic curve. Then either $\mathrm{End}(E) = \mathbf{Z}$ or $\mathrm{End}(E)$ is isomorphic to an order of $\mathbf{Q}(\sqrt{-D})$ for some integer $D > 0$.*

For this theorem, we need some facts about elliptic curves over $\mathbf{C}$. A lattice $\Lambda \subset \mathbf{C}$ is a discrete subgroup of $\mathbf{C}$ that spans $\mathbf{C}$ over $\mathbf{R}$. Two lattices $\Lambda_1, \Lambda_2 \subset \mathbf{C}$ are *homothetic* if $\Lambda_2 = \alpha\Lambda_1$ for some $\alpha \in \mathbf{C}^\times$. For any elliptic curve $E/\mathbf{C}$, there is a lattice $\Lambda \subset \mathbf{C}$ unique up to homothety such that there is a Lie group isomorphism $\mathbf{C}/\Lambda \cong E(\mathbf{C})$. The complex-analytic map $\mathbf{C}/\Lambda \to E(\mathbf{C})$ is referred to as a *uniformization*. In fact, there is an equivalence of categories between

(1) elliptic curves over $\mathbf{C}$ with isogenies, and
(2) lattices $\Lambda \subset \mathbf{C}$ up to homothety with

$$\mathrm{Hom}(\Lambda_1, \Lambda_2) = \{\alpha \in \mathbf{C} : \alpha\Lambda_1 \subset \Lambda_2\}.$$

Proof of Theorem 1.1. Let $\Lambda \subset \mathbf{C}$ be the lattice associated to $E/\mathbf{C}$. Then up to homothety, we may replace Λ by the lattice $\mathbf{Z} + \tau\mathbf{Z}$ for some $\tau \in \mathbf{C} \setminus \mathbf{R}$. Since $\mathrm{End}(E) \cong \{\alpha \in \mathbf{C} : \alpha\Lambda = \Lambda\}$, for any $\alpha \in \mathrm{End}(E)$ there exist $m, n, p, q \in \mathbf{Z}$ such that $\alpha = m + n\tau$ and $\alpha\tau = p + q\tau$. Eliminating τ from these equations yields

$$\alpha^2 - (m + q)\alpha + mq - np = 0,$$

which shows that $\mathrm{End}(E)$ is an integral extension of $\mathbf{Z}$. Suppose $\alpha \in \mathrm{End}(E)$ but $\alpha \notin \mathbf{Z}$. Then $n \neq 0$, and eliminating α from the equation above gives

$$n\tau^2 + (m-q)\tau - p = 0.$$

Since $\tau \notin \mathbf{R}$ by construction, this shows that $\mathbf{Q}(\tau)/\mathbf{Q}$ is imaginary quadratic, and thus is of the form $\mathbf{Q}(\sqrt{-D})$ for some integer $D > 0$. Now $\mathrm{End}(E) \otimes \mathbf{Q} = \mathbf{Q}(\tau)$ verifies that $\mathrm{End}(E)$ is an order. □

Definition. An elliptic curve $E/\mathbf{C}$ has *complex multiplication* (or CM for short) *by* R if $R = \mathrm{End}(E)$ is an order of an imaginary quadratic field $\mathbf{Q}(\sqrt{-D})$.

Now we are ready to state our main result. We assume familiarity with algebraic number theory and with the statements of class field theory. For reference of the former, see Sutherland [14]; for the latter see Poonen [7] and Kedlaya [3].

Recall the Kronecker-Weber theorem, which says that the ray class field of $\mathbf{Q}$ of conductor $N\infty$ is generated by a primitive Nth root of unity ζ_N. In particular, the maximal abelian extension (absolute class field) of $\mathbf{Q}$ is the union of all cyclotomic extensions of $\mathbf{Q}$. Recall also the Hermite-Minkowski theorem, which says that the maximal unramified extension (Hilbert class field) of $\mathbf{Q}$ is just $\mathbf{Q}$ itself. In other words, there are no proper unramified extensions over $\mathbf{Q}$. The theory of complex multiplication provides an analogue of these results with base field $\mathbf{Q}(\sqrt{-D})$ in place of $\mathbf{Q}$. Specifically:

Theorem 1.2. *Let R be an order of an imaginary quadratic field $K/\mathbf{Q}$. Let $E/\mathbf{C}$ be an elliptic curve with CM by R. Then*

(i) $K(j(E))$ is the maximal unramified extension of K;
(ii) if $x(E_{\mathrm{tors}})$ is the set of x-coordinates of torsion points (i.e., points of finite order) of E, then $K(j(E), x(E_{\mathrm{tors}}))$ is the maximal abelian extension of K.

For (ii) we assume that $j(E) \neq 0, 1728$. Note that the group law on elliptic curves allows one to talk about the order of points.

Section 2 of this paper is devoted to proving Theorem 1.2. The upshot is that studying intrinsically *geometric* objects such as elliptic curves yields fruitful *arithmetic* information. This is the *idée fixe* of complex multiplication. In Section 3 we study abelian varieties, which are generalizations of elliptic curves, and from which even more arithmetic information will be extracted.

2. CM of Elliptic Curves

In what follows, K will always denote an imaginary quadratic field, and $\mathrm{Ell}(R)$ the space of all elliptic curves $E/\mathbf{C}$ with CM by R. We also assume that R is the ring of integers of K, though this is not always necessary. The main reference for our exposition is Silverman [12].

2.1. From algebraic action to analytic action.

The goal of this subsection is to establish two important actions on $\mathrm{Ell}(R)$, one analytic and one algebraic. This sets up for the proof of Theorem 1.2 in the subsequent subsections.

We start with an easy observation: a nonzero fractional ideal $\mathfrak{a}$ of K is a lattice in $\mathbf{C}$, and thus gives rise to an elliptic curve $E_{\mathfrak{a}}/\mathbf{C}$ with CM by R. Two lattices are homothetic if as ideals they belong to the same ideal class. This leads us to consider the ideal class group $\mathrm{Cl}(R)$ of R. Let $\overline{\mathfrak{a}}$ be the image of $\mathfrak{a}$ in $\mathrm{Cl}(R)$.

Proposition 2.1. *There is a simply transitive action of* $\mathrm{Cl}(R)$ *on* $\mathrm{Ell}(R)$ *via*

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

Therefore $\#\mathrm{Ell}(R) = \#\mathrm{Cl}(R)$. *In particular* $\mathrm{Ell}(R)$ *is finite.*

Proof. See Silverman [12] □

The action of $\overline{\mathfrak{a}}$ is analytic, inducing a complex-analytic map $\mathbf{C}/\Lambda \to \mathbf{C}/\mathfrak{a}^{-1}\Lambda$. The kernel of this isogeny $E_\Lambda \to E_{\mathfrak{a}^{-1}\Lambda}$ is the *group of* $\mathfrak{a}$*-torsion points*

$$E[\mathfrak{a}] = \{P \in E : \alpha P = 0 \text{ for all } \alpha \in \mathfrak{a}\},$$

which is a free $R/\mathfrak{a}$-module of rank one, and thus $\#E[\mathfrak{a}] = \mathrm{Nm}_{K/\mathbf{Q}}\,\mathfrak{a}$. A proof of this assertion may be found in Silverman [12].

Now we turn to study the algebraic action of $\mathrm{Gal}(\overline{K}/K)$ on $\mathrm{Ell}(R)$. However, elliptic curves in $\mathrm{Ell}(R)$ are defined over $\mathbf{C}$, not K. So necessarily we need the following lemma to modify the field of definition.

Lemma 2.2. *The* j*-invariant of* $E \in \mathrm{Ell}(R)$ *is an algebraic number.*

Proof. Since $\mathrm{End}(E^\sigma) = \mathrm{End}(E)$ for any $\sigma \in \mathrm{Aut}(\mathbf{C})$, by Propostion 2.1 E^σ is one of the finitely many isomorphism classes of elliptic curves determined by $j(E^\sigma)$. Since the action of σ naturally extends to the j-invariant, we have $j(E^\sigma) = j(E)^\sigma$, which takes on only finitely many values as σ ranges over $\mathrm{Aut}(\mathbf{C})$. The claim now follows from the fact that $[\mathbf{Q}(j(E)) : \mathbf{Q}]$ is finite. □

Remark 2.3. An important observation from the proof of Lemma 2.2 is that $[\mathbf{Q}(j(E)) : \mathbf{Q}] \le h$, where $h = \#\mathrm{Cl}(R)$ is the class number of K. This will be used later in Section 2.2, where we shall obtain the equality $[\mathbf{Q}(j(E) : \mathbf{Q}] = h$. Another fact is that $j(E)$ is actually an algebraic integer, though we won't proof this.

For $E \in \mathrm{Ell}(R)$, consider the *universal elliptic curve* $E'/K(j(E))$ given by

$$y^2 + xy = x^3 - \frac{36}{j - 1728}x - \frac{1}{j - 1728},$$

which has the same j-invariant as E, $j(E') = j(E)$. Hence, $\mathrm{Ell}(R)$ can be identified with $\overline{\mathbf{Q}}$-isomorphism classes of elliptic curves $E/\overline{\mathbf{Q}}$ with CM by R obtained by identifying elliptic curves with same j-invariant. Hereafter, we shall tacitly assume that each element of $\mathrm{Ell}(R)$ has a model defined over $\overline{\mathbf{Q}}$.

For the next lemma, recall that a morphism φ of varieties is defined over a field L if $\varphi^\sigma = \varphi$ for all $\sigma \in \mathrm{Gal}(\overline{L}/L)$.

Lemma 2.4. *Let* E, E' *be elliptic curves defined over a field* $L \subset \mathbf{C}$. *Then*

(i) if $E \in \mathrm{Ell}(R)$, *then every element in* $\mathrm{End}(E)$ *is defined over* RL;
(ii) there exists a finite extension L'/L *such that every element in* $\mathrm{Hom}(E, E')$ *is defined over* L'.

Proof. See Silverman [12]. □

Since an elliptic curve $E \in \mathrm{Ell}(R)$ has a model defined over $\overline{\mathbf{Q}}$, every element in $\mathrm{End}(E)$ is defined over $R\overline{\mathbf{Q}} = \overline{\mathbf{Q}}$. Now it makes sense to talk about the $\mathrm{Gal}(\overline{K}/K)$-action on $\mathrm{Ell}(R)$. Since the action of $\mathrm{Cl}(R)$ is simply transitive by Proposition 2.1, for each $\sigma \in \mathrm{Gal}(\overline{K}/K)$ there exists a unique $\overline{\mathfrak{a}} \in \mathrm{Cl}(R)$ such that $E^\sigma = \overline{\mathfrak{a}} * E$. This defines a map $F : \mathrm{Gal}(\overline{K}/K) \to \mathrm{Cl}(R)$ which transfers the algebraic action into an analytic one.

Theorem 2.5. *The map $F : \mathrm{Gal}(\overline{K}/K) \to \mathrm{Cl}(R)$ characterized by $E^\sigma = F(\sigma) * E$ is a well-defined injective group homomorphism.*

Proof sketch. To see that F does not depend on the choice of E, let $E_1, E_2 \in \mathrm{Ell}(R)$ and suppose that $E_1^\sigma = \overline{\mathfrak{a}}_1 * E_1$ and $E_2^\sigma = \overline{\mathfrak{a}}_2 * E_2$. Since $\mathrm{Cl}(R)$ acts transitively on $\mathrm{Ell}(R)$, there exists some $\overline{\mathfrak{b}}$ such that $E_2 = \overline{\mathfrak{b}} * E_1$. Hence

$$(\overline{\mathfrak{b}} * E_1)^\sigma = \overline{\mathfrak{a}}_2 * (\overline{\mathfrak{b}} * E_1) = (\overline{\mathfrak{a}}_2 \overline{\mathfrak{b}} \overline{\mathfrak{a}}_1^{-1}) * E_1^\sigma.$$

It remains to show that $(\overline{\mathfrak{a}} * E)^\sigma = \overline{\mathfrak{a}}^\sigma * E^\sigma$. We know that if R is a Dedekind domain with fractional ideal $\mathfrak{a}$, then $\mathfrak{a}^{-1}M \cong \mathrm{Hom}_R(\mathfrak{a}, M)$ for M a torsion-free R-module (see Silverman [12]). Therefore $\mathrm{Hom}_R(\mathfrak{a}, \Lambda) = \mathfrak{a}^{-1}\Lambda$ and $\mathrm{Hom}_R(\mathfrak{a}, \mathbf{C}) = \mathfrak{a}^{-1}\mathbf{C} = \mathbf{C}$. The idea is that we want to describe $\mathrm{Hom}_R(\mathfrak{a}, E)$ as an algebraic group, not merely as an R-module. Let

$$P : R^m \xrightarrow{A} R^n \to \mathfrak{a} \to 0, \qquad Q : 0 \to \Lambda \to \mathbf{C} \to E \to 0$$

be two exact sequences and consider the double complex $\mathrm{Hom}_R(P, Q)$ spanned by P and Q. Applying the snake lemma we obtain another exact sequence

$$0 \to \mathfrak{a}^{-1}\Lambda \to \mathbf{C} \to \ker(E^n \xrightarrow{A^\intercal} E^m) \to \Lambda^n / A^\intercal \Lambda^m,$$

where $A^\intercal$ is the transpose of A. Since $\mathfrak{a} * E = \mathbf{C}/\mathfrak{a}^{-1}\Lambda$ is connected and $\Lambda^n/A^\intercal\Lambda^m$ is discrete, we conclude that $\mathfrak{a} * E$ is the identity component of $\ker A^\intercal$, which is a subvariety of E^n. Now since σ commutes with $A^\intercal : E^n \to E^m$, the map F is indeed well-defined. To check that F is an injective group homomorphism is routine. □

The crux of the proof of Theorem 2.7 is the following finiteness result of Proposition 2.6, which says that only finitely many primes are "bad". As is often the case, the finiteness result is used in conjunction with Chebotarev's density theorem (which is essentially an infiniteness result, see for example Sutherland[14]) in the following way: since there are infinitely many primes of the same Galois conjugacy class, it doesn't hurt discarding only finitely many "bad" ones. To describe what constitutes as "bad" in the case at hand, we recall the definition of a Frobenius element.

Let L/K be a Galois extension and $\mathfrak{P}$ a prime lying over an unramified prime $\mathfrak{p}$ of K. Let $\kappa_\mathfrak{P}$ and $\kappa_\mathfrak{P}$ be the corresponding residue fields. The *Frobenius element* $\sigma_\mathfrak{P} \in \mathrm{Gal}(L/K)$ is the generator of $\mathrm{Gal}(\kappa_\mathfrak{P}/\kappa_\mathfrak{p})$. If L/K is abelian, then $\sigma_\mathfrak{P} = \sigma_{\mathfrak{P}'}$ for any other prime $\mathfrak{P}'$ lying over $\mathfrak{p}$, so we simply write $\sigma_\mathfrak{p}$ for $\sigma_\mathfrak{P}$.

Proposition 2.6. *There is a finite set of rational primes $S \subset \mathbf{Z}$ such that if $p \notin S$ is a prime that splits completely in K, say $pR = \mathfrak{p}\mathfrak{p}'$, then $F(\sigma_\mathfrak{p}) = \overline{\mathfrak{p}}$.*

Proof. By Lemma 2.4, there is a finite extension L/K over which both a complete set $\{E_i\}$ of representatives of $\overline{K}$-homomorphism classes in $\mathrm{Ell}(R)$ and the isogenies in between are defined. Let S be the set of rational primes p that satisfy one of the following conditions

(i) p ramifies in L;
(ii) E_i has bad reduction at some prime $\mathfrak{P}$ of L for some i;
(iii) $\mathrm{Nm}_{L/\mathbf{Q}}(j(E_i) - j(E_k))$ contains some nonzero integer multiple of p for $i \neq k$.

Then S is finite. Now suppose that $p \notin S$ and $p = \mathfrak{p}\mathfrak{p}'$ in K. Let $\mathfrak{P}$ be a prime of L lying over $\mathfrak{p}$. Let $\mathfrak{a} \subset R$ be an integral ideal such that $(\mathfrak{a}, p) = 1$ and $\mathfrak{a}\mathfrak{p} = (\alpha)$ for

some $\alpha \in K^\times$. We have the following commutative diagram

$$\begin{array}{ccccccc} \mathbf{C}/\Lambda & \xrightarrow{z\mapsto z} & \mathbf{C}/\mathfrak{p}^{-1}\Lambda & \xrightarrow{z\mapsto z} & \mathbf{C}/\mathfrak{a}^{-1}\mathfrak{p}^{-1}\Lambda = \mathbf{C}/(\alpha^{-1})\Lambda & \xrightarrow{z\mapsto \alpha z} & \mathbf{C}/\Lambda \\ \downarrow & & \downarrow & & \downarrow & & \downarrow \\ E & \xrightarrow{\phi} & \overline{\mathfrak{p}} * E & \xrightarrow{\psi} & \overline{\mathfrak{a}} * \overline{\mathfrak{p}} * E = (\alpha) * E & \xrightarrow{\lambda} & E \end{array},$$

where the vertical maps are uniformizations. Let ω be the invariant differential (see Silverman [13]) of E. Then tracing around the diagram we get $(\lambda \circ \psi \circ \phi)^*\omega = \alpha\omega$. Since $\mathfrak{P} \mid \alpha$, in the reduction modulo $\mathfrak{P}$ we have

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

instead, so $\tilde{\lambda} \circ \tilde{\psi} \circ \tilde{\phi}$ is inseparable, as a nonconstant map of curves is separable if and only if the induced map on differentials is nonzero. By definition of ψ,

$$\deg \psi = \#E[\mathfrak{a}] = \mathrm{Nm}_{K/\mathbf{Q}}\, \mathfrak{a}.$$

Since the reduction $\mathrm{Hom}(E_1, E_2) \to \mathrm{Hom}(\tilde{E}_1, \tilde{E}_2)$ is injective and thus preserves degrees (see Proposition II.4.4 of Silverman [12]), we obtain

$$\deg \tilde{\psi} = \deg \psi = \mathrm{Nm}_{K/\mathbf{Q}}\, \mathfrak{a},$$

which is prime to p, so that $\tilde{\psi}$ is separable. Similarly, since $\deg \tilde{\lambda} = \deg \lambda = 1$, $\tilde{\lambda}$ is also separable, which implies that $\tilde{\phi}$ is inseparable. Any inseparable map factors through a p-th power Frobenius map (see Silverman [13]), but since

$$\deg \tilde{\phi} = \deg \phi = \mathrm{Nm}_{K/\mathbf{Q}}\, \mathfrak{p} = p,$$

$\tilde{\phi}$ must be the p-th power Frobenius map, that is, $\tilde{E}^{(p)} \cong \overline{\mathfrak{p}} * E$. Hence

$$j(\overline{\mathfrak{p}} * E) = j(E)^p = j(E)^{\mathrm{Nm}_{K/\mathbf{Q}}\, \mathfrak{p}} \equiv j(E)^{\sigma_\mathfrak{p}} = j(E^{\sigma_\mathfrak{p}}) = j(F(\sigma_\mathfrak{p}) * E) \pmod{\mathfrak{P}}.$$

Since $p \notin S$, $j(E_i) \cong j(E_k) \pmod{\mathfrak{P}}$ if and only if $E_i \cong E_k$, so $\overline{\mathfrak{p}} * E = F(\sigma_\mathfrak{p}) * E$. But $\mathrm{Cl}(R)$ acts simply on $\mathrm{Ell}(R)$, so $\overline{\mathfrak{p}} = F(\sigma_\mathfrak{p})$. □

2.2. **Constructing the Hilbert class field.** The goal of this subsection is to prove the first half of Theorem 1.2, which is contained in Theorem 2.7. Recall that elliptic curves in $\mathrm{Ell}(R)$ have well-defined models over $\overline{\mathbf{Q}}$.

Theorem 2.7 (Weber-Fueter)**.** *Let $E/\overline{\mathbf{Q}} \in \mathrm{Ell}(R)$. Then*

(i) $K(j(E))$ is the Hilbert class field H of K;
(ii) $[\mathbf{Q}(j(E)) : \mathbf{Q}] = [K(j(E)) : K] = h$, where $h = \#\mathrm{Cl}(R)$ is the class number;
(iii) let $E_1, \cdots, E_r$ be a complete set of representatives for $\mathrm{Ell}(R)$. Then $j(E_1), \cdots, j(E_r)$ is a complete set of conjugates for $j(E)$ under $\mathrm{Gal}(\overline{K}/K)$.

Before diving into the proof, let us recall some concepts from algebraic number theory. They can be read in detail from Sutherland [14]. A *modulus* $\mathfrak{m}$ of K is a formal product

$$\mathfrak{m} = \prod_v v^{e_v}$$

where the product is taken over all places v of K. The exponent $e_v \in \mathbf{Z}$ are zero for all but finitely many v's. In particular, if v is a real place, then $e_v \in \{0, 1\}$, and if v is a complex place then $e_v = 0$. Intuitively, one thinks of a modulus as a briefcase of data of an integral ideal of $\mathcal{O}_K$ along with a subset of real places.

The concept of modulus is applied in the classical version of global class field theory. Let L/K be an abelian extension. Let $\mathfrak{m}$ be a modulus of K that is divisible by all primes that ramify in L/K. Let $I(\mathfrak{m})$ be the group of fractional ideals of K coprime to $\mathfrak{m}$. The global Artin map

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

sends $\mathfrak{p}$ to $\sigma_{\mathfrak{p}}$. Then *Artin Reciprocity* claims that

$$P(\mathfrak{m}) = \{(\alpha) : \alpha \in K^*, \alpha \equiv 1 \,(\mathrm{mod}\, \mathfrak{m})\}$$

is in the kernel of the $\Theta_{L/K}$ for some appropriate choice of $\mathfrak{m}$. The smallest such $\mathfrak{m}$ is called the *conductor* of L/K, which we denote by $\mathfrak{m}_{L/K}$. Roughly speaking, the conductor is the minimal compilation of "bad" primes multiplied together.

Proof. (i) Let L be the fixed field of the kernel of $F : \mathrm{Gal}(\overline{K}/K) \to \mathrm{Cl}(R)$. Then

$$\begin{aligned}\mathrm{Gal}(\overline{K}/L) &= \{\sigma \in \mathrm{Gal}(\overline{K}/K) : E^\sigma = E\} \\ &= \{\sigma \in \mathrm{Gal}(\overline{K}/K) : j(E)^\sigma = j(E)\} = \mathrm{Gal}(\overline{K}/K(j(E))).\end{aligned}$$

Hence $L = K(j(E))$. Since F is injective, $K(j(E))/K$ is abelian. Consider

$$I(\mathfrak{m}_{L/K}) \xrightarrow{\Theta_{L/K}} \mathrm{Gal}(L/K) \xrightarrow{F} \mathrm{Cl}(R) \ .$$

For any $\mathfrak{a} \in I(\mathfrak{m}_{L/K})$, by Chebotarev's density theorem (Sutherland [14] Theorem 28.9) there exist infinitely many primes in $I(\mathfrak{m}_{L/K})$ in the same $P(\mathfrak{m}_{L/K})$-class as $\mathfrak{a}$ that split completely in L. Choose one such $\mathfrak{p} \in I(\mathfrak{m}_{L/K})$ that does not lie over any primes in the finite set S described in Proposition 2.6. That is, there exists $\alpha \in K^\times$ such that $\mathfrak{a} = \alpha\mathfrak{p}$ and $\alpha \equiv 1 \mod \mathfrak{m}_{L/K}$. Hence by Proposition 2.6,

$$F \circ \Theta_{L/K}(\mathfrak{a}) = F \circ \Theta_{L/K}(\mathfrak{p}) = \overline{\mathfrak{p}} = \overline{\mathfrak{a}},$$

so that $F \circ \Theta_{L/K}$ is just the natural projection. Therefore, any principal ideal $(\alpha) \in I(\mathfrak{m}_{L/K})$ is in the kernel of $F \circ \Theta_{L/K}$, and thus $(\alpha) \in \ker \Theta_{L/K}$, as F is injective. But $\mathfrak{m}_{L/K}$ is the smallest modulus $\mathfrak{m}$ for which $\mathfrak{m} \mid \alpha - 1$ implies $\Theta_{L/K}((\alpha)) = 1$, so $\mathfrak{m}_{L/K} = (1)$. Since $\mathfrak{m}_{L/K}$ is divisible by primes that ramify in L, we conclude that L/K is unramified.

On the other hand, since $I(\mathfrak{m}_{L/K}) = I((1)) \to \mathrm{Cl}(R)$ is surely surjective, F is also surjective. Therefore

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

which shows that $L = H$, the Hilbert class field of K.

(ii) By (i) we have $[K(j(E)) : K] = h$. We also have $[\mathbf{Q}(j(E)) : \mathbf{Q}] \leq h$ by Remark 2.3. Hence $[\mathbf{Q}(j(E)) : \mathbf{Q}] = h$ follows from the following diagram

$$\begin{array}{ccc} & & K(j(E)) \\ & \overset{h}{\nearrow} & \big| \leq 2 \\ K & & \mathbf{Q}(j(E)) \\ 2 \big| & \nearrow_{\leq h} & \\ \mathbf{Q} & & \end{array} .$$

(iii) Since $F : \mathrm{Gal}(\overline{K}/K) \to \mathrm{Gal}(L/K) \cong \mathrm{Cl}(R)$ is surjective, $\mathrm{Gal}(\overline{K}/K)$ acts transitively on a complete set of representatives of $\mathrm{Ell}(R)$. □

Corollary 2.8 (Hasse)**.** *For any nonzero fractional ideal* $\mathfrak{a}$ *of* K*,*

$$j(E)^{\Theta_{L/K}(\mathfrak{a})} = j(\overline{\mathfrak{a}} * E).$$

Here $\Theta_{L/K}(\mathfrak{a})$ acting on E is an algebraic action of the Galois group on an algebraic number. This corollary translates this purely Galois-theoretic algebraic action into a lattice action on E as an analytic object. This is a recurring theme in the theory of complex multiplication.

2.3. **Constructing the absolute class field.** In this section we prove the second half of Theorem 1.2, which is achieved in Theorem 2.9. We denote the Hilbert class field of K by H. Recall from the previous subsection that $H = K(j(E))$.

Definition. Let $E/H \in \mathrm{Ell}(R)$ be given by (assuming $\mathrm{char}(\overline{K}) \neq 2, 3$)

$$y^2 = x^3 + Ax + B, \quad A, B \in H.$$

Define the *Weber function* to be the map $h : E/H \to \mathbf{P}^1$ given by

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

In Theorem 1.2 we made the assumption that $j(E) \neq 0, 1728$. With the help of the Weber function, this assumption can be relaxed. Indeed, $j(E) \neq 0, 1728$ is equivalent to saying $AB \neq 0$, in which case taking the x-coordinate of torsion points suffices. However, if $j(E) = 1728$, in which case $B = 0$, then $u^4 = 1$, where u is such that every automorphism of E is given by a substitution $x = u^2 x'$ with $u^{-4}A = A$ and $u^{-6}B = B$ (see Silverman [13] Chapter III §10). To kill the additional automorphisms that give no additional arithmetic information, we need to take x^2 instead of x. Similarly if $j(E) = 0$, in which case $A = 0$, then we need to take x^3 to account for the redundancy. Therefore, taking the Weber function guarantees $\mathrm{Aut}(E)$-invariance, a crucial property that will be used later.

Theorem 2.9. *Let* $E/H \in \mathrm{Ell}(R)$*. If* $\mathfrak{m}$ *is a modulus of* K*, then* $K(j(E), h(E[\mathfrak{m}]))$ *is the ray class field of* $\mathfrak{m}$*. In particular,* $K(j(E), E_{\mathrm{tors}}))$ *is the maximal abelian extension (i.e., absolute class field) of* K*.*

The proof depends heavily on the following Frobenius lifting lemma.

Lemma 2.10. *Let* $p \mid \mathfrak{p} \mid \mathfrak{P}$ *be a tower of primes in* $\mathbf{Q} \subset K \subset H$*. Suppose that* $E/H \in \mathrm{Ell}(R)$*. For all but finitely many primes* $\mathfrak{p}$ *of* K *that satisfy* $\Theta_{H/K}(\mathfrak{p}) = 1$*, the* p*-th power Frobenius map* ϕ *on the reduction* $\tilde{E}$ *of* E *mod* $\mathfrak{P}$ *lifts to a unique* $\pi \in R$ *such that* $\mathfrak{p} = \pi R$ *and the following diagram commute:*

$$\begin{array}{ccc} E & \xrightarrow{\pi} & E \\ \downarrow & & \downarrow \\ \tilde{E} & \xrightarrow{\phi} & \tilde{E} \end{array} . \tag{2.11}$$

Proof sketch. Excluding finitely many primes $p \in S$ as in the proof of Proposition 2.6, we get a purely inseparable map

$$\tilde{E} \to \widetilde{\overline{\mathfrak{p}} * E} \cong \widetilde{E^{\sigma_{\mathfrak{p}}}}$$

of degree p, which factors through ϕ followed by a map ϵ of degree one:

$$\tilde{E} \xrightarrow{\phi} \tilde{E}^{(p)} \xrightarrow{\epsilon} \widetilde{E^{\sigma_\mathfrak{p}}} \ .$$

We wish to show that $\tilde{E}^{(p)}$ lifts directly to $E^{\sigma_\mathfrak{p}}$, that is, ϵ is an automorphism. It suffices to show that ϵ is the reduction of some $\epsilon_0 \in \mathrm{Aut}(E^{\sigma_\mathfrak{p}})$,

$$\begin{array}{ccccc} E & \xrightarrow{\pi} & E^{\sigma_\mathfrak{p}} & \xrightarrow{\epsilon_0} & E^{\sigma_\mathfrak{p}} \\ \downarrow & & \downarrow & & \downarrow \\ \tilde{E} & \xrightarrow{\phi} & \tilde{E}^{(p)} & \xrightarrow{\epsilon} & \widetilde{E^{\sigma_\mathfrak{p}}} \end{array},$$

so that we may replace π by $\epsilon_0^{-1} \circ \pi$, which is of degree p. Let $\sigma_\mathfrak{p} = \Theta_{H/K}(\mathfrak{p}) = 1$. Then we obtain the desired square (2.11). The uniqueness of π follows from the fact that the reduction $\mathrm{Hom}(E_1, E_2) \to \mathrm{Hom}(\tilde{E}_1, \tilde{E}_2)$ is injective.

To show that ϵ comes from some $\epsilon_0 \in \mathrm{Aut}(E^{\sigma_\mathfrak{p}})$, it is equivalent to showing that ϵ commutes with the image of $\mathrm{End}(E^{\sigma_\mathfrak{p}})$ in the reduction (see Silverman [12] Lemma II.5.2). With this in mind, for any $\alpha \in \mathrm{End}(E)$, we compute

$$\tilde{\alpha} \circ \epsilon \circ \phi = \tilde{\alpha} \circ \tilde{\pi} = \tilde{\pi} \circ \tilde{\alpha} = \epsilon \circ \phi \circ \tilde{\alpha} = \epsilon \circ \tilde{\alpha} \circ \phi.$$

Therefore $\tilde{\alpha} \circ \epsilon = \epsilon \circ \tilde{\alpha}$, and we are done. □

Now we proceed with the proof of Theorem 2.9.

Proof of Theorem 2.9. Let $L = H(h(E[\mathfrak{m}]))$. In order to show that L is the ray class field of modulus $\mathfrak{m}$, by class field theory it suffices to show that $\Theta_{L/K}(\mathfrak{p}) = 1$ if and only if $\mathfrak{p} \in P(\mathfrak{m})$. Excluding finitely many primes as before, we may assume that $\mathfrak{p}$ has residue field degree one in K and satisfies Lemma 2.10.

Suppose $\mathfrak{p} \in P(\mathfrak{m})$, so that $\mathfrak{p} = \mu R$ for some $\mu \in R$ with $\mu \equiv 1 \pmod{\mathfrak{m}}$. Since $\mathfrak{p}$ is principal, $\Theta_{H/K}(\mathfrak{p}) = 1$. Applying Lemma 2.10 we get (2.11) where $\mathfrak{p} = \pi R$. Hence there exists a unit $\xi \in R^\times$ with $\pi = \xi\mu$. Let $P \in E[\mathfrak{m}]$ be an $\mathfrak{m}$-torsion point. Then by commutativity of the square (2.11) we have

$$\widetilde{P^{\Theta_{L/K}(\mathfrak{p})}} = \phi(\widetilde{P}) = \widetilde{\pi(P)}.$$

A nontrivial fact says that the reduction $E \to \widetilde{E}$ modulo $\mathfrak{p}$ is injective on torsion points of order prime to $\mathfrak{p}$. Excluding finitely many primes we may assume the injectivity and therefore conclude that $P^{\Theta_{L/K}(\mathfrak{p})} = \pi(P)$. Since the map induced by a unit ξ is an automorphism of E, by the $\mathrm{Aut}(E)$-invariance of h,

$$h(P)^{\Theta_{L/K}(\mathfrak{p})} = h(P^{\Theta_{L/K}(\mathfrak{p})}) = h(\pi(P)) = h(\mu(P)) = h(P),$$

as $P \in E[\mathfrak{m}]$ and $\mu \equiv 1 \pmod{\mathfrak{m}}$. Therefore, $\Theta_{L/K}(\mathfrak{p}) = 1$ as desired.

Conversely, suppose that $\Theta_{L/K}(\mathfrak{p}) = 1$. Choosing $P \in E[\mathfrak{m}]$ and $\sigma \in \mathrm{Gal}(\overline{K}/K)$ with $\sigma|_{K^{\mathrm{ab}}} = \Theta_{K^{\mathrm{ab}}/K}(\mathfrak{p})$, we may again apply (2.11) and compute

$$\tilde{h}(\tilde{\pi}(\tilde{P})) = \tilde{h}(\widetilde{\pi(P)}) = \tilde{h}(\phi(\tilde{P})).$$

But as in the proof of Lemma 2.10, the p-th power Frobenius ϕ lifts to σ, so that

$$\tilde{h}(\phi(\tilde{P})) = \tilde{h}(\widetilde{P^\sigma}) = \widetilde{h(P)^\sigma} = \widetilde{h(P)} = \tilde{h}(\tilde{P}),$$

as $\sigma|_L = \Theta_{L/K}(\mathfrak{p}) = 1 = \Theta_{H/K}(\mathfrak{p}) = \sigma|_H$. Hence $\tilde{h}(\tilde{\pi}(P)) = \tilde{h}(\tilde{P})$, which implies that there exists some $\xi \in \mathrm{Aut}(E)$ such that $\tilde{\pi}(\tilde{P}) = \tilde{\xi}(\tilde{P})$. Injectivity of reduction

on torsion points allows us to conclude that $(\pi - \xi)P = O$. Since $E[\mathfrak{m}]$ is a free $R/\mathfrak{m}$-module of rank one, there exists a single $\xi \in R^\times$ such that $\pi - \xi$ annihilates all of $E[\mathfrak{m}]$. Therefore $\xi^{-1}\pi \equiv 1 \pmod{\mathfrak{m}}$, which implies that $\mathfrak{p} \in P(\mathfrak{m})$. □

Example (A numerical illustration)**.** The following computation is taken from Silverman [12]. Consider an elliptic curve given by

$$E : y^2 = x^3 + x.$$

Then $j(E) = 1728$, so E possesses nontrivial automorphisms. The endomorphism

$$\alpha : (x, y) \mapsto \left(\alpha^{-2}\left(x + \frac{1}{x}\right), \alpha^{-3} y \left(1 - \frac{1}{x^2}\right)\right), \qquad \alpha = 1 + \sqrt{-1}$$

is of degree two, but is different from the multiplication-by-two map $[2] \in \mathrm{End}(E)$. Hence E has CM. In fact, it has CM by the Gaussian integers $\mathbf{Z}[i]$. Since

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

one sees that the ray class field of $\mathbf{Q}(i)$ of modulus (2) is just $\mathbf{Q}(i)$. Finding the x-coordinates of 3-torsion points amounts to solving the equation

$$3x^4 + 6x^2 - 1 = 0 \quad \Longrightarrow \quad x = \alpha, -\alpha, \frac{1}{\sqrt{3}\alpha}, -\frac{1}{\sqrt{3}\alpha}, \qquad \alpha = \sqrt{\frac{2\sqrt{3} - 3}{3}}.$$

Since the Weber function for E is $h(x, y) = x^2$, we obtain the ray class field of $\mathbf{Q}(i)$ of modulus (3) is $\mathbf{Q}(i, \sqrt{3})$. The x-coordinates of 4-torsion points satisfy

$$x^6 + 5x^4 - 5x^2 - 1 = 0 \quad \Longrightarrow \quad x = \pm 1, \pm\gamma, \pm\gamma^{-1}, \qquad \gamma = \sqrt{-1}\left(\sqrt{2} - 1\right).$$

Hence the ray class field of $\mathbf{Q}(i)$ of modulus (4) is $\mathbf{Q}(i, \sqrt{2})$.

We end the section by stating the so-called Main Theorem of Complex Multiplication. The reason that we state this result is because it can be generalized rather directly to the case of abelian varieties (see Theorem 3.10). Note that we have essentially developed all the tools necessary to prove the theorem, but we choose to omit the proof as it is lengthy and does not directly concern the construction of class fields, which was our main goal.

We again recollect some notions from algebraic number theory. For details see Sutherland [14]. The *idèle group* of K is the topological group

$$\mathbb{A}_K^\times := \left\{(a_v) \in \prod_v K_v^\times : a_v \in \mathcal{O}_v^\times \text{ for all bu t finitely many } v\right\},$$

where v ranges through all places of K. Similar to the role that modulus play in the classical global class field theory, the idèle group packs together information of all places of K. The global Artin map defined by

$$\begin{aligned} \mathbb{A}_K^\times / K^\times &\to \mathrm{Gal}(K^{\mathrm{ab}}/K) \\ s &\mapsto [s, K] \end{aligned}$$

will be denoted by $s \mapsto [s, K]$. If L/K is finite abelian and (s) is not divisible by any primes that ramify in L, then $[s, K]|_L = \Theta_{L/K}(s)$ is the local Artin map.

Note that multiplication by an idèle s amounts to multiplying the $\mathfrak{p}$-primary of s locally as ideals, and then patching together places $\mathfrak{p}$ to get the global result.

Theorem 2.12 (The main theorem of CM of elliptic curves)**.** *For $E/\mathbf{C} \in \mathrm{Ell}(R)$ fix a uniformization $\xi : \mathbf{C}/\mathfrak{a} \xrightarrow{\sim} E$ for some fractional ideal $\mathfrak{a}$ of K. Fix $\sigma \in \mathrm{Aut}(\mathbf{C})$ and choose $s \in \mathbf{A}_K^\times$ with $[s, K] = \sigma|_{K^{\mathrm{ab}}}$. There exists a unique uniformization*

$$\xi' : \mathbf{C}/s^{-1}\mathfrak{a} \xrightarrow{\sim} E^\sigma(\mathbf{C})$$

such that the following diagram commutes:

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

Proof. See Silverman [12]. □

3. CM of Abelian Varieties

The corresponding theory of CM for abelian varieties is much more profound, initially established by Shimura, Taniyama, and Weil in the 1950s. We won't be able to develop all the proofs rigorously and leave that task to a serious textbook such as Milne [5]. We are content with understanding some important statements.

3.1. **A primer on abelian varieties.**

The canonical reference for abelian varieties is Mumford's text[6]. We shall assume that the reader has some exposure to scheme theory as introduced in, for instance, Hartshorne [2]. We shall frequently point out whether or not the construction parallels that of elliptic curves.

Definition. Let S be a scheme. A *group scheme* G over S is a scheme such that for any S-scheme T, the hom-set $\mathrm{Hom}(T, G)$ is endowed with a group structure that is functorial in T[1]. Let K be a field. An *abelian variety* A/K is a reduced, connected, and projective group scheme over $\mathrm{Spec}(K)$.

Remark 3.1. By a result known as the rigidity lemma, the group law on abelian varieties is commutative, making $A(\overline{K})$ into an abelian group.

To see how abelian varieties generalize elliptic curves, note that the set $A(\overline{K})$ of $\overline{K}$-rational points forms a group. Also note that reduced groups schemes over a field are smooth. Hence elliptic curves are by definition abelian varieties. In fact, they are abelian varieties of dimension one.

A morphism of abelian varieties is a morphism of varieties compatible with the group structure, that is, it commutes with multiplication, identity, and inverse.

Definition. Let $f : A \to B$ be a morphism of abelian varieties. Then f is an *isogeny* if it is surjective and $\dim A = \dim B$. The *degree* of f is the degree of the field extension $K(X)/f^*K(Y)$. We set $\deg f = 0$ if f is not an isogeny.

An abelian variety is *simple* if there is no nontrivial abelian subvariety. Now we show that the category of abelian varieties up to isogeny is a *semisimple category*, that is, every abelian variety is isogenous to a direct sum of simple ones. We need the following lemma, known as the Poincaré's complete reducibility theorem:

[1]By the Yoneda lemma, it is equivalent to say that G is a group object in the category of S-schemes.

Lemma 3.2. *If A' is an abelian subvariety of A, then there exists an abelian subvariety A'' of A such that $A' \times A'' \to A$ is an isogeny.*

Let $\mathrm{End}(A)$ be the endomorphism ring of a simple abelian variety A. It can be shown that the *endomorphism algebra* $\mathrm{End}^0(A) := \mathrm{End}(A) \otimes_{\mathbf{Z}} \mathbf{Q}$ is a $\mathbf{Q}$-division algebra. Now suppose that A is isogenous to $A_1^{n_1} \times \cdots \times A_r^{n_r}$ with each A_i simple and A_i non-isogenous to A_j for $i \neq j$. Then from the fact that

$$\mathrm{End}(X \times Y) \cong \mathrm{End}(X) \oplus \mathrm{Hom}(X, Y) \oplus \mathrm{Hom}(Y, X) \oplus \mathrm{End}(Y)$$

we are able to conclude that

$$\mathrm{End}^0(A) \cong \prod_{i=1}^{r} \mathcal{M}_{n_i}(D_i),$$

where $\mathcal{M}_{n_i}(D_i)$ is the ring of $n_i \times n_i$ matrices with coefficients in $D_i = \mathrm{End}^0(A_i)$.

Proposition 3.3. *For an abelian variety A, $\mathrm{End}^0(A)$ is a semisimple $\mathbf{Q}$-algebra.*

Proof sketch. A semisimple $\mathbf{Q}$-algebra is a finite-dimensional $\mathbf{Q}$-algebra that can be written as a product of simple subalgebras (i.e., an algebra that has no nontrivial proper two-sided ideal). Since $\mathrm{End}^0(A)$ is already a product of simple subalgebras, it remains to prove the $\mathbf{Q}$-finiteness. Let $\dim A = g$. The ℓ^n-torsion subgroup is given by

$$A[\ell^n] \cong \begin{cases} (\mathbf{Z}/\ell^n\mathbf{Z})^{2g}, & \mathrm{char}(K) \nmid \ell \\ (\mathbf{Z}/\ell^n\mathbf{Z})^i \text{ for some } i \leq g, & \mathrm{char}(K) = \ell \end{cases}.$$

Intuitively, view A as a complex torus, which is topologically a product of $2g$ copies of S^1. On each copy of S^1, points of order ℓ^n forms a copy of $\mathbf{Z}/\ell^n\mathbf{Z}$. Hence the ℓ-adic Tate module of A, defined by the inverse limit

$$T_\ell(A) = \varprojlim_n A[\ell^n],$$

has finite $\mathbf{Z}_\ell$-rank. Now it suffices to show that the map

$$\mathrm{End}(A) \otimes \mathbf{Z}_\ell \to \mathrm{End}_{\mathbf{Z}_\ell}(T_\ell(A))$$

is injective, since tensoring with $\mathbf{Q}_\ell$ we get

$$\mathbf{Q}_\ell \otimes_{\mathbf{Q}} \mathrm{End}^0(A) \hookrightarrow \mathrm{End}_{\mathbf{Q}_\ell}\left(\mathbf{Q}_\ell \otimes_{\mathbf{Z}_\ell} T_\ell(A)\right),$$

which shows that $\mathrm{End}^0(A)$ is finite over $\mathbf{Q}$ since the target is finite over $\mathbf{Q}_\ell$. The proof of injectivity is analogous to the ingenious proof in the elliptic curve case (see Silverman [13] Theorem III.7.4). □

Recall that for an elliptic curve $E/\mathbf{C}$, there is a uniformization $E(\mathbf{C}) \cong \mathbf{C}/\Lambda$ for some lattice $\Lambda \subset \mathbf{C}$. Abelian varieties $A/\mathbf{C}$ of dimension g is isomorphic to $\mathbf{C}^g/\Lambda$ for some lattice $\Lambda \subset \mathbf{C}^g$. But the converse, that any complex torus $\mathbf{C}^g/\Lambda$ can be realized as an abelian variety, is only true in general for $g = 1$, that is, for elliptic curves. That is because that a nice embedding of $\mathbf{C}^g/\lambda$ into the projective space might not exist.

In algebraic geometry, this undesirable situation is remedied by fixing the data of an ample line bundle on the abelian variety. Recall that a line bundle (i.e., free $\mathcal{O}_A$-module of rank one) is ample if taking large enough tensor power of itself induces an embedding into projective spaces. This is the concept of *polarization*. Here we shall define polarization complex-analytically:

Definition. A complex torus $\mathbf{C}^g/\Lambda$ is *polarized* if on it there exists an alternating $\mathbf{R}$-bilinear form $E : \mathbf{C}^g \times \mathbf{C}^g \to \mathbf{R}$, called the *Riemann form*, that satisfies:

(i) $E(\Lambda \times \Lambda) \subset \mathbf{Z}$;
(ii) the bilinear form $(z, w) \mapsto E(z, \sqrt{-1}w)$ is symmetric and positive-definite.

We explain three reasons why fixing a polarization is nice:

(i) A complex torus $\mathbf{C}^g/\Lambda$ admitting a polarization is an abelian variety. Hence we have an equivalence of categories from the category of abelian varieties over $\mathbf{C}$ to the category of polarizable complex tori.
(ii) The automorphism group of a polarized abelian variety is finite. (For elliptic curves this is always true. In fact, the order of the automorphism groups can only be 2, 4, 6, 12, or 24. See Chapter III §10 of Silverman [13].)
(iii) As we shall see in Section 3.3, fixing a polarization gives a more precise CM-type information. It is an indispensable piece of information in the field of moduli that allows us to construct class fields.

3.2. **Abelian varieties with CM.** Recall that an elliptic curve E has complex multiplication if the endormorphism algebra $\mathrm{End}(E) \otimes \mathbf{Q}$ is an *imaginary quadratic field*. This is now generalized to so-called *CM-algebras*, which are totally imaginary quadratic extensions of a totally real field.

We start with some results from algebra.

Fix a field K of characteristic zero. Let B be a semisimple algebra over K. The Wedderburn–Artin theorem says that B decomposes into a finite product of matrix algebras $B_i = \mathcal{M}_{n_i}(D_i)$ over K-division algebras D_i. Let K_i be the center of each D_i. Then $[B_i : k_i]$ is a square. We define the *reduced degree* of B over K to be

$$[B : k]_{\mathrm{red}} := \sqrt{[B_i : k_i]}[k_i : k].$$

Equivalently, it is the degree of the maximal étale k-subalgebra (finite product of finite separable extensions of k).

Lemma 3.4. *Notation as above, if M is a faithful B-module, then*

$$\dim_k M \geq [B, k]_{red},$$

where equality holds if and only if B_i are matrix algebras over k_i.

Now we come back to abelian varieties. Recall from the proof of Theorem 1.1 that for an elliptic curve E isomorphic to $\mathbf{C}/\Lambda$, it is useful to interpret its endomorphism ring complex-analytically as

$$\mathrm{End}(E) \cong \{\alpha \in \mathbf{C} : \alpha\Lambda = \Lambda\}.$$

Let $A/\mathbf{C}$ be an abelian variety isomorphic to a complex torus $\mathbf{C}^g/\Lambda$. The following analogous interpretation is referred to as an *analytic representation*:

$$\mathrm{End}^0(A) \cong \{M \in \mathcal{M}_g(\mathbf{C}) : M\mathbf{Q}\Lambda \subset \mathbf{Q}\Lambda\}, \tag{3.5}$$

as it is a g-dimensional complex representation of $\mathrm{End}^0(A)$. Since $\mathbf{R}\Lambda = \mathbf{C}^n$, any $\mathbf{C}$-linear endomorphism that is identity on $\mathbf{Q}\Lambda$ is identity on the whole of $\mathbf{C}^n$. Hence $\mathbf{Q}\Lambda$ is a faithful $\mathrm{End}^0(A)$-module. Applying Lemma 3.4,

$$[\mathrm{End}^0(A) : \mathbf{Q}]_{\mathrm{red}} \leq \dim_{\mathbf{Q}} \mathbf{Q}\Lambda = 2 \dim A.$$

Definition. An abelian variety $A/\mathbf{C}$ has *complex multiplication* (or CM) if

$$[\mathrm{End}^0(A) : \mathbf{Q}]_{\mathrm{red}} = 2 \dim A.$$

Therefore, if A has CM, then $\mathrm{End}^0(A)$, which is a product of matrix algebras $\mathcal{M}_{n_i}(D_i)$, contains an étale $\mathbf{Q}$-subalgebra of dimension $2\dim A$. It follows that each algebra $D_i = \mathrm{End}^0(A_i)$ has degree $2\dim A_i$ over $\mathbf{Q}$. That is to say, A has CM if and only if each of its simple factors has CM.

Definition. A *CM-field* K is a totally imaginary quadratic extension of a totally real field. A *CM-algebra* is a finite product of CM-fields.

Obviously imaginary quadratic fields $\mathbf{Q}(\sqrt{-D})$ are examples of CM-fields. For other examples, $\mathbf{Q}(\zeta_N)/\mathbf{Q}(\zeta_N + \overline{\zeta_N})$ is a CM-field for $N > 2$.

The following classification result that we won't prove relates the definition of CM of abelian varieties to CM-fields.

Theorem 3.6. *An abelian variety $A/\mathbf{C}$ has complex multiplication if and only if one of the following cases holds*

(i) A is simple and $\mathrm{End}^0(A)$ is a CM-field of degree $2\dim A$ over $\mathbf{Q}$;
(ii) A is isotypic, that is, A is isogenous to A_0^n for some simple A_0, and $\mathrm{End}^0(A)$ contains a number field of degree $2\dim A$ over $\mathbf{Q}$;
(iii) $\mathrm{End}^0(A)$ contains an étale $\mathbf{Q}$-subalgebra of dimension $2\dim A$.

In cases (ii) and (iii), the number field (resp. étale $\mathbf{Q}$-subalgebra) can be chosen to be a CM-field (resp. CM-algebra) invariant under some involution induced by a polarization of A. The involution is called Rosati involution.

Recall that for elliptic curves E, there are only two embeddings $\mathrm{End}(E) \hookrightarrow \mathbf{C}$. We tacitly choose the canonical one that preserves the invariant differential (see Silverman [12] Proposition II.1.1). But for a CM-field K, since every complex embedding $\phi : K \hookrightarrow \mathbf{C}$ commutes with complex conjugation ι, it is important to choose one from each duple $\{\phi, \iota \circ \phi\}$. This motivates the following definition.

Definition. A *CM-type* on a CM-field K is a set Φ of complex embeddings $K \hookrightarrow \mathbf{C}$ such that $\Phi \cap \iota\Phi = \emptyset$ and $\Phi \cup \iota\Phi$ is the set of all complex embeddings of K. For CM-algebras, a CM-type amounts to choosing a CM-type for each of its factors.

A technicality in the case of abelian varieties is that automorphisms $\sigma \in \mathrm{Aut}(\mathbf{C})$ permutes Φ. But as we shall see, for abelian varieties A and A^σ to be isogenous, σ has to preserve the CM-type of $K = \mathrm{End}^0(A)$. Hence we need some field K^* over which automorphisms $\sigma \in \mathrm{Aut}(\mathbf{C}/K^*)$ preserve (K, Φ).

Definition. The *reflex field* K^* of CM-type (K, Φ) is the CM-field

$$K^* := \mathbf{Q}\left(\left\{\sum_{\phi\in\Phi} \phi(x)\right\}_{x\in K}\right).$$

Equivalently, by identifying $\Phi \sqcup \iota\Phi$ with $\mathrm{Gal}(K/\mathbf{Q})$, K^* is the fixed field of set of $\sigma \in \mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ such that $\sigma\Phi = \Phi$. Inverses of elements in Φ, viewed as elements of $\mathrm{Gal}(\overline{K}/K)$, restricted to K^* give a CM-type Φ^* on K^* called the *reflex type*.

If K is an imaginary quadratic field as in the elliptic curve case, then $K = K^*$. Hence in the Theorem 2.12 it suffices to take $\sigma \in \mathrm{Aut}(\mathbf{C}/K)$.

Definition. Let (K, Φ) be a CM-type. The *reflex norm* is the map $N_\Phi : K^* \to \mathbf{C}$ defined by $N_\Phi(x) = \prod_{\psi\in\Phi^*} \psi(x)$.

The reflex norm can be extended to a map on the idèle $\mathbb{A}_{K^*}^\times$ of K^*. It will give crucial information about the abelian variety A^σ under action $\sigma \in \mathrm{Aut}(\mathbf{C}/K^*)$.

3.3. **Classification of abelian varieties with CM.** Let $\xi : \mathbf{C}^g/\Lambda \xrightarrow{\sim} A$ be an abelian variety with CM by a CM-field K and fix an embedding $\iota : K \hookrightarrow \mathrm{End}^0(A)$, through which the analytic representation (3.5) induces a faithful action

$$S : K \hookrightarrow \mathcal{M}_g(\mathbf{C}).$$

For $a \in K$, we may assume that $S(a) = \mathrm{diag}(\phi_1(a), \cdots, \phi_g(a))$ up to a change of basis. Since the action is faithful and $\mathbf{C}$-linear, and $\dim_{\mathbf{Q}} K = 2g$, we see that Φ defines a CM-type. We call (K, Φ) the *CM-type associated to the pair* (A, ι).

Let $\omega \in \mathbf{Q}\Lambda$ be nonzero. Since $S(K)(\omega) \subset \mathbf{Q}\Lambda$ and they both have dimension $2g$, $S(K)(\omega) \cong \mathbf{Q}\Lambda$. Scaling the basis by ω^{-1} we obtain a $\mathbf{Q}$-linear isomorphism $u_\Phi : K \to \mathbf{Q}\Lambda$ where $u_\Phi(a)$ is $S(a)$ acting on the vector $(1, \cdots, 1) \in \mathbf{C}^g$. Extending R-linearly to a map $u : K_{\mathbf{R}} = K \otimes \mathbf{R} \to \mathbf{R}\Lambda = \mathbf{C}^g$ and putting $\mathfrak{a} = u^{-1}(\Lambda)$, we obtain a commutative diagram with exact rows:

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \mathfrak{a} & \longrightarrow & K_{\mathbf{R}} & \longrightarrow & K_{\mathbf{R}}/\mathfrak{a} & \longrightarrow & 0 \\ & & \downarrow & & \downarrow{\scriptstyle u} & & \downarrow & & \\ 0 & \longrightarrow & \Lambda & \longrightarrow & \mathbf{C}^n & \xrightarrow{\xi} & A & \longrightarrow & 0 \end{array}.$$

We will also say that (A, ι) is of CM-type $(K, \Phi, \mathfrak{a})$, where $\mathfrak{a}$ depends on ξ. The construction is easily generalized to the case of CM-algebras W by taking products. We call (A, ι) *principal* if $\iota^{-1}(\mathrm{End}^0(A)) = \mathcal{O}_W$ is the maximal order of W.

An isogeny $\mu : (A_1, \iota_1) \to (A_2, \iota_2)$ of abelian varieties with CM by a CM-algebra W is an isogeny $\mu : A_1 \to A_2$ such that the diagram below commutes:

$$\begin{array}{ccc} A_1 & \xrightarrow{\mu} & A_2 \\ {\scriptstyle \iota_1(f)}\downarrow & & \downarrow{\scriptstyle \iota_2(f)} \\ A_1 & \xrightarrow{\mu} & A_2 \end{array}, \quad \text{for any } f \in W.$$

We now show that the associated CM-type (W, Φ) classifies (A, ι) up to isogeny.

Theorem 3.7. *Two abelian varieties (A_1, ι_1) and (A_2, ι_2) with CM by a CM-algebra W are isogenous if and only if they have the same associated CM-type.*

Proof. If (A_1, ι_1) and (A_2, ι_2) are isogenous, then there is a linear isomorphism $\mu^* : \mathrm{End}^0(A_1) \to \mathrm{End}^0(A_2)$ given by $\alpha \mapsto \mu \circ \alpha \circ \mu^{-1}$. Hence $\iota_2 = \mu^* \circ \iota_1$, which means that ι_1 and ι_2 induces the same diagonalization, and thus the same CM-type.

Conversely, suppose that (A_1, ι_1) and (A_2, ι_2) are of CM-types $(W, \Phi, \mathfrak{a}_1)$ and $(W, \Phi, \mathfrak{a}_2)$ respectively. Since $\mathfrak{a}_1, \mathfrak{a}_2 \in W$ are lattices, there exists some $c \in \mathbf{Z}$ such that $c\mathfrak{a}_1 \subset \mathfrak{a}_2$. Thus we have the following commutative diagram:

$$\begin{array}{ccccc} W/\mathfrak{a}_1 & \xrightarrow{u} & \mathbf{C}^n/u(\mathfrak{a}_1) & \xrightarrow{\xi_1} & A_1 \\ \downarrow{\scriptstyle c} & & \downarrow{\scriptstyle c} & & \downarrow{\scriptstyle \mu} \\ W/\mathfrak{a}_2 & \xrightarrow{u} & \mathbf{C}^n/u(\mathfrak{a}_2) & \xrightarrow{\xi_2} & A_2 \end{array}.$$

Let $f \in W$ and $x = \xi_1(y) \in A_1$. Since embedding f into $\mathrm{End}^0(A_1)$ and then acting on x is equivalent to acting on y through the analytic representation S and then embedding into A_1 via ξ_1, we have

$$\mu \circ \iota_1(f)(x) = \mu \circ \xi_1(S(f)(y)), \quad \text{and similarly} \quad \xi_2(S(f)(cy)) = \iota_2(f) \circ \xi_2(cy).$$

Now by the commutativity of the square on the right we get $\mu\circ\iota_1(f) = \iota_2(f)\circ\mu$. $\square$

Next up, we show that fixing a polarization $\mathcal{C}$ on (A,ι) yields a more precise CM-type information $(K,\Phi,\mathfrak{a},\tau)$ that classifies $(A,\iota,\mathcal{C})$ up to *isomorphism* instead.

Let (A,ι) be of CM-type (K,Φ) for a CM-field K. Let E be the Riemann form associated to a polarization $\mathcal{C}$ on A that satisfies

$$E(S(a)x,y) = E(x,S(\overline{a})y), \quad \text{for } x,y\in\mathbf{C}^g \text{ and } a\in K. \tag{3.8}$$

Note that the $f : K\to\mathbf{Q}$ given by $f(a) = E(u(a),u(1))$ is $\mathbf{Q}$-linear, and is determined by its value on a $\mathbf{Q}$-basis of K. Linearity forces the map to be a sum of basis elements, and since the map is $\mathrm{Gal}(K/\mathbf{Q})$-invariant, the coefficients of basis elements in the sum has to be the same. Hence there exists some $\tau\in K$ such that

$$f(a) = \mathrm{Tr}_{K/\mathbf{Q}}(\tau a) \quad \text{for all } a\in K.$$

But by (3.8), for any $a,b\in K$ we have

$$E(u(a),u(b)) = E(u(a),S(b)u(1)) = E(S(\bar{b})u(a),u(1)) = E(u(a\bar{b}),u(1)),$$

so that $E(u(a),u(b)) = \mathrm{Tr}_{K/\mathbf{Q}}(\tau a\bar{b})$. Since E is alternating,

$$\mathrm{Tr}_{K/\mathbf{Q}}(\tau a\bar{b}) = -\mathrm{Tr}_{K/\mathbf{Q}}(\tau\bar{a}b) = -\mathrm{Tr}_{K/\mathbf{Q}}(\overline{\tau}a\bar{b}),$$

so that $\overline{\tau} = -\tau$ is imaginary. Hence $\overline{\phi(\tau)} = \phi(\overline{\tau})$ for any $\phi\in\Phi$. Moreover, since $u(K)\cong\mathbf{Q}\Lambda$ is dense in $\mathbf{C}^g$, identifying $\Phi\sqcup\overline{\Phi}$ with $\mathrm{Gal}(K/\mathbf{Q})$ we obtain

$$E(z,w) = \sum_{j=1}^{g}\phi_j(\tau)(z_j\overline{w_j} - \overline{z_j}w_j) \quad \text{for any } z,w\in\mathbf{C}^g. \tag{3.9}$$

By the positive-definite property of E and the the fact that

$$E(z,\sqrt{-1}z) = -2\sqrt{-1}\sum_{j=1}^{g}\phi_j(\tau)|z_j|^2,$$

it follows that $\Im\phi(\tau) > 0$ for any $\phi\in\Phi$. Conversely, given $\tau\in K$ that satisfies $\overline{\tau} = -\tau$ and $\Im\phi(\tau) > 0$ for any $\phi\in\Phi$, there exists an integer $q > 0$ such that qE is a Riemann form that satisfies (3.8), where E is defined as in (3.9).

We say that $(A,\iota,\mathcal{C})$ is of CM-type $(K,\Phi,\mathfrak{a},\tau)$, where both the lattice $\mathfrak{a}\subset K$ and τ depends on a uniformization $\xi : \mathbf{C}^g/\Lambda\xrightarrow{\sim}A$. Conversely, a triple $(A',\iota',\mathcal{C}')$ can be constructed from a CM-type $(K,\Phi,\mathfrak{a},\tau)$ as follows. Using Φ, we define $S : K\to\mathcal{M}_g(\mathbf{C})$ by $S(a) = \mathrm{diag}(\phi_1(a),\cdots,\phi_g(a))$. Let $u : K\to\mathbf{C}^n$ be such that $u(a)$ is $S(a)$ acting on the vector $(1,\cdots,1)\in\mathbf{C}^g$. Then $A' = \mathbf{C}^g/\Lambda$ with $\Lambda = u(\mathfrak{a})$. The embedding $\iota' : K\hookrightarrow\mathrm{End}^0(A)$ is recovered from

$$\iota'(a)\circ\xi = \xi\circ S(a).$$

Finally E defined by (3.9) is a Riemann form that determines a polarization $\mathcal{C}'$ of A' up to some integer $q > 0$. It can be checked that $(A',\iota',\mathcal{C}')$ is isomorphic to $(A,\iota,\mathcal{C})$. In fact, there is a one-to-one correspondence between isomorphism classes of $(A,\iota,\mathcal{C})$ and equivalence classes of CM-types $(K,\Phi,\mathfrak{a},\tau)$.

Note that the construction above is easily generalized to CM-algebras: instead of a single τ, we have a collection $\{\tau_i\}_i$, one τ_i for each CM-field factor K_i.

3.4. **The main theorem and the construction of class fields.** We state the main theorem of CM of abelian varieties, but we refrain from giving a proof.

Theorem 3.10 (The main theorem of CM of abelian varieties over the reflex field)**.** *Let $(A, \iota, \mathcal{C})$ be a polarized abelian variety of CM-type $(W, \Phi, \mathfrak{a}, \tau)$ with respect to a uniformization $\xi : \mathbb{C}^g/u(\mathfrak{a}) \xrightarrow{\sim} A$. Let W^* be the reflex field. Fix $\sigma \in \mathrm{Aut}(\mathbb{C}/W^*)$ and choose $s \in \mathbb{A}_W^\times$ with $[s, W] = \sigma|_{(W^*)^{ab}}$. There exists a unique uniformization*

$$\xi' : \mathbb{C}^g/u(\mathrm{Nm}_\Phi(s)^{-1}\mathfrak{a}) \xrightarrow{\sim} A^\sigma$$

such that A^σ is of CM-type $(W, \Phi, \mathrm{Nm}_\Phi(s)^{-1}\mathfrak{a}, \mathrm{Nm}_{K/\mathbb{Q}}((s))\tau)$ with respect to ξ', and we have the following diagram that commutes

$$\begin{array}{ccc} W/\mathfrak{a} & \xrightarrow{\mathrm{Nm}_\Phi(s)^{-1}} & W/\mathrm{Nm}_\Phi(s)^{-1}\mathfrak{a} \\ \downarrow{\scriptstyle \xi\circ u} & & \downarrow{\scriptstyle \xi'\circ u} \\ A & \xrightarrow{\sigma} & A^\sigma \end{array} .$$

Proof. See Shimura [11]. □

N.B. The reader is advised to compare this with the main theorem of CM of elliptic curve Theorem 2.12. In both case, an algebraic action σ is translated, via vertical analytic maps, to an arithmetic action of multiplication by an idèle.

Remark 3.11. In the main theorem above we restrict $\sigma \in \mathrm{Aut}(\mathbb{C}/W^*)$ over the reflex field W^* instead of over $\mathbf{Q}$. This is because for A and A^σ to be isogenous, σ has to preserve CM-type (W, Φ), and W^* is defined precisely to make this happen. The subsequent works of Langlands, Deligne, and Tate in the 1980s relaxed this restriction and proved the main theorem over $\mathbb{Q}$. For an account see Milne [5].

In any case, Theorem 3.10 is sufficient for constructing class fields. Consider a system $\mathcal{P} = (A, \iota, \mathcal{C}, T)$ of CM-type (W, Φ), where T is a set of torsion points of A.

Definition. A *field of moduli* $k_\mathcal{P} \subset \mathbf{C}$ of $\mathcal{P}$ is a field that satisfies the following:

(i) every field of definition k for $\mathcal{P}$, that is, a field k over which A, $\mathcal{C}$, $\iota(W)$, and T are rational, contains $k_\mathcal{P}$;
(ii) for every complex embedding $\sigma : k \hookrightarrow \mathbf{C}$ of a field of definition, $\sigma|_{k_\mathcal{P}}$ is the identity if and only if $\mathcal{P}$ is isomorphic to $\mathcal{P}^\sigma$, that is, there is an isomorphism $f : A \to A^\sigma$ of polarized abelian variety with $f(T) = T^\sigma$.

It turns out that $k_\mathcal{P}$ is uniquely characterized by (i) and (ii).

If $\mathcal{P}$ is defined over a number field K, then by Galois theory $k_\mathcal{P}$ is the field corresponding to the subgroup of $\mathrm{Gal}(K/\mathbf{Q})$ consisting of those $\sigma \in \mathrm{Gal}(K/\mathbf{Q})$ such that $\mathcal{P}$ is isomorphic to $\mathcal{P}^\sigma$.

Theorem 3.12. *Let $\mathcal{P} = (A, \iota, \mathcal{C})$ be of CM-type (W, Φ) with (A, ι) principal. Then the field of moduli $k_\mathcal{P}$ is an unramified extension of the reflex field W^*.*

To formulate the theorem for abelian extensions, we need an analogue of Weber function, that is, some model of A that is invariant under automorphisms. Recall that the automorphism group $\mathrm{Aut}(A, \mathcal{C})$ is finite once a polarization $\mathcal{C}$ is fixed. We call $A/\mathrm{Aut}(A, \mathcal{C})$ a *Kummer variety* with quotient $h : A \to A/\mathrm{Aut}(A, \mathcal{C})$.

Theorem 3.13. *Let $\mathcal{P} = (A, \iota, \mathcal{C})$ be of CM-type (W, Φ). Let $\mathfrak{m} = \mathfrak{m}_1 \times \cdots \times \mathfrak{m}_r$ be a modulus of W and m the least common multiple of $\mathfrak{m}_1, \cdots, \mathfrak{m}_r$. Then $k_{\mathcal{P}}(h(A[\mathfrak{m}]))$ is an abelian extension of W^* of conductor dividing m, where*

$$A[\mathfrak{m}] = \{P \in A : \alpha P = 0 \text{ for all } \alpha \in \mathfrak{m}\}$$

is the group of $\mathfrak{m}$-torsion points.

Remark 3.14. Comparing Theorem 3.12 and Theorem 3.13 to the corresponding statements for elliptic curves, Theorem 2.7 and Theorem 2.9, we notice that we only get *some* class fields, but not all of them. Hence we cannot talk about *maximal* (unramified) abelian extensions as we did for elliptic curves.

4. Where to go from here

There is an abundance of related aspects of complex multiplication that are not included here. We mention a few and give reference.

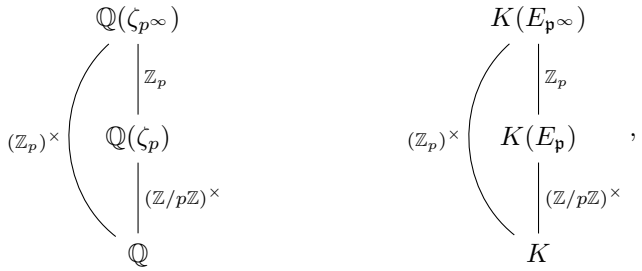
Integrality of the j-invariant. In Lemma 2.2 we proved that $j(E)$ is algebraic for E with CM. It turns out that $j(E)$ is an algebraic integer. Three different proofs of this fact of different flavors are given in Chapter II §6 of Silverman [12].

L-series and Hecke character. One can define an L-series associated to an elliptic curve E, which encodes, among many things, the ramification behavior of E during reduction. Recall that the Dirichlet L-function $L(s, \chi)$ which converges for $\Re s > 1$ has an analytic continuation to the whole complex plane and satisfies a functional equation. It remains a conjecture whether the L-series $L(s, E)$ associated to an elliptic curve E satisfy the same properties, namely, that it can be extended to the $\mathbf{C}$ and satisfies a functional equation of the form

$$L(E/L, 2) = L(E/L, 2 - s).$$

If E has CM, then this conjecture is verified. One can also define Hecke characters and Hecke L-series associated to an elliptic curve. See Chapter II §9, 10 of [12].

Iwasawa theory for elliptic curves. In the classical Iwasawa theory we consider the infinite cyclotomic tower over $\mathbf{Q}$ obtained by repetitively adjoining p^{th} root of unity and study the p-adic analogue of Riemann zeta function.



Substituting $\mathbf{Q}$ for K, an imaginary quadratic field, the role of ζ_{p^n} is played by the $\mathfrak{p}^n$-torsion points of E. We thus have an analogous infinite tower, the one on the right. The p-adic L-series $L(E, s)$ tells us about the p-part of Tate-Shafarevich group, which is helpful to understanding the conjecture of Birch and Swinnerton-Dyer. Skinner [9] has a nice exposition of this topic.

CM lifting problems. If A is an isotypic abelian variety defined over a finite field $\mathbb{F}_p$, then we may endow a CM structure on A with CM by a CM-field. We ask: under what conditions does A *lift* to an abelian scheme A' defined over a domain R of characteristic zero, such that $R \to \mathbb{F}_p$ is surjective and A' is isomorphic/isogenous to A over $\mathbb{F}_p$? For details we refer the reader to Conrad-Chai-Oort [1].

Modular forms and Galois representations. One can extend the notion of CM to the study of modular forms. Let f be a Hecke eigenform on $\Gamma_1(N)$ and denote by a_n the n-th coefficient of its Fourier expansion. Let φ be a nontrivial Dirichlet character mod N. We say that f has CM by φ if $\varphi(p)a_p = a_p$ for almost all primes p. Hecke and Shimura explicitly constructed newforms with CM.

Let K be the field generated by eigenvalues of f corresponding to the Hecke operators $\langle d\rangle$ and T_n. Let L the largest totally real subfield of K. Then it is not hard to prove that either $K = L$, or that K/L is a CM-field.

The theory of CM of eigenforms comes up in the study of ℓ-adic Galois representations attached to an eigenform. For many reasons, it is crucial to decipher the image of such a representation. It turns out, very roughly speaking, that f has CM if and only if the image of the associated Galois representation is abelian. Ribet [8] contains detail of the above discussions.

Elliptic-curve cryptography (ECC). Elliptic curves with CM also has fruitful applications to cryptography. The analytic action $\mathfrak{a} * E$ we studied in Section 2.1 can be usefully implemented as an encryption method. The theory of CM is also used to algorithmically generate an elliptic curve with prescribed number of points. This is called the *CM method*. The literature is vast.

Acknowledgments

It is a pleasure to thank my mentor Wei Yao who suggested to me this fascinating topic to read on in the first place. I thank both of my mentors, Wei and Pallav Goyal, for conducting weekly meetings with me and answering my questions. I also thank Prof. Peter May for organizing the REU from which I learned a lot of exciting new mathematics; I also thank him for providing me with valuable feedback. Finally, I thank Prof. Matthew Emerton for his encouragement and advice on learning mathematics.

References

[1] Conrad, Chai, & Oort. *Complex Multiplication and Lifting Problems.* American Mathematical Society, 2014.
[2] Hartshorne, Robin. *Algebraic Geometry,* GTM 52. Springer 1977.
[3] Kedlaya, Kiran S. *Notes on class field theory.* https://kskedlaya.org/cft/book-1.html
[4] Lang, Serge. *Elliptic Functions,* GTM 112. Springer-Verlag, New York, 1987.
[5] Milne, J.S. *The Fundamental Theorem of Complex Multiplication.* https://www.jmilne.org/math/articles/2007c.pdf
[6] Mumford, David. *Abelian varieties.* Tata Institute of Fundamental Research, Bombay, 1970.
[7] Poonen, Bjorn. *A Brief Summary of the Statements of Class Field Theory.* https://math.mit.edu/~poonen/papers/cft.pdf
[8] Ribet, K.A. *Galois representations attached to eigenforms with nebentypus.* Modular Functions of one Variable V, Bonn 1976. Springer Lecture Notes 601.
[9] Skinner, Christopher. *Lectures on the Iwasawa Theory of Elliptic Curves.* https://swc-math.github.io/aws/2018/2018SkinnerNotes.pdf
[10] Serre, J.P. *Local fields,* GTM 67. Springer, 1979.

[11] Shimura, Goro. *Abelian Varieties with Complex Multiplication and Modular Functions.* Princeton University Press, 1997.
[12] Silverman, Joseph H. *Advanced Topics in the Arithmetic of Elliptic Curves,* GTM 151. Springer, 1994.
[13] Silverman, Joseph H. *The Arithmetic of Elliptic Curves,* GTM 106. Springer, 2009.
[14] Sutherland, Andrew Note 28 Global class field theory and the Chebotarev density theorem, 18.785 MIT Number Theory I Notes. https://math.mit.edu/classes/18.785/2021fa/LectureNotes28.pdf
[15] Vakil, Ravi. *The Rising Sea: Foundations Of Algebraic Geometry,* version of Nov. 18, 2017. http://math.stanford.edu/~vakil/216blog/FOAGnov1817public.pdf