CLASS FIELD THEORY FOR NUMBER FIELDS AND COMPLEX MULTIPLICATION

GWYNETH MORELAND

Abstract. We state the main results of class field theory for a general number field, and then specialize to the case where K is imaginary quadratic. By looking at elliptic curves with $\mathrm{End}_{\mathbb{C}}(E) \cong \mathcal{O}_K$, i.e. E with complex multiplication by $\mathcal{O}_K$, we determine the Hilbert class field and ray class fields of K.

Contents

1. Introduction

A natural question in mathematics is classifying and understanding the extensions of a field. However, this is an incredibly difficult task – it is easier to understand Galois extensions, especially those with abelian Galois group. Such extensions are called abelian, and class field theory is the study of abelian extensions. One nice property of abelian extensions, and one of the main ideas of class field theory, is the surprising phenomenon where external properties of a field relate to intrinsic information. One of the first examples of this external-to-internal idea is quadratic reciprocity:

Example 1.1. For q, p distinct odd primes, quadratic reciprocity states:

$$\left(\frac{q}{p}\right)\left(\frac{p}{q}\right) = (-1)^{(\frac{p-1}{2})(\frac{q-1}{2})},$$

where (q/p) is the Legendre symbol. Essentially, knowing (q/p), it is easy to calculate (p/q). On the other hand, theory of quadratic number fields and their discriminants yields

- p ramifies in $\mathbb{Q}(\sqrt{q}) \iff (p) = \mathfrak{p}^2 \iff q = p$,
- p is totally split in $\mathbb{Q}(\sqrt{q}) \iff (p) = \mathfrak{p}\mathfrak{p}'$ for distinct prime ideals $\mathfrak{p}, \mathfrak{p}'$ $\iff (q/p) = 1$,
- p is inert in $\mathbb{Q}(\sqrt{q}) \iff (p)$ prime $\iff (q/p) = -1$.

Fix q, and vary p. Then checking the splitting behavior of p in $\mathbb{Q}(\sqrt{q})$ initially requires calculating the Legendre symbol (q/p) each time. But quadratic reciprocity allows us to calculate (p/q) instead, and there are only finitely many congruence classes to check to learn how all the different p split. Note that the $\mathbb{Z}/p\mathbb{Z}$ have no inherent relation to $\mathbb{Q}(\sqrt{q})$, while $\mathbb{Z}/q\mathbb{Z}$ depends on q like $\mathbb{Q}(\sqrt{q})$. Hence we can relate the external information of arithmetic in $\mathbb{Z}/p\mathbb{Z}$ and splitting behavior of q in quadratic extensions to the internal information of arithmetic in $\mathbb{Z}/q\mathbb{Z}$ and prime splitting in $\mathbb{Q}(\sqrt{q})$.

In our case, we want to relate field extensions to the instrinsic information of the class group, and the connection is the Artin map, which takes Galois groups to certain class-group type objects. The problem is that the main theorems of class field theory are rather non-constructive. However, in the case of quadratic number fields, we can give more explicit descriptions of the abelian extensions. We will utilize elliptic curves with "complex multiplication," which are elliptic curves whose endomorphism ring is larger than $\mathbb{Z}$. In this case $\mathrm{End}_{\mathbb{C}}(E) \cong \mathcal{O}_K$ where K is an imaginary quadratic extension of $\mathbb{Q}$, and by adjoining certain quantities coming from E we can obtain the abelian extensions of K.

We will begin with a review of number fields and basic class field theory, much of which draws from [Cox]. We will then specialize to imaginary quadratic number fields and use elliptic curves to better understand class field theory in that situation. In particular, we want to understand the Hilbert class field and ray class fields.To motivate why one would want to calculate these objects note that the Hilbert class field H is the maximal unramified abelian extension of K, and has the property that a prime ideal splits completely in H if and only if it is principal. In addition, any abelian extension of K is contained in a ray class field.

Our main result, which follows from Theorems 8.1 and 9.2, is the following:

Theorem 1.2. *Let K be an imaginary quadratic field, and E an elliptic curve over $\mathbb{C}$ with j-invariant $j(E)$. Suppose $\mathrm{End}_{\mathbb{C}}(E) \cong \mathcal{O}_K$. Let h be the Weber function and $\mathfrak{m}$ an $\mathcal{O}_K$-ideal. Then*

(i) $K(j(E))$ is the Hilbert class field of K,
(ii) $K(j(E), h(E[\mathfrak{m}]))$ is the ray class field of K of modulus $\mathfrak{m}$.

2. A review of number fields

2.1. **Basic properties.** Recall that a number field is a finite extension of $\mathbb{Q}$. Before continuing we remind the reader of the properties of number fields we'll need. This material is dealt with in most number theory books, and in particular [BoSh] and [La]. A reader familiar with number fields, definitions of ramification and splitting completely, and decomposition and inertia groups may skip this section.

Let K be a number field. We say $\alpha \in K$ is **integral** if it satisfies a monic polynomial in $\mathbb{Z}[x]$. Equivalently, $\mathbb{Z}[\alpha]$ is a finitely generated $\mathbb{Z}$ module. We then define $\mathcal{O}_K$ to be the set of integral elements of K. By the second formulation of integrality, it is clear that $\mathcal{O}_K$ is a ring, and we call it the **ring of integers of** K. Note that $\mathbb{Z} = \mathcal{O}_{\mathbb{Q}}$ under this definition.

One can show that $\mathcal{O}_K$ has K as its field of fractions, and that $\mathcal{O}_K$ is a free $\mathbb{Z}$-module of rank $[K : \mathbb{Q}]$. From the latter it is clear $\mathcal{O}_K/\mathfrak{a}$ must be finite for any nonzero ideal $\mathfrak{a}$ of $\mathcal{O}_K$. We define the norm of an ideal as

$$N(\mathfrak{a}) = |\mathcal{O}_K/\mathfrak{a}|. \tag{2.1}$$

A nice property of rings of integers of number fields is that they are **Dedekind**, which means $\mathcal{O}_K$ is integrally closed, Noetherian, and every nonzero prime ideal of $\mathcal{O}_K$ is maximal (Ch 9,[AM]). The most important property of Dedekind domains is that they have unique factorization of ideals (Corollary 9.4, [AM]). That is, if $\mathfrak{a}$ is an $\mathcal{O}_K$-ideal, we can write

$$\mathfrak{a} = \mathfrak{p}_1^{e_1} \dots \mathfrak{p}_g^{e_g},$$

where the $\mathfrak{p}_i$'s are distinct and prime. The decomposition is unique up to ordering, and the $\mathfrak{p}_i$ are precisely the prime ideals containing $\mathfrak{a}$. In general, we are not interested in the zero prime, and implicitly mean "nonzero prime ideal" when we say "prime ideal." We also use "prime of K" to mean a nonzero prime ideal of $\mathcal{O}_K$.

If $\mathfrak{a} = \mathfrak{p}_1^{e_1} \dots \mathfrak{p}_{\mathfrak{g}}{}^{e_g}$, then the Chinese remainder theorem says

$$\mathcal{O}_K/\mathfrak{a} \cong \mathcal{O}_K/(\mathfrak{p}_1{}^{e_1}) \times \dots \times \mathcal{O}_K/(\mathfrak{p}_r^{e_r}),$$

which can be used to calculate the factors $\mathfrak{p}_i$. One can also compute using the valuations of localizations of a Dedekind domain.

Let A be a Dedekind domain, $\mathfrak{a}$ a nonzero ideal of A. For any prime $\mathfrak{p}$ of A, $A_{\mathfrak{p}}$ is a DVR, i.e. local and a principal ideal domain. Let $\mathfrak{m}$ be the maximal ideal. Then there is a unique $n \in \mathbb{N} \cup \{0\}$ such that

$$\mathfrak{a}^e = \mathfrak{m}^n,$$

where $\mathfrak{m}^0 := (1)$, and $\mathfrak{a}^e$ is the extension of $\mathfrak{a}$ to $A_{\mathfrak{p}}$. We define this n to be the **valuation of $\mathfrak{a}$ at $\mathfrak{p}$**, and denote it by $\nu_{\mathfrak{p}}(\mathfrak{a})$. Then:

$$\mathfrak{a} = \prod_{\mathfrak{p} \text{ prime}} \mathfrak{p}^{\nu_{\mathfrak{p}}(\mathfrak{a})}.$$

This unique factorization applies to fractional ideals as well. A **fractional ideal** I of $\mathcal{O}_K$ is a nonzero $\mathcal{O}_K$-submodule of K such that $\alpha I \subseteq \mathcal{O}_K$ for some $\alpha \in K^*$.

Equivalently, since $\mathcal{O}_K$ is Noetherian, they are the nonzero finitely generated $\mathcal{O}_K$-submodules of K.

Proposition 2.1. *Let $\mathfrak{a}$ be a fractional $\mathcal{O}_K$-ideal. Then:*

(i) $\mathfrak{a}$ is invertible: there exists a fractional $\mathcal{O}_K$-ideal $\mathfrak{b}$ such $\mathfrak{ab} = \mathcal{O}_K$. The inverse of $\mathfrak{a}$ is denoted $\mathfrak{a}^{-1}$.

(ii) $\mathfrak{a}$ can uniquely be written as a product

$$\mathfrak{a} = \mathfrak{p}_1^{e_1} \dots \mathfrak{p}_r^{e_r},$$

where the e_i's are in $\mathbb{Z}$ and the $\mathfrak{p}_i$ are prime ideals in $\mathcal{O}_K$.

The above makes I_K, the set of invertible ideals of $\mathcal{O}_K$, into an abelian group. The principal ideals

$$P_K = \{\alpha\mathcal{O}_K : \alpha \in K^\times\}$$

form a subgroup.

Definition 2.2. Then the **class group of** $\mathcal{O}_K$ is given by

$$\mathrm{C}(\mathcal{O}_K) = I_K/P_K.$$

Remark 2.3. *Intuitively, the class group is supposed to measure the degree to which $\mathcal{O}_K$ fails to be a UFD. For example, $\mathbb{Z}[\sqrt{-5}] = \mathcal{O}_{\mathbb{Q}(\sqrt{-5})}$ does not have unique factorization, as*

$$2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5}).$$

However, $\mathbb{Z}[\sqrt{-5}]$ almost has a divison algorithm, as in integer translates of the ellipse $x^2 + 5y^2 = 1$ corresponding to the norm on $\mathbb{Z}[\sqrt{-5}]$ almost tile the plane. Recall that Euclidean domains (domains with a notion of division) are UFDs. So the fact that $\mathbb{C}(\mathbb{Z}[\sqrt{-5}]) = \mathbb{Z}/2\mathbb{Z}$ is small but nontrivial lines up with this intuition of "barely failing" to have unique factorization.

2.2. **Ramification and splitting.** We now turn our attention to the notion of ramification. Let K be a number field, and L a finite extension. We are interested in studying how primes $\mathfrak{p}$ of K decompose in $\mathcal{O}_L$. If $\mathfrak{p}$ is a prime ideal of $\mathcal{O}_K$, then $\mathfrak{p}\mathcal{O}_L$ is an ideal, and has a prime factorization:

$$\mathfrak{p}\mathcal{O}_L = \mathfrak{P}_1^{e_1} \dots \mathfrak{P}_g^{e_g},$$

where the $\mathfrak{P}_i$ are the primes of $\mathcal{O}_L$ containing $\mathfrak{p}$. Such primes are said to **lie over** $\mathfrak{p}$.

The integer $e_i = \nu_{\mathfrak{P}_i}(\mathfrak{p}\mathcal{O}_L)$ is often called the **ramification index** of $\mathfrak{p}$ in $\mathfrak{P}_i$, and is often written $e_{\mathfrak{P}_i|p}$.

Each prime $\mathfrak{P}_i$ of L containing $\mathfrak{p}$ gives an extension of residue fields

$$\mathcal{O}_K/\mathfrak{p} \subseteq \mathcal{O}_L/\mathfrak{P}_i,$$

and the degree of this extension f_i or $f_{\mathfrak{P}_i|\mathfrak{p}}$ is the **inertial degree** of $\mathfrak{p}$ in $\mathfrak{P}_i$. These two quantities are related to the degree of L/K via a nice identity.

Theorem 2.4. *Let $\mathfrak{p}$ be a prime of K, and L/K be a finite extension. Let $\mathfrak{p}\mathcal{O}_L = \mathfrak{P}_1^{e_1} \dots \mathfrak{P}_g^{e_g}$, with inertial degrees f_i for each respective prime $\mathfrak{P}_i$. Then:*

$$\sum_{i=1}^{g} e_i f_i = [L : K]. \tag{2.2}$$

Proof. See Chapter 3, Section 5 of [BoSh], namely equation (5.12) and surrounding exposition. Alternatively, see I.§7, Proposition 21 of [La]. □

In the case where L is Galois over K, the situation becomes nicer:

Theorem 2.5. *Suppose L is Galois over K, and $\mathfrak{p}$ is a prime of K. Then $\mathrm{Gal}(L/K)$ acts transitively on the primes of L lying over (containing) $\mathfrak{p}$, i.e. if $\mathfrak{P}, \mathfrak{P}'$ lie over $\mathfrak{p}$, then there exists $\sigma \in \mathrm{Gal}(L/K)$ such that $\sigma(\mathfrak{P}) = \mathfrak{P}'$. Consequently all the primes $\mathfrak{P}_1, \ldots, \mathfrak{P}_g$ of L lying over $\mathfrak{p}$ all have the same ramification index e and the same inertial degree f. Hence formula (2.2) becomes*

$$efg = [L : K]. \tag{2.3}$$

Proof. See Lang ([La]), I.§7, Corollary 2. □

For a finite extension L/K, we say $\mathfrak{p}$ a prime of K **ramifies** in L if any of the e_i are greater than 1, and $\mathfrak{p}$ is **unramified** if all the e_i equal 1. For Galois extensions L of K, this reduces to $\mathfrak{p}$ is ramified if $e > 1$ and unramified if $e = 1$. In general, only a finite number of primes ramify (see III.§2, Proposition 8 in [La]).

For a Galois extension, we have a stronger condition: $\mathfrak{p}$ is said to **split completely** if $e = f = 1$. Looking at formula (2.2), this says $\mathfrak{p}$ splits into the maximum number of primes possible, $[L : K]$.

Example 2.6. The most basic example is rational primes factoring in $\mathbb{Z}[i]$. Let (p) be a prime ideal of $\mathbb{Z} = \mathcal{O}_{\mathbb{Q}}$.

(i) If $p \equiv 3 \bmod 4$, then (p) remains prime in $\mathbb{Z}[i] = \mathcal{O}_{\mathbb{Q}(i)}$, and (p) has inertial degree 2 as $\mathbb{Z}[i]/(p) \cong \mathbb{F}_{p^2}$. In this case equation (2.2) becomes $1 \cdot 2 \cdot 1 = 2 = [\mathbb{Q}(i) : \mathbb{Q}]$, and (p) is unramified.

(ii) If $p \equiv 1 \bmod 4$, then (p) splits as $(p) = (a + bi)(a - bi)$ with $a + bi, a - bi$ prime. In this case $\mathbb{Z}[i]/(a+bi) \cong \mathbb{Z}[i]/(a-bi) \cong \mathbb{F}_p$. Equation (2.2) becomes $1 \cdot 1 \cdot 2 = 2$, and (p) splits completely.

(iii) If $p = 2$, then $(2) = (1 + i)^2$. Hence (2) is the only prime of $\mathbb{Q}$ that ramifies, and the ramification index of the only prime lying above it is 2.

Again take L to be Galois over K. For a prime $\mathfrak{P}$ of L lying over $\mathfrak{p}$ in K, we can relate $\widetilde{D} := \mathrm{Gal}((\mathcal{O}_L/\mathfrak{P})/(\mathcal{O}_K/\mathfrak{p}))$ to a subgroup of $\mathrm{Gal}(L/K)$.

Definition 2.7. We define the **decomposition group** and **inertia group** of $\mathfrak{P}$ to be

$$D_{\mathfrak{P}} = \{\sigma \in \mathrm{Gal}(L/K) : \sigma(\mathfrak{P}) = \mathfrak{P}\},$$
$$I_{\mathfrak{P}} = \{\sigma \in \mathrm{Gal}(L/K) : \sigma(\alpha) \equiv \sigma \bmod \mathfrak{P} \text{ for all } \alpha \in \mathcal{O}_L\},$$

respectively. Note the dependence on K.

By definition $I_{\mathfrak{P}}$ is contained in $D_{\mathfrak{P}}$. An element of $\sigma \in D_{\mathfrak{P}}$ induces $\widetilde{\sigma} \in \widetilde{D}$ since σ fixes $\mathfrak{p} = \mathfrak{P} \cap \mathcal{O}_K$. The kernel of $\sigma \mapsto \widetilde{\sigma}$ is clearly $I_{\mathfrak{P}}$.

Proposition 2.8. *Reduction modulo $\mathfrak{P}$ induces an exact sequence:*

$$1 \to I_{\mathfrak{P}} \to D_{\mathfrak{P}} \to \widetilde{D} \to 1$$

such that

(i) $\widetilde{D}$ is cyclic of order f,

(ii) $|I_{\mathfrak{P}}| = e$,

(iii) $[\mathrm{Gal}(L/K) : D_{\mathfrak{P}}] = g$.

Proof. See [La], I.§5, Proposition 14 and I.§7, Corollary 3. □

Corollary 2.9.

(i) $\mathfrak{p}$ *is unramified in* $L \iff D_{\mathfrak{P}} \cong \widetilde{D}$.
(ii) $\mathfrak{p}$ *splits* ($\mathfrak{p}\mathcal{O}_L$ *is not prime in* $\mathcal{O}_L$) $\iff D_{\mathfrak{P}} \neq \mathrm{Gal}(L/K)$,
(iii) $\mathfrak{p}$ *splits completely* $\iff D_{\mathfrak{P}}$ *is trivial.*

3. Unramified class field theory and the Artin symbol

The Hilbert class field H is the maximal unramified abelian extension: no primes of K ramify in H, $\mathrm{Gal}(H/K)$ is abelian, and any other extension of K with this property is contained in H. This object has a few interesting properties: the "class" in the name comes from its relation to the class group, both in its Galois group and how splitting behavior in H corresponds to being trivial or nontrivial in $\mathrm{C}(\mathcal{O}_K)$.

However, to discuss the Hilbert class field, we need to refine the notion of unramified. Specifically, we want to keep track of so-called "infinite primes". A **real infinite prime** is an embedding $\sigma : K \to \mathbb{R}$, while a **complex infinite prime** is a pair of conjugate embeddings $\sigma, \overline{\sigma} : K \to \mathbb{C}$ with $\sigma(K) \not\subseteq \mathbb{R}$. An infinite prime σ of K ramifies in L if σ is real but any of its extensions to L is complex.

An **unramified extension of** K is an extension where all primes of K, finite or infinite, are unramified. This is a rather unwieldly condition in general, but for unramified abelian extensions we have the following:

Theorem 3.1. *The Hilbert class field exists, and forms a finite extension of* K.

The proof is delayed until Section 4. Clearly H is unique, and we call it the Hilbert class field. To study its relation to the class group, we introduce the Artin symbol.

Proposition 3.2. *Let* L *be Galois over* K. *Let* $\mathfrak{p}$ *be a prime of* K, *unramified in* L. *If* $\mathfrak{P}$ *is a prime of* L *lying over* $\mathfrak{p}$, *then there is a unique* $\sigma \in \mathrm{Gal}(L/K)$ *such that for all* $\alpha \in \mathcal{O}_L$:

$$\sigma(\alpha) \equiv \alpha^{N(\mathfrak{p})} \bmod \mathfrak{P} \tag{3.1}$$

Proof. First we show existence. Consider $D_{\mathfrak{P}}$ and $I_{\mathfrak{P}}$ the decomposition and inertial groups for $\mathfrak{P}$, respectively. As $\mathfrak{p}$ is unramified in L, Proposition 2.8 tells us $|I_{\mathfrak{P}}| = e_{\mathfrak{P}|p} = 1$ and that

$$D_{\mathfrak{P}} \cong \widetilde{D},$$

via $\sigma \mapsto \widetilde{\sigma}$. If $\mathcal{O}_K/\mathfrak{p}$ has $q = N(\mathfrak{p})$ elements, then $\widetilde{G}$ is generated by the Frobenius automorphism $x \mapsto x^q$. Hence there is a *unique* $\sigma \in D_{\mathfrak{P}}$ that maps to this Frobenius element, and it satisfies the desired condition

$$\sigma(\alpha) \equiv \alpha^{N(\mathfrak{p})} \bmod \mathfrak{P}.$$

For uniqueness, if $\sigma' \in \mathrm{Gal}(L/K)$ satisfies (3.1) then for any $\alpha \in \mathfrak{P}$, $\sigma'(\alpha) \cong 0 \bmod \mathfrak{P}$, and hence $\sigma' \in D_{\mathfrak{P}}$. □

We call the unique $\sigma \in \mathrm{Gal}(L/K)$ satisfying (3.1) the **Artin symbol** and denote it by

$$\left(\frac{L/K}{\mathfrak{P}}\right).$$

Corollary 3.3. *Let L be Galois over K, $\mathfrak{p}$ a prime of K unramified in L, and $\mathfrak{P}$ a prime lying over it. Then:*

(i) For $\sigma \in \mathrm{Gal}(L/K)$, we have

$$\left(\frac{L/K}{\sigma(\mathfrak{P})}\right) = \sigma\left(\frac{L/K}{\mathfrak{P}}\right)\sigma^{-1} \tag{3.2}$$

(ii) The order of $((L/K)/\mathfrak{P})$ is the inertial degree $f = f_{\mathfrak{P}|\mathfrak{p}}$.
(iii) $\mathfrak{p}$ splits completely in L if and only if $((L/K)/\mathfrak{P}) = 1$.

If $\mathrm{Gal}(L/K)$ is abelian, then the Artin symbol $((L/K)/\mathfrak{P})$ only depends on the prime $\mathfrak{p} = \mathfrak{P} \cap \mathcal{O}_K$. In this case it is appropriate to write $((L/K)/\mathfrak{p})$ for the Artin symbol and talk about an Artin symbol of $\mathfrak{p}$, a prime of K.

When L/K is an unramified Abelian extension, $((L/K)/\mathfrak{p})$ is defined for all primes of K. By Proposition 2.1, any fractional ideal $\mathfrak{a} \in I_K$ factors as $\mathfrak{a} = \prod_{i=1}^{r} \mathfrak{p}_i^{r_i}$, $r_i \in \mathbb{Z}$. So we may extend the Artin symbol to a homomorphism, called the **Artin map**

$$\left(\frac{L/K}{\cdot}\right) : I_K \to \mathrm{Gal}(L/K)$$

by setting

$$\left(\frac{L/K}{\mathfrak{a}}\right) = \prod_{i=1}^{r}\left(\frac{L/K}{\mathfrak{p}_i}\right)^{r_i}.$$

The next few propositions make clear the correspondence between unramified abelian extensions and the class group. Their proofs will follow from Section 4.

Theorem 3.4 (Artin reciprocity for the Hilbert class field)**.** *If H is the Hilbert class field of K, then the Artin map*

$$\left(\frac{H/K}{\cdot}\right) : I_K \to \mathrm{Gal}(H/K),$$

is surjective with kernel P_K. Hence the Artin map descends to an isomorphism $\mathrm{C}(\mathcal{O}_K) \cong \mathrm{Gal}(H/K)$.

Applying the Galois correspondence between subgroups and subfields yields:

Corollary 3.5. *There is a one-to-one correspondence between unramified Abelian extensions M of K and subgroups H of $\mathrm{C}(\mathcal{O}_K)$. If M is the fixed field of $H \leq \mathrm{C}(\mathcal{O}_K) \cong \mathrm{Gal}(H/K)$, then the Artin map $((M/K), \cdot)$ induces an isomorphism:*

$$\mathrm{C}(\mathcal{O}_K)/H \cong \mathrm{Gal}(M/K).$$

Corollary 3.6 (Principal Ideal Theorem)**.** *Let H be the Hilbert class field of K. Let $\mathfrak{p}$ be a prime of K. Then*

$$\mathfrak{p} \text{ splits completely in } H \iff \mathfrak{p} \text{ is a principal ideal of } K.$$

Proof. All primes are unramified in H, so Corollary 3.3 says $\mathfrak{p}$ splits completely if and only if $((L/K)/\mathfrak{p}) = 1$, which is equivalent by Theorem 3.4 to $\mathfrak{p}$ being trivial in $\mathrm{C}(\mathcal{O}_K)$. □

4. General class field theory

Class field theory allows us to relate external information, abelian extensions of K, in terms of information internal to K, the generalized ideal class groups. We saw an example of this in Section 3, but in this section we will outline the main theorems of class field theory in their full power.

4.1. **Generalized class groups.** As the name suggests, generalized ideal class groups look like a set of fractional ideals quotiented out by some principal subgroup. We parametrize these via moduli. A **modulus** $\mathfrak{m}$ of K is a product $\mathfrak{m}_0\mathfrak{m}_\infty$, where $\mathfrak{m}_0$ is a product of primes and $\mathfrak{m}_\infty$ is a product of distinct infinite primes.

We define $I_K(\mathfrak{m})$ to be the subgroup of I_K generated by $\mathcal{O}_K$-ideals coprime to $\mathfrak{m}$ (i.e. coprime to $\mathfrak{m}_0$). Inside it is $P_{K,1}(\mathfrak{m})$, the subgroup generated by principal $\mathcal{O}_K$-ideals of the form $\alpha\mathcal{O}_K$ where α satisfies:

(1) $\alpha \equiv 1 \bmod \mathfrak{m}_0$,
(2) $\sigma(\alpha) > 0$ for every real infinite prime $\sigma \mid \mathfrak{m}_\infty$.

$P_{K,1}(\mathfrak{m})$ has finite index in $I_K(\mathfrak{m})$ (see IV.1.3 in [Ja]). A subgroup $H \leq I_K(\mathfrak{m})$ is a **congruence subgroup** for $\mathfrak{m}$ if

$$P_{K,1}(\mathfrak{m}) \subseteq H \subseteq I_K(\mathfrak{m}),$$

holds, and the quotient

$$I_K(\mathfrak{m})/H,$$

is called a **generalized ideal class group** for $\mathfrak{m}$. For $\mathfrak{m} = 1$, $P_K = P_{K,1}(1)$ and $I_K = I_K(1)$. Then the class group $\mathrm{C}(\mathcal{O}_K) = I_K(1)/P_{K,1}(1)$ is a generalized ideal class group.

4.2. **The basic theorems of class field theory.** We now state the correspondence between generalized ideal class groups of K and abelian extensions of K. The link between these two is the Artin symbol from Proposition 3.2. Let L be a finite abelian extension of K a number field. Suppose $\mathfrak{m}$ is a modulus divisible by all primes of K ramifying in L. Then for $\mathfrak{p}$ not dividing $\mathfrak{m}$, the Artin symbol $((L/K)/\mathfrak{p})$ is defined. Note that $I_K(\mathfrak{m})$ is generated by all the prime ideals coprime to $\mathfrak{m}$. Extending by multiplicativity, we have a homomorphism:

$$\Phi_\mathfrak{m} : I_K(\mathfrak{m}) \to \mathrm{Gal}(L/K), \tag{4.1}$$

which we call the **Artin map** for L/K. There are multiple extensions for which $\Phi_\mathfrak{m}$ is defined: when we want to refer to a specific extension and its Artin map, we write $\Phi_{L/K,\mathfrak{m}}$.

Theorem 4.1 (Artin Reciprocity Theorem)**.** *Let L/K be a finite abelian extension, $\mathfrak{m}$ a modulus divisible by all primes of K, finite or infinite, that ramify in L. Then:*

(i) The Artin map $\Phi_\mathfrak{m}$ is surjective.
(ii) If the exponents of the finite primes of $\mathfrak{m}$ are sufficiently large, then $\ker(\Phi_\mathfrak{m})$ is a congruence subgroup for $\mathfrak{m}$ and

$$\Phi_\mathfrak{m} : I_K(\mathfrak{m})/\ker(\Phi_\mathfrak{m}) \xrightarrow{\cong} \mathrm{Gal}(L/K),$$

realizes $\mathrm{Gal}(L/K)$ as a generalized ideal class group for the modulus $\mathfrak{m}$.

Proof. See Janusz ([Ja]), Chapter V, Theorem 5.7. □

The "reciprocity" in the name of Theorem 3.4 refers to the fact that the Artin symbol lets us relate external information (extensions of K) to internal information and arithmetic (the class group). A key fact is that $P_{K,1}(\mathfrak{m}) \subseteq \ker(\Phi_{\mathfrak{m}})$ tells us the Artin symbol does not change by multiplication by $\alpha \in \mathcal{O}_K$ with $\alpha \equiv 1 \bmod \mathfrak{m}$.

We say a finite abelian extension L/K **admits** a modulus $\mathfrak{m}$ if every prime that ramifies along L/K appears in $\mathfrak{m}$ and $\ker \Phi_{L/K,\mathfrak{m}}$ is a congruence subgroup for $\mathfrak{m}$. Unfortunately, L/K does not admit a unique modulus: if $\mathfrak{m} \mid \mathfrak{n}$, then

$$P_{K,1}(\mathfrak{m}) \subseteq \ker(\Phi_{\mathfrak{m}}) \Rightarrow P_{K,1}(\mathfrak{n}) \subseteq \ker(\Phi_{\mathfrak{n}}). \tag{4.2}$$

The implication above suggests that there might be a nice, minimal modulus.

Theorem 4.2 (Conductors and Existence)**.** *Let K be a number field.*

(i) Every finite abelian extension L/K admits some modulus, and there is a minimal such modulus $\mathfrak{f} = \mathfrak{f}(L/K)$ under the divisibility relation, called the ***conductor****.*

(ii) Given a modulus $\mathfrak{m}$, the map $L \mapsto \ker \Phi_{L/K,\mathfrak{m}}$ is an inclusion-reversing bijection between finite abelian extensions that admit $\mathfrak{m}$ and congruence subgroups for $\mathfrak{m}$.

Proof. For (i), see [Ja], Chapter V, Section 6 and Theorem 12.7. For (ii), see [Ja], Chapter V, Theorem 9.16. □

Corollary 4.3. *Let L, M be abelian extensions of K. Then $L \subseteq M$ if and only if there exists a modulus $\mathfrak{m}$, divisible by all primes of K that ramify in L or M such that*

$$P_{K,1}(\mathfrak{m}) \subseteq \ker(\Phi_{M/K,\mathfrak{m}}) \subseteq \ker(\Phi_{L/K,\mathfrak{m}}).$$

Proof. See Corollary 8.7 in [Cox]. □

With the main theorems of class field theory, we can now show the existence of the Hilbert class field. Consider the modulus $\mathfrak{m} = 1$. In this case, $I_K(\mathfrak{m}) = I_K$ and $P_{K,1}(\mathfrak{m}) = P_K$. Applying the existence theorem to $\mathfrak{m} = 1$ and the congruence subgroup P_K, we get a unique abelian extension H such that the Artin map gives an isomorphism $\mathrm{C}(\mathcal{O}_K) \cong \mathrm{Gal}(H/K)$. We call H the Hilbert class field of K. Clearly, H is an unramified extension. It is also the maximal such extension.

Proof of Theorem 3.1. We wish to show that any unramified abelian extension of K is contained in H. Let M be an unramified abelian extension. It is clear from the basic properties of the conductor that $\mathfrak{f}(M/K) = 1$ and that

$$\ker(\Phi_{H/K,1}) = P_K \subseteq \ker(\Phi_{M/K,1}).$$

By Corollary 4.3, $M \subseteq H$. □

4.3. **Čebotarev density.** We can define a density on the set of finite primes, called the Dirichlet density. By studying the Artin L-functions of a number field, one can derive some properties about the density. More details can be found in §8.B of [Cox], but some of the main results are presented here.

Proposition 4.4. *Let L be an abelian extension of K. Let $\mathfrak{m}$ be a modulus divisible by all primes that ramify in L, finite or infinite. Then for any $\sigma \in \mathrm{Gal}(L/K)$, there are infinite many primes $\mathfrak{p}$ of K with $((L/K)/\mathfrak{p}) = \sigma$.*

We have the following, which is a more general version of Dirichlet's theorem on primes in arithmetic progressions.

Theorem 4.5. *Let K be a number field, $\mathfrak{m}$ an integral ideal of K (note that these are the moduli if K is imaginary quadratic). Then every ideal class of $I_K(\mathfrak{m})/P_{K,1}(\mathfrak{m})$ contains infinitely many degree-1 primes of K, i.e. $\mathfrak{p}$ with $N(\mathfrak{p}) = p$.*

Lastly, one of the most useful results from Čebotarev density is the ability to show containment of extensions based on their prime splitting behavior.

Corollary 4.6. *Let L, M be Galois extensions of K. Then $L \subseteq M$ if and only if*

$$\mathfrak{p} \text{ splits completely in } M \Rightarrow \mathfrak{p} \text{ splits completely in } L$$

holds for all but finitely many primes $\mathfrak{p}$ of K.

Proof. See Theorem 8.19 in [Cox]. □

4.4. **Class field theory over $\mathbb{Q}$.** Class field theory over $\mathbb{Q}$ is summarized by Kronecker-Weber, which says every abelian extension of $\mathbb{Q}$ is contained in a cyclotomic field. Our results from 4.1 allow us to give a quick proof.

Lemma 4.7. *The conductor $\mathfrak{f} = \mathfrak{f}(\mathbb{Q}(\zeta_m)/\mathbb{Q})$ is $m\infty$. Here ζ_m is a primitive m-th root of unity, $m > 2$, and ∞ is the real prime of $\mathbb{Q}$.*

Proof. First we want that a prime divides $m\infty$ if and only if it ramifies in $\mathbb{Q}(\zeta_m)$. Note that ∞ ramifies when extended to $\mathbb{Q}(\zeta_m)$. For a treatment of the finite primes, see I.§10 in [Neu].

The Galois group $\mathrm{Gal}(\mathbb{Q}(\zeta_m)/\mathbb{Q}))$ is isomorphic to $(\mathbb{Z}/m\mathbb{Z})^\times$, where $[a] \in (\mathbb{Z}/m\mathbb{Z})^\times$ acts by $\zeta \mapsto \zeta^a$. We wish to calculate the Artin symbol $((\mathbb{Q}(\zeta_m)/\mathbb{Q})/p)$, for $p \nmid m$. But knowing that $\mathcal{O}_{\mathbb{Q}(\zeta_m)} = \mathbb{Z}[\zeta_m]$ (see I.§10.2 in [Neu]), it is clear that $[p]$ is the Artin symbol. Hence:

$$\begin{aligned}\Phi_{\mathbb{Q}(\zeta_m)/\mathbb{Q},m\infty} : I_{\mathbb{Q}}(m\infty) &\to \mathrm{Gal}(\mathbb{Q}(\zeta_m)/\mathbb{Q})) = (\mathbb{Z}/m\mathbb{Z})^\times \\ (a/b)\mathbb{Z} &\mapsto [a][b]^{-1}.\end{aligned}$$

It follows that

$$\ker(\Phi_{\mathbb{Q}(\zeta_m)/\mathbb{Q},m\infty}) = P_{\mathbb{Q},1}(m\infty).$$

Then $m\infty$ satisfies the minimality condition of the conductor, so $f(\mathbb{Q}(\zeta_m)/\mathbb{Q}) = m\infty$. □

Theorem 4.8 (Kronecker-Weber)**.** *A finite abelian extension L of $\mathbb{Q}$ is contained in some cyclotomic field. That is, $L \subseteq \mathbb{Q}(\zeta_m)$ for some m.*

Proof. Artin Reciprocity (Theorem 4.1) says there is a modulus $\mathfrak{m}$ such that

$$P_{\mathbb{Q},1}(\mathfrak{m}) \subseteq \ker(\Phi_{L/\mathbb{Q},\mathfrak{m}}).$$

By (4.2), we may assume $\mathfrak{m} = m\infty$. From the calculation in Lemma 4.7, we have

$$P_{\mathbb{Q},1}(\mathfrak{m}) = \ker(\Phi_{\mathbb{Q}(\zeta_m)/\mathbb{Q},\mathfrak{m}}) \subseteq \ker(\Phi_{L/K,\mathfrak{m}}).$$

By Corollary 4.3, $L \subseteq \mathbb{Q}(\zeta_m)$. □

5. Orders in quadratic fields

5.1. **Basic definitions.** We want analogues of the Hilbert class field and results on quadratic-looking rings besides $\mathcal{O}_K$ for K an imaginary quadratic field. To motivate this: if $d \equiv 1 \bmod 4$, then

$$\mathcal{O}_{\mathbb{Q}(\sqrt{d})} = \mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right],$$

(see [Sa], §§2.5, Theorem 1). Section 3 gives us information about $\mathbb{Z}[\frac{1+\sqrt{d}}{2}]$, but $\mathbb{Z}[\sqrt{d}]$ is also a completely natural ring to study. Understanding these rings is tied to understanding symmetry of elliptic curves, as we will see in Section 7. The question becomes: what can we say about "nice" subrings of $\mathcal{O} \subsetneq \mathcal{O}_K$ for K a quadratic number field? While $\mathcal{O}$ isn't Dedekind and fractional ideals are not always invertible, perhaps we can get unique factorization for certain ideals and define a modified class group. The objects we want to study are called **orders** along with **proper ideals**.

Definition 5.1. An **order** $\mathcal{O}$ of a quadratic number field K is a subring $\mathcal{O} \subseteq K$ such that:

(i) $\mathcal{O}$ is a finitely generated $\mathbb{Z}$-module,
(ii) $\mathcal{O}$ is generated over $\mathbb{Z}$ by a $\mathbb{Q}$-basis of K.

Note that $\mathcal{O} \subseteq \mathcal{O}_K$ and $\mathcal{O}$ is a free $\mathbb{Z}$-module of rank 2 as a consequence of the definition.

All orders can be described in terms of the maximal order $\mathcal{O}_K$:

Lemma 5.2. *Let $\mathcal{O}$ be an order in a quadratic number field K. Then $\mathcal{O}$ has finite index in $\mathcal{O}_K$, and setting $f := [\mathcal{O}_K : \mathcal{O}]$ we see*

$$\mathcal{O} = \mathbb{Z} + f\mathcal{O}_K.$$

*We call the index $f = [\mathcal{O}_K : \mathcal{O}]$ the **conductor** of $\mathcal{O}$.*

Proof. See Lemma 7.2 in [Cox]. □

The same proof for $\mathcal{O}_K$ shows $\mathcal{O}$ is Noetherian and all prime ideals are maximal, but if the conductor is greater than 1, $\mathcal{O}$ is not integrally closed in $K = \mathrm{Frac}(\mathcal{O})$ and therefore not Dedekind. However, if we had a way to move between ideals of $\mathcal{O}$ and $\mathcal{O}_K$, we could transport information and properties of $\mathcal{O}_K$. To this end, we define proper ideals. An ideal $\mathfrak{a}$ of $\mathcal{O}$ is **proper** provided that

$$\mathcal{O} = \{\beta \in K : \beta\mathfrak{a} \subseteq \mathfrak{a}\}.$$

For $\mathcal{O} = \mathcal{O}_K$, note that all ideals are proper. A **fractional ideal** of $\mathcal{O}$ is a nonzero finitely generated $\mathcal{O}$-submodule of K. Every such fractional ideal is of the form $\alpha\mathfrak{a}$ with $\alpha \in K^\times$ and $\mathfrak{a}$ is an $\mathcal{O}$-ideal. Similarly, a fractional $\mathcal{O}$-ideal $\mathfrak{b}$ is proper provided that

$$\mathcal{O} = \{\beta \in K : \beta\mathfrak{b} \subseteq \mathfrak{b}\}.$$

Lemma 5.3. *Let $\mathfrak{a}$ be a fractional $\mathcal{O}$-ideal. Then $\mathfrak{a}$ is proper if and only if $\mathfrak{a}$ is invertible.*

Proof. See Proposition 7.4 in [Cox]. □

The following is a useful criterion for properness:

Lemma 5.4. *Let $\mathcal{O}$ be an order with conductor f.*

(i) An $\mathcal{O}$-ideal $\mathfrak{a}$ is coprime to f (i.e. $\mathfrak{a} + f\mathcal{O} = \mathcal{O}$) if and only if $N(\mathfrak{a}) = |\mathcal{O}/\mathfrak{a}|$ is relatively prime to f.

(ii) Every $\mathcal{O}$-ideal coprime to f is proper.

From the previous results,

$$I(\mathcal{O}) = \{\mathfrak{a} : \mathfrak{a} \text{ a proper fractional } \mathcal{O}\text{-ideal}\}$$

is a group, and it has a subgroup $P(\mathcal{O})$ consisting of all principal $\mathcal{O}$-ideals.

Definition 5.5. The **ideal class group** of $\mathcal{O}$ is defined as:

$$\mathrm{C}(\mathcal{O}) := I(\mathcal{O})/P(\mathcal{O}).$$

We will prove a few other useful expressions for $\mathrm{C}(\mathcal{O})$. By Lemma 5.4, and the fact that $N(\mathfrak{ab}) = N(\mathfrak{a})N(\mathfrak{b})$, the $\mathcal{O}$-ideals coprime to (f) are closed under multiplication. Take $I(\mathcal{O}, f)$ to be the subgroup of $I(\mathcal{O})$ *generated* by $\mathcal{O}$-ideals coprime to f. Inside it is the subgroup $P(\mathcal{O}, f)$, generated by the principal $\mathcal{O}$-ideals coprime to f.

We can also define $I_K(f)$, the subgroup of I_K generated by $\mathcal{O}_K$ ideals coprime to f. Inside of it is $P_{K,\mathbb{Z}}(f)$, generated by principal ideals of the form $\alpha\mathcal{O}_K$ where $\alpha \equiv a \bmod f\mathcal{O}_K$ for some integer a relatively prime to f.

Theorem 5.6.

(i) If $\mathfrak{a}$ is an $\mathcal{O}_K$-ideal coprime to f, then $\mathfrak{a} \cap \mathcal{O}$ is an $\mathcal{O}$-ideal coprime to f. If $\mathfrak{b}$ is an $\mathcal{O}$-ideal coprime to f then $\mathfrak{b}\mathcal{O}_K$ is an $\mathcal{O}_K$-ideal coprime to f. These maps are norm-preserving, and induce an isomorphism $I_K(f) \cong I(\mathcal{O}, f)$.

(ii) There are natural isomorphisms

$$\mathrm{C}(\mathcal{O}) \cong I(\mathcal{O}, f)/P(\mathcal{O}, f) \cong I_K(f)/P_{K,\mathbb{Z}}(f),$$

where $I(\mathcal{O}, f)/P(\mathcal{O}, f) \cong I_K(f)/P_{K,\mathbb{Z}}(f)$ is induced by the maps in (i).

Corollary 5.7. *The elements of $I(\mathcal{O}, f)$ have unique factorization into prime ideals that are also coprime to f.*

Proof. Follows from Theorem 5.6 by transporting the factorization in $I_K(f)$ to $I(\mathcal{O}, f)$. Moving the factorization back to $I_K(f)$ shows uniqueness. □

Theorem 5.6 lets us view ideals coprime to the conductor as ideals in $\mathcal{O}_K$ which, as evidenced by the above Corollary, is quite useful.

5.2. **The ring class field.** For the ideal class group of an order, we have the presentation $\mathrm{C}(\mathcal{O}) \cong I_K(f)/P_{K,\mathbb{Z}}(f)$ from Theorem 5.6. Looking at the definition of $I_K(\mathfrak{m}), P_{K,1}(\mathfrak{m})$, we see

$$P_{K,1}(f\mathcal{O}_K) \subseteq P_{K,\mathbb{Z}}(f) \subseteq I_K(f) = I_K(f\mathcal{O}_K).$$

So $\mathrm{C}(\mathcal{O})$ is a generalized ideal class group, with $P_{K,\mathbb{Z}}(f)$ a congruence subgroup for $\mathfrak{m} = f\mathcal{O}_K$. By the Existence theorem (4.2), this data determines a unique abelian extension L of K. We call this extension the **ring class field**. Observe that the ring class field of $\mathcal{O}_K$ is the Hilbert class field.

The basic properties of the ring class field H are that any primes that ramify in H divide $f = [\mathcal{O}_K : \mathcal{O}]$, and that the Artin map induces an isomorphism

$$\mathrm{C}(\mathcal{O}) \cong I_K(f)/P_{K,\mathbb{Z}}(f) \cong \mathrm{Gal}(L/K).$$

6. Elliptic curves

We begin our discussion of complex multiplication with a brief review of elliptic curves. We draw on [Cox] and [Si] for this section, and most of the details can be found in those texts.

6.1. **Elliptic curves and isogenies.** For the rest of the paper we assume k is a field with char $k \neq 2, 3$. An elliptic curve E over k is a nonsingular algebraic curve of the form

$$\{(x, y) \in k^2 : y^2 = ax^3 + bx^2 + cx + d\},$$

with $a, b, c, d \in k$. After a change of coordinates, we may assume the curve looks like

$$y^2 = x^3 + Ax + B \tag{6.1}$$

with $A, B \in k$. There may be multiple equations that each cut out the curve E. We call an equation of the form (6.1) a Weierstrass equation for the elliptic curve E. We often look at elliptic curves projectively, as the solutions to

$$y^2 z = x^3 + Axz^2 + Bz^3 \tag{6.2}$$

in the projective plane $\mathbb{P}^2_k$. The unique point at infinity $[0 : 1 : 0]$ is known as the **origin**. The **j-invariant** of an elliptic curve is

$$j(E) = -1728\frac{4A^3}{-(4A^3 + 27B^2)} = -1728\frac{4A^3}{\Delta},$$

where Δ is the discriminant of the cubic x^3+Ax+B. The condition that the elliptic curve is nonsingular is precisely that Δ does not vanish, and so the j-invariant is always defined.

One of the basic nice properties of elliptic curves is that the points on an elliptic curve form an abelian group with $[0 : 1 : 0]$ as the zero element (see [Si], III.2). An isogeny between two elliptic curves is a nonconstant regular map that preserves the origin. Crucially, isogenies respect the group law and have finite kernel.

Proposition 6.1. *Every isogeny of elliptic curves over k is a group homomorphism.*

We define:

$$\mathrm{Hom}_k(E_1, E_2) := \{(\phi : E_1 \to E_2) : \phi \text{ is an isogeny over } k\} \cup \{\phi : E_1 \to E_2,\ p \mapsto [0 : 1 : 0]\}.$$

Note that $\mathrm{Hom}_k(E_1, E_2)$ has the structure of an abelian group. The identity element is given by the constant map to the origin. We can equip the endomorphisms of E, $\mathrm{End}_k(E) = \mathrm{Hom}_k(E, E)$, with the structure of a ring where multiplication is given by composition. Then the multiplicative identity is the identity map id_E.

An isomorphism of elliptic curves E_1, E_2 over k is a pair of k-isogenies $\phi : E_1 \to E_2, \psi : E_2 \to E_1$ satisfying $\psi \circ \phi = \mathrm{id}_{E_1}$, $\phi \circ \psi = \mathrm{id}_{E_2}$.

6.2. **Elliptic functions and lattices.** Over $\mathbb{C}$, elliptic curves become particularly well-behaved: they correspond to lattices via the Weierstrass $\wp$ function. A lattice in $\mathbb{C}$ is a two-dimensional $\mathbb{Z}$-submodule of $\mathbb{C}$, i.e. of the form $\lambda_1\mathbb{Z} + \lambda_2\mathbb{Z}$ with the appropriate nondegeneracy conditions. Maps of lattices in this setting are given by scalars:

$$\mathrm{Hom}(L_1, L_2) := \{\lambda \in \mathbb{C} : \lambda L_1 \subseteq L_2\}.$$

Two lattices L_1, L_2 are **homothetic** if there exists $\lambda \in \mathbb{C}$ such that $\lambda L_1 = L_2$. This is our notion of isomorphic lattices.

For a lattice L, the **Weierstrass $\wp$ function** is defined as

$$\wp_L(z) = \sum_{\omega \in L \setminus \{0\}} \left(\frac{1}{(z-w)^2} - \frac{1}{\omega^2} \right).$$

We write $\wp(z)$ when the choice of lattice is clear. $\wp$ is an even function with double poles at the points of L and no singularities elsewhere. The derivative

$$\wp'(z) = \frac{-2}{z^3} + \sum_{\omega \in L \setminus \{0\}} \frac{-2}{(z-\omega)^3}$$

is periodic with respect to L, i.e. $\wp'(z+\omega) = \wp'(z)$ for any $\omega \in L$. This fact implies $\wp(z)$ is constant by translates in L (see Proposition 5.5, [Ke]).

The Weierstrass $\wp$ function and its derivative satisfy a Weierstrass equation.

Proposition 6.2. *$\wp$ satisfies the following differential equation:*

$$\wp'^2 = 4\wp^3 - g_2(L)\wp - g_3(L),$$

where g_2, g_3 are the following constants dependent on the lattice:

$$g_2(L) = 60 \sum_{\omega \in L \setminus \{0\}} \frac{1}{\omega^4}, \quad g_3(L) = 140 \sum_{\omega \in L \setminus \{0\}} \frac{1}{\omega^6}.$$

Furthermore the map:

$$\begin{aligned} \mathrm{Lat}_{\mathbb{C}} &\to \mathrm{Ell}(\mathbb{C}) \\ \Lambda &\mapsto \{[\wp'(z) : \wp(z) : 1] : z \in \mathbb{C}\} \end{aligned}$$

yields an equivalence of categories between complex lattices under scaling, and elliptic curves over $\mathbb{C}$ under isogeny.

Proof. See II.1 of [Si2]. □

Corollary 6.3. *We have a natural isomorphism of rings $\mathrm{End}_{\mathbb{C}}(E) \cong \mathrm{End}(L)$ where E is the elliptic curve corresponding to L via the Weierstrass parametrization of Proposition 6.2.*

For a lattice L, we define the j-invariant of L to be:

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

where $\Delta(L) = g_2(L)^3 - 27 g_3(L)^2$ and g_2, g_3 are as defined in Proposition 6.2. It is a straightforward check to show that the j-invariant of a lattice L equals the j-invariant of the associated elliptic curve.

Proposition 6.4. *For lattices L, L' in $\mathbb{C}$, $j(L) = j(L')$ if and only if L and L' are homothetic.*

Proof. This is a relatively short computation. See Theorem 10.9 in [Cox]. □

The above and previous results imply that the set of isomorphism classes of elliptic curves over $\mathbb{C}$ is the affine line, $\mathbb{A}^1_{\mathbb{C}}$.

6.3. **Separability and reduction modulo primes.** We can view an elliptic curve E as a variety in the projective plane. It therefore makes sense to talk about $k(E)$, the field of rational functions on E. An isogeny of elliptic curves $\lambda : E_1 \to E_2$ induces a nontrivial map $\lambda^* : k(E_2) \to k(E_1)$,which makes $k(E_1)$ into an extension of $k(E_2)$. The degree of λ is defined as $[k(E_1) : k(E_2)]$.

λ is separable, inseparable, or purely inseparable if λ^* makes $k(E_1)$ into a separable, inseparable, or purely inseparable extension of $k(E_2)$, respectively. Maps of elliptic curves defined in characteristic p factor into a separable map and a q-th power Frobenius-type map.

Definition 6.5. Suppose k has finite characteristic not equal to 2 or 3. Let q be a power of char k. For E an elliptic curve defined over k, let E^q denote the elliptic curve obtained by applying the q-th power map to its Weierstrass equation. Note that we have an isogeny $E \to E^q, x \mapsto x^q$, which we call the q-Frobenius isogeny.

Proposition 6.6. *The q-Frobenius isogeny has degree q and purely inseparable.*

Proof. See Proposition II.2.11 in [Si]. □

Proposition 6.7. *Let $\varphi : E_1 \to E_2$ be an isogeny of elliptic curves that are defined in characteristic p. Then for some q, $\varphi = \mu \circ \lambda$ where $\lambda : E_1 \to E_1^q$ is the q-Frobenius isogeny and $\mu : E_1^q \to E_2$ separable.*

Proof. See Corollary II.2.12 in [Si]. □

Observe that the degree of the map φ is the product of the degrees of λ, μ. We call $\deg \lambda$ the inseparable degree of φ and $\deg \mu$ the separable degree of φ. We can characterize separable maps by their pullbacks:

Lemma 6.8. *A regular map $f : X \to Y$ of varieties is separable if and only if its pullback $f^* : \Omega Y \to \Omega Y$ is nonzero.*

In addition, we need that degree 1 isogenies are well-behaved:

Proposition 6.9. *A degree 1 isogeny $\lambda : E_1 \to E_2$ is an isomorphism.*

Proof. λ^* induces an isomorphism $k(E_1) \to k(E_2)$. Then E_1, E_2 are two birationally equivalent smooth projective curves, so they are isomorphic. That is, there is an isogeny inverse to λ. □

We will later consider elliptic curves over a number field K, and the reduction of its Weierstrass equations modulo primes of K.

Definition 6.10. Let E be an elliptic curve over F a field. Let $\mathfrak{p}$ be a prime of F. E has **good reduction** at $\mathfrak{p}$ if one of its Weierstass equations is nonsingular modulo $\mathfrak{p}$. E has **bad reduction** otherwise.

Note that a Weierstrass equation for E only picks up singularities if $\mathfrak{p}$ divides the discriminant. Therefore a given E has bad reduction at only finitely many primes. The key property of good reductions is that they preserve degrees.

Remark 6.11. *For elliptic curves E, E' with coefficients in F a number field, note that a $\mathbb{C}$ isogeny $\sigma \in \mathrm{Hom}_{\mathbb{C}}(E, E')$ has coefficients in a finite extension of F. To see this, note that σ is determined up to an automorphism of E by its kernel. But the automorphism group of E is finite, $\ker \sigma$ is finite, and E has finitely many subgroups of size n. If we take G to be the subgroup of $Aut(\mathbb{C})$ that fixes F, then*

the G-orbit of σ is finite. Hence the coefficients of σ are contained in some number field L. See [Si2]*, II.2.2 for more details.*

7. Complex Multiplication and the Class Group

The idea of complex multiplication is that certain types of elliptic curves have extra symmetry, which corresponds to their ring of endomorphisms being larger than expected. These curves can be used to gain insight into the Hilbert class fields of their endomorphism rings, and ultimately yield an analogue of Kronecker-Weber for imaginary quadratic fields.

We may view an elliptic curve defined over $\mathbb{C}$ as a lattice L. Recall that the endomorphism ring can be viewed as scalars that preserve the lattice:

$$\mathrm{End}_{\mathbb{C}}(E) \cong \{\lambda \in \mathbb{C} : \lambda L \subseteq L\} \tag{7.1}$$

Most elliptic curves have $\mathrm{End}_{\mathbb{C}}(E) = \mathbb{Z}$. If $\mathrm{End}_{\mathbb{C}}(E) \neq \mathbb{Z}$, which corresponds to the intuition of extra symmetry, then we say E has complex multiplication (CM). It turns out that the possibilities for $\mathrm{End}_{\mathbb{C}}(E)$ are quite limited.

Lemma 7.1. *Let E be an elliptic curve over $\mathbb{C}$ corresponding to a lattice L. E has CM if and only if L is homothetic to $\mathbb{Z} \oplus \omega\mathbb{Z}$ with $\mathbb{Q}(\omega)$ an imaginary quadratic field. In this case, $\mathrm{End}_{\mathbb{C}}(E)$ is isomorphic to an order $\mathcal{O}$ in $\mathbb{Q}(z)$.*

Proof. See Lemma 2.2 in [Gh]. □

In the case described by Lemma 7.1, we say E has **complex multiplication by $\mathcal{O}$**. We want that we can choose an identification of $\mathcal{O}_K$ with $\mathrm{End}_{\mathbb{C}}(E)$ that interacts nicely with the pullback on ΩE. Here ΩE is the space of differential forms on E (unfamiliar readers should see III.4 in [Si]).

Lemma 7.2. *Recall that $\alpha \in \mathcal{O}_K$ determines an endomorphism $[\alpha]$ given by commutivity of:*

$$\begin{array}{ccc} \mathbb{C}/L & \xrightarrow{x \mapsto \alpha x} & E \\ \phi \downarrow & & \downarrow \phi \\ \mathbb{C}/L & \xrightarrow{[\alpha]} & E \end{array}$$

*Then $[\,\cdot\,] : \mathcal{O}_K \to \mathrm{End}_{\mathbb{C}}(E)$ is the unique isomorphism such that for $\alpha\omega \in \Omega E$, we have $[\alpha]^*\omega = \alpha\omega$. Such a pair $(E, [\,\cdot\,])$ is called **normalized**.*

Proof. See II.1.1 in [Si2]. □

Lemma 7.3. *If E, E' have CM by $\mathcal{O}_K$, $\lambda : E \to E'$ is an isogeny, and $(E, \theta), (E', \theta')$ are normalized pairs, then for any $\alpha \in \mathcal{O}_K$, we have*

$$\lambda \circ \theta(\alpha) = \theta'(\alpha) \circ \lambda.$$

Remark 7.4. *Note that for a lattice L and corresponding elliptic curve E, $[\alpha]$ as defined in Lemma 7.2 is the map given by*

$$[\alpha] : E \to E,\ (\wp(x), \wp'(x)) \mapsto (\wp(\alpha x), \wp'(\alpha x)).$$

And so having complex multiplication by α is the same as $\wp(\alpha x)$ being a rational function of $\wp(x)$.

Note that proper fractional $\mathcal{O}$-ideals also give rise to elliptic curves with CM by $\mathcal{O}$. Any nonzero proper invertible $\mathcal{O}$-ideal is a 2-dimensional free $\mathbb{Z}$-module, and thus can be viewed as a lattice in $\mathbb{C}$. Since $\mathfrak{a}$ is closed under multiplication by $\mathcal{O}$ and proper, it follows that $\mathrm{End}_{\mathbb{C}}(\mathfrak{a}) = \mathcal{O}$. An even stronger result classifies the elliptic curves over $\mathbb{C}$ having complex multiplication:

Theorem 7.5. *Let $\mathcal{O}$ be an order of K. There is a one-to-one correspondence between isomorphism classes of elliptic curves with CM by $\mathcal{O}$ and elements of the class group $C(\mathcal{O})$ given by:*

$$\begin{aligned} \mathrm{C}(\mathcal{O}) &\to \mathcal{E}_{\mathbb{C}}(\mathcal{O}) \\ [\mathfrak{a}] &\mapsto \mathbb{C}/\mathfrak{a} \end{aligned}$$

Proof. Note that the above map is defined since $\mathfrak{a}$ because two invertible ideals differing by a nonzero principal ideal implies the two associated ideals are homothetic. Bijectivity follows from Theorem 10.14 in [Cox]. □

Corollary 7.6. *If E has CM by an order $\mathcal{O}$, then $j(E)$ is an algebraic number.*

Proof. Recall that $\alpha \in \mathbb{C}$ is algebraic if and only if $\mathrm{Aut}(\mathbb{C})\alpha$ is finite. Fix $\sigma \in \mathrm{Aut}(\mathbb{C})$. Let E^σ denote the elliptic curve with σ applied to its Weierstrass equation. Since σ is a field automorphism, $j(E)^\sigma = j(E^\sigma)$. Furthermore, $\mathrm{End}_{\mathbb{C}}(E) \cong \mathrm{End}_{\mathbb{C}}(E^\sigma)$ via:

$$\begin{aligned} \mathrm{End}_{\mathbb{C}}(E) &\to \mathrm{End}_{\mathbb{C}}(E^\sigma) \\ \phi &\mapsto \phi^\sigma, \end{aligned}$$

where ϕ^σ denotes the regular map given by ϕ with σ applied to its coefficients. Note that ϕ^σ still fixes the point at infinity. Therefore, E^σ also has CM by $\mathcal{O}$. Thus $j(E)^\sigma = j(E^\sigma)$ can take at most $|\mathrm{C}(\mathcal{O})|$ values, making $j(E)$ algebraic. □

8. The j-invariant and the ring class field

8.1. **Introduction.** The goal of this section is to prove the following:

Theorem 8.1. *Suppose E has CM by $\mathcal{O}$. Then $K(j(E))$ is the ring class field of $\mathcal{O}$.*

For the rest of this section, $\mathcal{O}$ is an order in an imaginary quadratic field K, and H will denote the ring class field of $\mathcal{O}$. We write $\mathfrak{a}_1, \ldots, \mathfrak{a}_m$ for representatives of the classes of $\mathrm{C}(\mathcal{O})$. Note that $j(\mathfrak{a}_1), \ldots, j(\mathfrak{a}_m)$ comprises all j-invariants of elliptic curves with CM by $\mathcal{O}$. For each i, let E_i denote the elliptic curve corresponding to $\mathfrak{a}_i$.

We will present an algebraic proof of Theorem 8.1 following the exposition in [Ke]. The idea is we can the relate action of $\mathrm{Gal}(\overline{K}/K)$ to the action of the class group of $\mathcal{O}$ on the j-invariants via the Artin symbol.

Knowing the two actions are compatible, we can then show $\mathrm{Gal}(\overline{K}/K)$ acts transitivity on the $\{j(\mathfrak{a}_1), \ldots, j(\mathfrak{a}_m)\}$ and so $K(j(\mathfrak{a}_1), \ldots, j(\mathfrak{a}_m))$ is Galois over K. We also use the compatibility to define an injective map

$$\mathrm{Gal}(K(j(\mathfrak{a}_1), \ldots, j(\mathfrak{a}_m))/K) \to \mathrm{C}(\mathcal{O}),$$

so up to a finite set $H, K(j(\mathfrak{a}_1), \ldots, j(\mathfrak{a}_m))$ split the same primes. Then Theorem 4.6 says $K(j(\mathfrak{a}_1), \ldots, j(\mathfrak{a}_m)) = H$, and it is quick to show $K(j(\mathfrak{a}_i))$ is at least degree $|\mathrm{Gal}(H/K)|$ over K, so $K(j(\mathfrak{a}_i)) = H$. The "compatibility" is detailed below:

Theorem 8.2. *Let $\mathcal{O}$ be an order of an imaginary quadratic field K with ring class field H. Let $\mathfrak{a}$ be a proper ideal of $\mathcal{O}$, and $\sigma \in \mathrm{Gal}(\mathbb{C}/K)$. Then*

$$j(\mathfrak{a})^\sigma = j(\mathfrak{s}^{-1}\mathfrak{a}), \tag{8.1}$$

where $\mathfrak{s}$ is any proper ideal whose Artin symbol with respect to H/K is the restriction of σ, i.e.

$$\left(\frac{L/K}{\mathfrak{s}}\right) = \sigma|_H.$$

Note that we can always find a $\sigma \in \mathrm{Gal}(\mathbb{C}/K)$ such that $\sigma|_L = ((L/K)/\mathfrak{s})$, since any automorphism of a subfield of $\mathbb{C}$ can be extended to an automorphism of $\mathbb{C}$.

Lemma 8.3. *Suppose L is some field containing $K(j(\mathfrak{a}_1), \ldots, j(\mathfrak{a}_m))$ and H. Consider the rational primes p that split as $p\mathcal{O} = \mathfrak{p}\mathfrak{p}'$. Suppose all but finitely many such primes satisfy*

$$j(\mathfrak{p}\mathfrak{a})^p \equiv j(\mathfrak{a}) \mod \mathfrak{q}, \tag{8.2}$$

for any prime $\mathfrak{q}$ of L lying over $\mathfrak{p}$. Then Theorem 8.2 holds.

Proof. We can reduce to the case where $\mathfrak{s}$ is a prime ideal $\mathfrak{p}$ by multiplicativity. For $\sigma \in \mathrm{Gal}(\mathbb{C}/K)$, Čebotarev density (see Theorem 4.5) guarantees infinitely many degree-1 primes $\mathfrak{p}$ of $\mathcal{O}$ whose Artin symbol is $\sigma|_H$. Infinitely many are unramified and satisfy

$$j(\mathfrak{p}\mathfrak{a})^\sigma \equiv j(\mathfrak{p}\mathfrak{a})^p \equiv j(\mathfrak{a}) \mod \mathfrak{q},$$

by assumption. All the $\mathfrak{p}$ have the same Artin symbol, so all the $j(\mathfrak{p}\mathfrak{a})$ are equal. Then $j(\mathfrak{p}\mathfrak{a})^\sigma - j(\mathfrak{a})$ has infinitely many prime divisors and must be zero. Then $j(\mathfrak{a})^\sigma = j(\mathfrak{p}^{-1}\mathfrak{a})$, which is what we wanted. □

In the context of Lemma 8.3, the primes $\mathfrak{p}$ we want to avoid are those where the E_i's are not defined mod $\mathfrak{p}$. When working modulo good primes, the *degree* of a map of elliptic curves is preserved after reducing, which is key to showing the Hasse congruence (8.2).

Knowing Propositions 6.7 and 6.9, if we could get an isogeny $\lambda : \widetilde{E}_1' \to \widetilde{E}_2'$ with inseparable degree p and separable degree 1 for the right curves E_1', E_2', we would have $j(E_1'^p) \equiv j(E_1')^p \equiv j(E_2')$ modulo some prime $\mathfrak{q}$, which echoes the hypothesis of 8.3.

Lemma 8.4. *There exists a chain of finite extensions $K \subseteq K' \subseteq K''$ such that*

(i) $E_1, \ldots, E_m$ are all defined over K',
(ii) every element of $Hom(E_i, E_j)$ is defined over K'',
(iii) for all but finitely many primes $\mathfrak{p}$ of K'', the E_i's have good reductions and for every prime $\mathfrak{q}$ of K'' lying over $\mathfrak{p}$ we have every K''-isogeny descends to an $\mathcal{O}_{K''}/\mathfrak{q}$-isogeny.

Proof. Chapter III, Prop 1.4(c) in [Si] says E_i is $\mathbb{C}$-isomorphic to an elliptic curve with coefficients in $K(j(\mathfrak{a}_i))$. So we may take E_i to have coefficients in $K(j(\mathfrak{a}_i))$, and all the E_i's are defined over $K(j(\mathfrak{a}_1), \ldots, j(\mathfrak{a}_m)) := K'$.

From Remark 6.11, we know that $\sigma \in \mathrm{Hom}_{\mathbb{C}}(E_i, E_j)$ has coefficients in a finite extension of K'. But $\mathrm{Hom}_{\mathbb{C}}(E_i, E_j) \cong \mathfrak{a}_j\mathfrak{a}_i^{-1}$, a 2-dimension $\mathbb{Z}$-module. So if the two generators and addition map are defined over a field, so is all of $\mathrm{Hom}_{\mathbb{C}}(E_i, E_j)$. Therefore, there exists a finite extension of K' such that all elements of $\mathrm{Hom}_{\mathbb{C}}(E_i, E_j)$

have coefficients in that field. Since there are finitely many (E_i, E_j) pairs to consider, there is some K'' finite over K' satisfying (ii).

For (iii), note that each E_i has bad reduction at finitely many primes, and that a given isogeny $\sigma \in \mathrm{Hom}_{\mathbb{C}}(E_i, E_j)$ does not descend to an element of $\mathrm{Hom}_{\mathcal{O}_{K''}/\mathfrak{q}}(\widetilde{E}_i, \widetilde{E}_j)$ for only finitely many $\mathfrak{q}$. Using once more that $\mathrm{Hom}_{\mathbb{C}}(E_i, E_j)$ is finitely generated and there are finitely many (E_i, E_j) pairs to check, part (iii) follows. □

Note that we may take K'' to be Galois and contain H for convenience.

Theorem 8.5. *There is a Galois extension L of K containing $K(j(\mathfrak{a}_1), \ldots, j(\mathfrak{a}_m))$ and H, and a finite set S of rational primes such that: if p splits as $p\mathcal{O} = \mathfrak{p}\mathfrak{p}'$ and $p \notin S$, then:*

$$j(\mathfrak{p}\mathfrak{a})^p \equiv j(\mathfrak{a}) \pmod{\mathfrak{P}}$$

for any prime $\mathfrak{P}$ lying over $\mathfrak{p}$ in L.

Proof. Let $L = K''$, where we've taken K'' to be Galois and contain H. Consider the set S' from (iii) of Lemma 8.4. Let S be the set of rational primes p such that $p = 2$, $p = 3$, or an element of S' lies over p.

Suppose p splits as $p\mathcal{O} = \mathfrak{p}\mathfrak{p}'$, and $p \notin S$.

Without loss of generality, $[\mathfrak{a}_1] = [\mathfrak{a}]$ and $[\mathfrak{a}_2] = [\mathfrak{p}\mathfrak{a}]$ in $\mathrm{C}(\mathcal{O})$. So we may write E_1 for the elliptic curve given by $\mathfrak{a}$ and E_2 for the elliptic curve given by $\mathfrak{p}\mathfrak{a}$. Note that E_1, E_2 have coefficients in L.

We get a map $\pi : E_2 \to E_1$ since $\mathfrak{p}\mathfrak{a} \subseteq \mathfrak{a}$. We calculate

$$\deg \pi = |\mathfrak{a}/\mathfrak{p}\mathfrak{a}| = N(\mathfrak{p}) = p.$$

On the other hand, by Čebotarev density (see Theorem 4.5), there are infinitely many ideals $\mathfrak{i}$ coprime to p such that $[\mathfrak{i}] = [\mathfrak{p}']$ in $\mathrm{C}(\mathcal{O})$. Fix such an $\mathfrak{i}$. Then looking at multiplication in the class group, we see $\mathfrak{i}\mathfrak{p} = \alpha\mathcal{O}$ for some $\alpha \in \mathfrak{p}$. Then multiplication by α induces a map $\times\alpha : \mathbb{C}/\mathfrak{a} \to \mathbb{C}/\mathfrak{p}\mathfrak{a}$ and hence a map $\mu : E_1 \to E_2$. The degree of μ is $N(\mathfrak{i})$ which is coprime to $\mathfrak{p}$ by construction.

We now have the following diagram. $\widetilde{\mu}, \widetilde{\pi}$ denote the reductions of μ, π mod $\mathfrak{P}$.

$$\begin{array}{ccccc}
\mathbb{C}/\mathfrak{a} & \xrightarrow{\times\alpha} & \mathbb{C}/\mathfrak{p}\mathfrak{a} & \longrightarrow & \mathbb{C}/\mathfrak{a} \\
\downarrow & & \downarrow & & \downarrow \\
E_1 & \xrightarrow{\mu} & E_2 & \xrightarrow{\pi} & E_1 \\
\downarrow & & \downarrow & & \downarrow \\
\widetilde{E_1} & \xrightarrow{\widetilde{\mu}} & \widetilde{E_2} & \xrightarrow{\widetilde{\pi}} & \widetilde{E_1}
\end{array} \tag{8.3}$$

$\pi \circ \mu$ is just multiplication by α, so after a normalized identification of $\mathrm{End}_{\mathbb{C}}(E_1)$ with $\mathcal{O}$, the pullback $(\pi \circ \mu)^*$ is multiplication by α on ΩE_1. Since $\alpha \in \mathfrak{q}$ (as $\mathfrak{P}$ lies over $\mathfrak{p}$), $(\widetilde{\pi \circ \mu})^*$ is zero and by Lemma 6.8 $\widetilde{\pi} \circ \widetilde{\mu}$ is inseparable.

Good reductions preserve degrees (see [Si2], II.§4, Proposition 4.4), so $\deg \mu = \deg \widetilde{\mu}$ is coprime to $\mathfrak{q}$ and $\widetilde{\mu}$ is separable. This forces $\widetilde{\pi}$ to be inseparable. As $\deg \widetilde{\pi} = \deg \pi = p$, λ has inseparable degree p and separable degree 1.

By Lemma 6.7, $\widetilde{\pi}$ factors into a p-Frobenius isogeny and a degree 1 separable isogeny $i : E_2^p \to E_1$, which is an isomorphism by Lemma 6.9. Taking j-invariants, we see

$$j(\widetilde{E}_1) = j(\widetilde{E}_2^p) = j(\widetilde{E}_2)^p,$$

so $j(\mathfrak{p}\mathfrak{a})^p \equiv j(\mathfrak{a}) \bmod \mathfrak{P}$. □

Proof of Theorem 8.2. Let L be a Galois extension of K containing $K(j(\mathfrak{a}_1), \ldots, j(\mathfrak{a}_m))$. Let S be the finite set described in the proof of Theorem 8.5.

For rational primes splitting as $p\mathcal{O} = \mathfrak{p}\mathfrak{p}'$ and not in S, the Hasse congruence (8.2) holds by the previous theorem. Then we have satisfied the hypothesis of Lemma 8.3 and proven Theorem 8.2. □

8.2. **Splitting behavior over $K(j(\mathfrak{a}_1), \ldots, j(\mathfrak{a}_m))$.** It follows from Theorem 8.2 that $\mathrm{Gal}(\overline{K}/K)$ acts transitively on $\{j(\mathfrak{a}_1), \ldots, j(\mathfrak{a}_m)\}$ and hence $K(j(\mathfrak{a}_1), \ldots, j(\mathfrak{a}_m))$ is Galois over K. So, we may apply results of Čebotarev density: $H = K(j(\mathfrak{a}_1), \ldots, j(\mathfrak{a}_m))$ if and only if they split the same rational primes (up to a finite set).

Theorem 8.6. $H = K(j(\mathfrak{a}_1), \ldots, j(\mathfrak{a}_m))$.

Proof. Let $H' = K(j(\mathfrak{a}_1), \ldots, j(\mathfrak{a}_m))$. The same proof as Theorem 8.2 says that

$$j(\mathfrak{a})^{((H'/K)/\mathfrak{p})} = j(\mathfrak{p}^{-1}\mathfrak{a}).$$

So we get a map

$$\Psi : \mathrm{Gal}(H'/K) \to \mathrm{C}(\mathcal{O}) \cong I(f)/P_{K,\mathbb{Z}}(f).$$
$$\left(\frac{H'/K}{\mathfrak{p}}\right) \mapsto [\mathfrak{p}^{-1}]$$

Clearly this map is surjective. Furthermore, we claim this map is injective. Suppose $\sigma \in \ker \Psi$. Then σ acts trivially on the j-invariants, which says precisely that σ is trivial in $\mathrm{Gal}(H'/K)$. Now recall that the Artin map induces an isomorphism $\mathrm{Gal}(H/K) \to \mathrm{C}(\mathcal{O})$. Then these two isomorphisms give us

$$\left(\frac{H'/K}{\mathfrak{p}}\right) = 1 \iff \left(\frac{H/K}{\mathfrak{p}}\right) = 1.$$

Suppose $\mathfrak{p}$ a prime of K is unramified in both H, H', which excludes finitely many primes. Then Corollary 3.3 says that for all but finitely many primes $\mathfrak{p}$,

$$\mathfrak{p} \text{ splits completely in } H \iff \mathfrak{p} \text{ splits completely in } H'.$$

Theorem 4.6 then implies $H = H' = K(j(\mathfrak{a}_1), \ldots, j(\mathfrak{a}_m))$. □

Proof of Theorem 8.1. By Theorem 8.6, we know $H = K(j(\mathfrak{a}_1), \ldots, j(\mathfrak{a}_m))$. Looking at the Galois group, we know

$$[H : K] = |\mathrm{C}(\mathcal{O})|.$$

But $K(j(\mathfrak{a}_i)) \subseteq H$,and we know the orbit of $j(\mathfrak{a}_i)$ under $\mathrm{Gal}(\overline{K}/K)$ is size $|\mathrm{C}(\mathcal{O})|$. Hence $K(j(\mathfrak{a}_i)) = H$. □

9. Ray class fields & an analogue of Kronecker-Weber

Class field theory for $\mathbb{Q}$ boils down to Kronecker-Weber (see 4.8), which says every finite abelian extension of $\mathbb{Q}$ is contained in $\mathbb{Q}(\zeta_m)$ for some m-th primitive root of unity ζ_m. Note that adjoining ζ_m is adjoining the m-torsion points of the multiplicative group $\mathbb{C}^\times$, which corresponds to the group scheme $\mathbb{G}_m = \operatorname{Spec} \mathbb{C}[t, t^{-1}]$.

A similar story happens in imaginary quadratic fields: consider an elliptic curve E, which is also a group scheme, with CM by $\mathcal{O}_K$. Then any abelian extension of K is contained in what is essentially H, the Hilbert class field of K, adjoined the n-torsion points of E.The problem is that extra symmetry coming from the nontrivial automorphism group of E is preventing $H(E[n])$ from being abelian over K. We will eventually resolve this by adjoining (basically) the x-coordinates of the torsion points.

For this section we follow the exposition of Ghate ([Gh]) and Lang's *Elliptic Functions* ([La2]). We begin with a discussion of ray class fields.

Definition 9.1. Observe that $I_K(\mathfrak{m})/P_{K,1}(\mathfrak{m})$. is a generalized ideal class group for the modulus $\mathfrak{m}$. Then Theorem 4.2 says there is a unique abelian extension $K(\mathfrak{m})/K$ such that the Artin map induces an isomorphism

$$\Phi_{K(\mathfrak{m})/K,\mathfrak{m}} : I_K(\mathfrak{m})/P_{K,1}(\mathfrak{m}) \to \operatorname{Gal}(K(\mathfrak{m})/K).$$

We call $K(\mathfrak{m})$ the **ray class field** for K of modulus $\mathfrak{m}$.

As the imaginary quadratic field K is usually clear, we just say "the ray class field of modulus $\mathfrak{m}$." A few properties are clear from Section 4. The conductor of $K(\mathfrak{m})$ divides $\mathfrak{m}$, and if L is another abelian extension:

$$\text{the conductor of } L \text{ divides } \mathfrak{m} \iff L \subseteq K(\mathfrak{m}). \tag{9.1}$$

By the above, it is clear that every abelian extension of K is contained in a ray class field. So to understand abelian extensions of K, it is a good start to construct the ray class fields of K.

Note that in the proof of Lemma 4.7, we showed that the Artin map induces an isomorphism $\operatorname{Gal}(\mathbb{Q}(\zeta_m)/\mathbb{Q}) \cong I_{\mathbb{Q}}(m\infty)/P_{\mathbb{Q},1}(m\infty)$. So the ray class field for $\mathbb{Q}$ of modulus $m\infty$ is indeed $\mathbb{Q}(\zeta_m)$. While this does not give all ray class fields, it is enough in that any modulus divides some $m\infty$.

In our case, we wish to show the following:

Theorem 9.2. *Let K be an imaginary quadratic field with Hilbert class field H, and let h denote the Weber function. Then $H(h(E[\mathfrak{m}]))$ is the ray class field of modulus $\mathfrak{m}$.*

Remark 9.3. *Note that $\mathfrak{m}$-torsion makes sense for E with CM by $\mathcal{O}_K$: it is the set*

$$\{p \in E : [\alpha](p) = 0 \text{ for all } \alpha \in \mathfrak{m}\}.$$

On the lattice side, let $\mathbb{C}/\mathfrak{a}$ be a model for E, with $\mathfrak{a}$ a fractional $\mathcal{O}_K$-ideal. The $\mathfrak{m}$-torsion points are $\mathfrak{m}^{-1}\mathfrak{a}/\mathfrak{a}$. See Lemma 7.2 for the definition of $[\alpha]$.

We now turn our attention to defining the Weber function. If E is an elliptic curve over $\mathbb{C}$ with CM by $\mathcal{O}_K$, then $\operatorname{Aut}(E) = \mathcal{O}_K^\times$. It is straightforward to check that

$$\mathrm{Aut}(E) = \begin{cases} \{\pm 1\} & \text{if } j(E) \neq 0, 1728 \\ \{\pm 1, \pm i\} & \text{if } j(E) = 1728 \\ \{\pm 1, \pm\omega, \pm\omega^2\} & \text{if } j(E) = 0 \end{cases},$$

where $\omega = e^{2\pi i/3}$ is a primitive third root of unity. Note that the second case corresponds to $g_3 = 0$. A representative for this isomorphism class is $y^2 = x^3 + Ax$, and the action of i can be seen by $y \mapsto iy, x \mapsto -x$. The third case corresponds to $g_2 = 0$. A representative for this class is $y^2 = x^3 + B$, and the action of ω is given by $y \mapsto y, x \mapsto \omega x$. We summarize the automorphisms on points below:

$$\mathrm{Aut}(E) = \begin{cases} (x, y) \mapsto (x, \pm y) & \text{if } j(E) \neq 0, 1728 \\ (x, y) \mapsto (x, \pm y), (-x, \pm iy) & \text{if } j(E) = 1728 \\ (x, y) \mapsto (\omega^n x, \pm y) & \text{if } j(E) = 0 \end{cases}.$$

We define the **Weber function** $h : E \to \mathbb{P}^1$ by:

$$\mathrm{Aut}(E) = \begin{cases} (g_2 g_3/\Delta) \cdot x & \text{if } j(E) \neq 0, 1728 \\ (g_2^2/\Delta) \cdot x^2 & \text{if } j(E) = 1728 \\ (g_3/\Delta) \cdot x^3 & \text{if } j(E) = 0 \end{cases}, \tag{9.2}$$

The constants ensure h is invariant under a change of variables that scales x, y. The powers of x are to help ensure points in the same orbit of $\mathrm{Aut}(E)$ have the same value.

Lemma 9.4. *Suppose E is an elliptic curve over $\mathbb{C}$. Then:*

(i) For $P, P' \in E$, we have $h(P') = h(P) \iff P' = \epsilon P$ for some $\epsilon \in \mathrm{Aut}(E)$.
(ii) If $\phi : E \to E'$ is an isomorphism of elliptic curves then $h_E = h_{E'} \circ \phi$, where h_E denotes the Weber function for E.

Proof. (i) is just a quick computation using the explicit formulas for elements of $\mathrm{Aut}(E)$ found in (9.2). (ii) uses that isomorphisms of elliptic curves have a particular form. See Lemma 7.3 in [Gh] for a full proof. □

Lemma 9.5. *Suppose E is defined over a number field L, and $\mathfrak{P}$ a prime of L at which E has good reduction. Let $\widetilde{E}$ denote the reduction of E modulo $\mathfrak{P}$. We have the natural map:*

$$\theta : \mathrm{End}_L(E) \to \mathrm{End}_L(\widetilde{E}), \phi \mapsto \widetilde{\phi}.$$

Then for any $\gamma \in \mathrm{End}_L(\widetilde{E})$ we have:

$$\gamma \in \mathrm{Im}(\theta) \iff \gamma \text{ commutes with every element of } \mathrm{Im}(\theta).$$

Proof. See [Si2], II.5.2. Using that $\mathrm{End}_L(\widetilde{E})$ has a limited number of possibilities (order in an imaginary quadratic field or quaternion algebra), this becomes a relatively short computation. □

Lemma 9.6. *Let K be an imaginary quadratic field with Hilbert class field H. Let $\mathfrak{p}$ be a degree-1 prime of K, $\mathfrak{a}$ a fixed ideal. Let $\phi : \mathbb{C}/\mathfrak{a} \to E$ be an analytic representation. Let K'' be as defined in Lemma 8.4.*

For all but finitely many such $\mathfrak{p}$, we can find an analytic representation

$$\psi : \mathbb{C}/\mathfrak{p}^{-1}\mathfrak{a} \to E^{\sigma},$$

and isogeny λ such that the following commutes:

$$\begin{array}{ccc} \mathbb{C}/\mathfrak{a} & \xrightarrow{\pi} & \mathbb{C}/\mathfrak{p}^{-1}\mathfrak{a} \\ \downarrow{\scriptstyle \phi} & & \downarrow{\scriptstyle \psi} \\ E & \xrightarrow{\lambda} & E^{\sigma} \end{array} \tag{9.3}$$

with $\widetilde{\lambda} = \mathrm{Frob}_p$, the degree-$p$ Frobenius map. Here the tilde denotes the reduction modulo $\mathfrak{q}$ a prime of K'' lying over $\mathfrak{p}$ and π is the canonical projection, using that $\mathfrak{p}^{-1}\mathfrak{a} \supseteq \mathfrak{a}$.

Proof. Note that $\sigma = ((H/K), \mathfrak{p})$, so $\widetilde{E^{\sigma}} = \widetilde{E}^p$. Here we use that E, E^{σ} have coefficients in H. Similar to the proof of Theorem 8.5, we have a commutative diagram

$$\begin{array}{ccc} \mathbb{C}/\mathfrak{a} & \xrightarrow{\pi} & \mathbb{C}/\mathfrak{p}^{-1}\mathfrak{a} \\ \downarrow{\scriptstyle \phi} & & \downarrow{\scriptstyle \psi'} \\ E & \xrightarrow{\lambda} & E^{\sigma} \end{array}$$

where λ is an isogeny that is purely separable of degree p that factors as $\widetilde{\lambda} = \widetilde{\epsilon} \circ \mathrm{Frob}_p$, where $\widetilde{\epsilon}$ is an automorphism of $\widetilde{E}^p$. We claim that $\widetilde{\epsilon}$ is the reduction of an element of $\mathrm{Aut}_{K''}(E^{\sigma})$. Let θ denote the natural map $\mathrm{End}_{K''}(E^{\sigma}) \to \mathrm{End}_{\mathcal{O}_{K''}/\mathfrak{q}}(\widetilde{E^{\sigma}})$. It is enough to show that $\widetilde{\epsilon}$ commutes with every element of Im θ by Lemma 9.5. We are crucially using that good reductions preserve degrees of isogenies (see [Si2], II.§4, Proposition 4.4) to get that the lift of $\widetilde{\epsilon}$ is also an automorphism.

If (E, θ) is normalized and hence $(E^{\sigma}, \theta^{\sigma})$ is normalized, we have $\lambda \circ \theta(\gamma) = \theta(\gamma)^{\sigma} \circ \lambda$ by Lemma 7.3. Reducing and substituting, we have:

$$\widetilde{\epsilon} \circ \mathrm{Frob}_p \circ \widetilde{\theta(\gamma)} = \widetilde{\theta(\gamma)^{\sigma}} \circ \widetilde{\epsilon} \circ \mathrm{Frob}_p. \tag{9.4}$$

On the other hand, since $\mathfrak{p}$ has norm p, we get

$$\widetilde{\theta(\gamma)^{\sigma}} = \left(\widetilde{\theta(\gamma)}\right)^p,$$

and so:

$$\widetilde{\epsilon} \circ \mathrm{Frob}_p \circ \widetilde{\theta(\gamma)} = \widetilde{\epsilon} \circ \widetilde{\theta(\gamma)^{\sigma}} \circ \mathrm{Frob}_p. \tag{9.5}$$

Comparing the right-hand sides of (9.4), 9.5 and composing by the right power of Frob_p, we get that

$$\widetilde{\epsilon} \circ \widetilde{\theta(\gamma)^{\sigma}} = \widetilde{\theta(\gamma)^{\sigma}} \circ \widetilde{\epsilon}. \tag{9.6}$$

Hence there exists an ϵ a lift of $\widetilde{\epsilon}$. Multiplying λ by ϵ^{-1} on the left, which changes ψ' by an automorphism to ψ, we get commutivity of Diagram (9.3) and that $\widetilde{\lambda} = \mathrm{Frob}_p$. □

Lemma 9.7. *$K(j(E), h(E[\mathfrak{m}]))$ is Galois over K.*

Proof. Let $\sigma \in \mathrm{Gal}(\overline{K}/K)$. Note that $E^\sigma = E^{\sigma|_H}$. Note that the map (not isogeny) $E \to E^\sigma, (x,y) \to (x^\sigma, y^\sigma)$ sends $\mathfrak{m}$-torsion points of E to $\mathfrak{m}$-torsion points of E^σ. We wish to understand this map better.

Let $\sigma|_H = ((H/K)/\mathfrak{s})$. The projection maps $\mathbb{C}/\mathfrak{a} \to \mathbb{C}/\mathfrak{s}^{-1}\mathfrak{a}$ yield various isogenies $\phi_\mathfrak{s} : E \to E^\sigma$ of degree $N(\mathfrak{s})$. If $N(\mathfrak{s})$ and $\mathfrak{m}$ are coprime (and we can always find such $\mathfrak{s}$ by Theorem 4.5) then

$$\phi_\mathfrak{s} : E[\mathfrak{m}] \xrightarrow{\cong} E^\sigma[\mathfrak{m}].$$

This isomorphism is not canonical. But each isomorphism differs by an element of $\mathcal{O}_K^\times$, acting on $E[\mathfrak{m}]$ or $E^\sigma[\mathfrak{m}]$. Hence we get a canonical isomorphism

$$E[\mathfrak{m}]/\mathcal{O}_K^\times \cong E^\sigma[\mathfrak{m}]/\mathcal{O}_K^\times.$$

Therefore, an element of $\mathrm{Gal}(\overline{H}/H)$ fixes $H(E[\mathfrak{m}]/\mathcal{O}_K^\times)$ if and only if it fixes $H(E^\sigma[\mathfrak{m}]/\mathcal{O}_K^\times)$. Thus $H(E[\mathfrak{m}]/\mathcal{O}_K^\times) = K(j(E), E[\mathfrak{m}]/\mathcal{O}_K^\times)$ does not depend on the choice of E, and hence is Galois over K.

Since h has coefficients in H which is Galois over K, $K(j(E), h(E[\mathfrak{m}]))$ is Galois over K. □

Proof of Theorem 9.2. Lemma 9.7 tells us that $K(j(E), h(E[\mathfrak{m}]))$ is Galois, so we may apply results of Čebotarev density. By part (iii) of Corollary 3.3 it is enough to show

$$\mathfrak{p} \text{ splits completely in } K(j(E), h(E[\mathfrak{m}])) \iff \mathfrak{p} = (\alpha) \text{ with } \alpha \in \mathcal{O}_K \text{ and } \alpha \equiv 1 \bmod \mathfrak{m}$$

holds, since an unramified prime splits in the ray class field of modulus $\mathfrak{m}$ if and only if the righthand side is true. We may proceed assuming $\mathfrak{p}$ is unramified in both the ray class field and $K(j(E), h(E[\mathfrak{m}]))$, as this excludes finitely many primes.

Consider the diagram of Lemma 9.6. For $q \in E[\mathfrak{m}]$, we have:

$$\widetilde{\lambda(q)} = \widetilde{\lambda}\widetilde{q} = \mathrm{Frob}_p(\widetilde{q}) = \widetilde{\sigma(q)},$$

where reduction is modulo $\mathfrak{q} \subseteq L'$ lying over $\mathfrak{p}$, as in the Lemma.

Say $N(\mathfrak{p}) = p^m$. For $\mathfrak{p}$ with p coprime to the modulus, which is all but finitely many such $\mathfrak{p}$, reduction modulo $\mathfrak{q} \subseteq L'$ is an injection on $E[\mathfrak{m}]$. Hence we may take $\lambda = \sigma$ on $E[\mathfrak{m}]$, and the diagram becomes:

$$\begin{array}{ccc} (K/\mathfrak{a})_\mathfrak{m} & \xrightarrow{\pi} & (K/\mathfrak{p}^{-1}\mathfrak{a})_\mathfrak{m} \\ \Big\downarrow{\scriptstyle \phi} & & \Big\downarrow{\scriptstyle \psi} \\ E[\mathfrak{m}] & \xrightarrow{\sigma} & E^\sigma[\mathfrak{m}] \end{array} \tag{9.7}$$

The idea is that by making certain compositions the identity map on $E[\mathfrak{m}]$, we can force a multiplicative factor α to be be equivalent to 1 mod $\mathfrak{m}$ for one direction of the proof, and force σ to permute $\mathcal{O}_K^\times$ orbits for the other direction (thereby acting trivially after taking $h(P)$).

Now suppose a prime $\mathfrak{p}$ of K is of the form $\mathfrak{p} = (\alpha)$ with $\alpha \in \mathcal{O}_K, \alpha \equiv 1 \bmod \mathfrak{m}$. Then $\mathfrak{p}$ splits completely in $K(j(E))$, and thus $E = E^\sigma$. Then we get analytic representations ϕ', a such that the following commutes:

$$\begin{array}{ccccc} (K/\mathfrak{a})_{\mathfrak{m}} & \xrightarrow{\pi} & (K/\mathfrak{p}^{-1}\mathfrak{a})_{\mathfrak{m}} & \xrightarrow{\times\alpha} & (K/\mathfrak{a})_{\mathfrak{m}} \\ \downarrow{\scriptstyle\phi} & & \downarrow{\scriptstyle\psi} & & \downarrow{\scriptstyle\phi'} \\ E[\mathfrak{m}] & \xrightarrow{\sigma} & E^{\sigma}[\mathfrak{m}] & \xrightarrow{a} & E[\mathfrak{m}] \end{array} \tag{9.8}$$

Note that ϕ, ϕ' differ by an automorphism of E. But if $\alpha \equiv 1 \bmod \mathfrak{m}$, then $\sigma \circ a$ is the identity map. Therefore, σ must act trivially on the $h(q)$ for all q for the diagram to commute. But then any prime of $K(j(E), h(E[\mathfrak{m}]))$ above $\mathfrak{p}$ has inertial degree 1, so $\mathfrak{p}$ splits completely in $K(j(E), h(E[\mathfrak{m}]))$.

Conversely, suppose $\mathfrak{p}$ splits completely in $K(j(E), h(E[\mathfrak{m}]))$. Consequently, $\mathfrak{p}$ splits in $K(j(E)$, so $\mathfrak{p} = \alpha$ is principal and $E^{\sigma} = E$. We obtain Diagram (9.8) once more, with $a = \mathrm{id}$. Since the Weber function is defined over $K(j(E)$, $\sigma(h) = h$. Pick $u \in (K/\mathfrak{a})_{\mathfrak{m}}$. We calculate:

$$\begin{aligned} h(\phi(u)) &= h^{\sigma}(\phi(u)^{\sigma}) \\ &= h(\phi(u)^{\sigma}) \\ \text{(by (9.8))} \qquad &= h(\phi'(\alpha u)) \\ (\phi, \phi' \text{ differ by an aut.}) \qquad &= h(\phi(\alpha u)) \end{aligned}$$

$(k/\mathfrak{a})_{\mathfrak{m}} \cong \mathfrak{m}^{-1}\mathcal{O}_K/\mathcal{O}_K \cong \mathcal{O}_K/\mathfrak{m}\mathcal{O}_K$ is generated by a single element over $\mathcal{O}_K$. Pick a generator u_0. Then the classification of $\mathbb{C}$-automorphisms of E tells us

$$\alpha u_0 = \zeta u_0,$$

for some root of unity ζ contained in $\mathcal{O}_K$. Changing the generator α of $\mathfrak{p}$ to $\zeta^{-1}\alpha$. Then:

$$\alpha u_0 = u_0.$$

Hence $\alpha u = u$ for all $u \in (K/\mathfrak{a})_{\mathfrak{m}}$. This holds only if $\alpha \equiv 1 \bmod \mathfrak{m}$. So we've shown that for all but finitely many primes of $\mathfrak{p}$:

$$\mathfrak{p} \text{ splits completely in } K(j(E), h(E[\mathfrak{m}])) \iff \mathfrak{p} = (\alpha) \text{ with } \alpha \in \mathcal{O}_K \text{ and } \alpha \equiv 1 \bmod \mathfrak{m},$$

thus for all but finitely many primes, $\mathfrak{p}$ splits in $(K/\mathfrak{a})_{\mathfrak{m}}$ if and only if it splits in the ray class field. Therefore (by Theorem 4.6) $K(j(E), E[\mathfrak{m}]) = K(\mathfrak{m})$, the ray class field of modulus $\mathfrak{m}$. □

Corollary 9.8. *Let K be an imaginary quadratic extension. Let E_{tors} be the set of torsion points on E. The maximal abelian extension of K is $K^{ab} = K(j(E), h(E_{\mathrm{tors}}))$, where E is an elliptic curve over $\mathbb{C}$ with CM by $\mathcal{O}_K$.*

10. Acknowledgements

I would like to thank my mentors, Keerthi Madapusi Pera and Minh-Tam Trinh, for their help and guidance throughout the program. Many thanks to Jesse Wolfson for insightful chats on connections between algebraic geometry and algebraic topology, and the lecturers for giving such great and interesting talks, especially the number theory lecturers (Frank Calegari, Keerthi Madapusi Pera) and dynamics

lecturers (Aaron Brown, Kathryn Lindsey, Howard Masur). Lastly, I would like to thank Peter May for organizing the REU.

Appendix A. Adeles and ideles

The goal for this appendix is to reformulate class field theory for number fields in terms of **ideles**. By considering all primes at once, we do not require moduli to state the results, and all our isomorphisms come from a single map. A more thorough discussion of the idelic formulation can be found in V.5 of [Mi] and IV.2 of [Neu], with the latter explaining the correspondence between idelic and ideal-theoretic formulations.

We begin by defining:

$$\widehat{\mathbb{Z}} = \prod_{\mathfrak{p}} \mathbb{Z}_p,$$

where $\mathbb{Z}_p$ denotes the completion of $\mathbb{Z}$ at the finite prime p. We then define the **finite adeles** by allowing multiplication by a fixed denominator in all coordinates:

$$\begin{aligned}\mathbb{A}_f &= \widehat{\mathbb{Z}}\left[\tfrac{1}{n} : n \in \mathbb{Z}\right] \\ &= \{(a_p) : a_p \in \mathbb{Q}_p, \text{ with } a_p \in \mathbb{Z}_p \text{ for all but finitely many } a_p\}\end{aligned}$$

We then have $\mathbb{A}_\infty = \mathbb{R}$, the completion of $\mathbb{Q}$ at the "infinite prime," i.e. with respect to the Euclidean metric. The ring of adeles of $\mathbb{Q}$ is given by:

$$\mathbb{A}_{\mathbb{Q}} := \mathbb{A}_f \times \mathbb{A}_\infty.$$

Now consider a number field F. We obtain the adeles of F by taking the adele ring of $\mathbb{Q}$ and tensoring with F. Observe that

$$\mathbb{Z}_p \otimes \mathcal{O}_F = \prod_{\mathfrak{p}|p} \mathcal{O}_{F,\mathfrak{p}},$$

where $\mathcal{O}_{F,\mathfrak{p}}$ denotes the completion of $\mathcal{O}_F$ at $\mathfrak{p}$. Note that $\widehat{\mathbb{Z}} \otimes F$ contains $\widehat{\mathbb{Z}} \otimes \mathcal{O}_F$, and it is clear that the **finite adeles of** F have the following presentation:

$$\begin{aligned}\mathbb{A}_{f,F} &:= \mathbb{A}_f \otimes F \\ &= \{(a_\mathfrak{p}) : a_\mathfrak{p} \in F_\mathfrak{p} \text{ with } a_\mathfrak{p} \in \mathcal{O}_{F,\mathfrak{p}} \text{ for all but finitely many } \mathfrak{p}\}\end{aligned}$$

We then define the **ring of adeles of** F as:

$$\mathbb{A}_F := F \otimes \mathbb{A}_{\mathbb{Q}} \tag{A.1}$$

$$= \mathbb{A}_{f,F} \times (\mathbb{R} \otimes F). \tag{A.2}$$

We wish to understand $(\mathbb{R} \otimes F)$ better. Consider the example $F = \mathbb{Q}[x]/(x^3 - 2)$. Then:

$$\begin{aligned}F = \frac{\mathbb{Q}[x]}{(x^3-2)} \otimes \mathbb{R} = \frac{\mathbb{R}[x]}{(x^3-2)} &= \frac{\mathbb{R}[x]}{(x - \sqrt[3]{2})} \times \frac{\mathbb{R}[x]}{(x - \omega\sqrt[3]{2})((x - \omega^2\sqrt[3]{2})} \\ &= \mathbb{R} \times \mathbb{C}\end{aligned}$$

Note that the factors above correspond to F having one real embedding and a pair of complex conjugate embeddings. Hence we can describe:

$$\mathbb{A}_F := \mathbb{A}_{f,F} \times (\mathbb{R}^{r_1} \times \mathbb{C}^{r_2}), \tag{A.3}$$

where r_1 is the number of real embeddings of F and r_2 is one half times the number of complex embeddings. That is r_1, r_2 count the number of infinite primes. An element of $\mathbb{A}_F$ is called an adele, and is written $(a_\mathfrak{p})$, where $\mathfrak{p}$ is now understood to range over all primes, infinite or finite, of F.

We use $\mathbb{A}_F^\times$ to denote the group of ideles, which are the elements of $\mathbb{A}_F$ that are invertible in $\mathbb{A}_F$. Note $(a_\mathfrak{p}) \in \mathbb{A}_F^\times$ if and only if $a_\mathfrak{p} \in \mathcal{O}_{F,\mathfrak{p}}^\times$ for all but finitely many $\mathfrak{p}$.

Now, note that $F^\times$ embeds into $\mathbb{A}_F^\times$, via $\alpha \mapsto (a_\mathfrak{p})$ where $a_\mathfrak{p} = \alpha$ for all $\mathfrak{p}$. Note that this is well defined, since α is a unit in $\mathcal{O}_{F,\mathfrak{p}}$ for all but finitely many $\mathfrak{p}$ (because $v_\mathfrak{p}(\alpha) = 0$ for all but finitely many primes).

Definition A.1. The **idele class group** of F is defined as:

$$\mathbb{C}(F) = \mathbb{A}_F^\times / F^\times.$$

Class field theory stated idelically is a correspondence between abelian extensions of a number field F and certain "norm subgroups" of $\mathbb{C}(F)$. One can put a topology on $\mathbb{A}_F^\times$ coming from these "norm groups" around the identity, leading to a topology of $\mathbb{C}(F)$. It turns out that these norm subgroups are essentially the open subgroups of finite index in $\mathbb{C}(F)$.

Let F be a field and L a finite extension. Pick $\alpha \in L$. Let $\sigma_1(\alpha), \ldots, \sigma_n(\alpha)$ be the roots (with multiplicity) of the minimal polynomial of α in K. The field norm of L/F is:

$$\mathrm{N}_{L/F}(\alpha) = \prod_{i=1}^{n} \sigma_j(\alpha)^{[L:K(\alpha)]}. \tag{A.4}$$

This is the determinant of the F-linear map $m_\alpha : L \to L, x \mapsto \alpha x$, and hence is an element of F. For L Galois over F, we have:

$$\mathrm{N}_{L/F}(\alpha) = \prod_{\sigma \in \mathrm{Gal}(L/F)} g(\alpha). \tag{A.5}$$

Furthermore there is a canonical isomorphism

$$L \otimes_F F_\mathfrak{p} \cong \prod_{\mathfrak{P}|\mathfrak{p}} L_\mathfrak{P},$$

and it follows that

$$\mathrm{N}_{L/K}(\alpha) = \prod_{\mathfrak{P}|\mathfrak{p}} \mathrm{N}_{L_\mathfrak{P}/F_\mathfrak{p}}(\alpha). \tag{A.6}$$

Definition A.2. Let L be a finite extension of F. For an idele $(a_\mathfrak{p}) \in \mathbb{A}_L^\times$, we define:

$$\begin{aligned} \mathrm{N}_{L/K} : \mathbb{A}_L^\times &\to \mathbb{A}_F^\times \\ (a_\mathfrak{P}) &\mapsto (b_\mathfrak{p}), \end{aligned}$$

where $b_\mathfrak{p} = \prod_{\mathfrak{P}|\mathfrak{p}} \mathrm{N}_{L_\mathfrak{P}/F_\mathfrak{p}}(a_\mathfrak{P})$.

From (A.6) we have commutivity of the following diagram:

$$\begin{array}{ccc} L^\times & \longrightarrow & \mathbb{A}_L^\times \\ \Big\downarrow{\scriptstyle \mathrm{N}_{L/F}} & & \Big\downarrow{\scriptstyle \mathrm{N}_{L/F}} \\ F^\times & \longrightarrow & \mathbb{A}_F^\times \end{array}$$

Consider $\mathbb{C}(F)$. $\mathbb{A}_F^\times$ has the structure of a topological group, where the topology is generated by $\mathrm{N}_{L/F}(\mathbb{A}_L^\times)$, where L runs over the finite Galois extensions of F. Notice that $\mathrm{N}_{L/F}$ sends $L^\times$ to $K^\times$, so it descends to a map

$$\mathrm{N}_{L/F} : \mathbb{C}(L) \to \mathbb{C}(F).$$

Similarly, we can put a norm topology on $\mathbb{C}(F)$, generated by $\mathrm{N}_{L/F}(\mathbb{C}(L))$ for all finite Galois extensions L. Note that this equals the quotient topology from $\mathbb{A}_F^\times$.

We also have a topology on $\mathbb{A}_F^\times$ coming from the valuation on $F_\mathfrak{p}^\times$. We give a basis:

$$\prod_\mathfrak{p} U_\mathfrak{p},$$

where $U_\mathfrak{p}$ is open in $K_\mathfrak{p}^\times$ for all $\mathfrak{p}$, and $U_\mathfrak{p} = \mathcal{O}_{F,\mathfrak{p}}^\times$ for all but finitely many $\mathfrak{p}$. This induces a quotient topology on $\mathbb{C}(F)$. We call this the natural topology on $\mathbb{A}_F^\times$ or $\mathbb{C}(F)$, respectively.

Proposition A.3. *The open subgroups of finite index in $\mathbb{C}(F)$ are the same for both the norm topology and the natural topology.*

Proof. See IV.7.1 in [Neu2]. □

Appendix B. Idelic formulation of class field theory

We can now state some of the results of Section 4 in terms of ideles. Let F be a number field, and L a finite abelian extension. Using local class field theory, one can define a map $(\cdot, L/F) : \mathbb{A}_F^\times \to \mathrm{Gal}(L/F)$, and all these maps are really coming from the "restriction" of a map $\phi : \mathbb{A}_F^\times \to \mathrm{Gal}(F^{\mathrm{ab}}/F)$. This map $(\cdot, L/F)$ has a few defining properties, which are roughly

(i) $(u, L/F) = 1$ for every $u = (u_\mathfrak{p})$ satisfying
- $u_\mathfrak{p}$ is a unit in $\mathcal{O}_{F,\mathfrak{p}}$ for $\mathfrak{p}$ unramified in L,
- $u_\mathfrak{p}$ is sufficiently close to 1 for $\mathfrak{p}$ ramified
- $u_\mathfrak{p} > 0$ for real infinite primes that ramify in L.

(ii) For $\mathfrak{p}$ unramified in L, $a = (a_{\mathfrak{p}'})$ maps to the Frobenius element $((L/F), \mathfrak{p})$ in $\mathrm{Gal}(L/F)$ where

$$a_{\mathfrak{p}'} = \begin{cases} \pi & \mathfrak{p}' = \mathfrak{p} \\ 1 & \text{else} \end{cases},$$

and π is a prime element of $\mathcal{O}_{F,\mathfrak{p}}$.

See Summary 5.10 in Chapter V of [Mi] for more. The above lets us detect ramification behavior with the map $(\cdot, L/F) : \mathbb{A}_F^\times \to \mathrm{Gal}(L/F)$ as we would want to, knowing the ideal-theoretic formulation.

Theorem B.1 (Artin Reciprocity)**.** *For every finite abelian extension of a number field F, $(\cdot, L/F)$ is surjective and descends to an isomorphism*

$$(\cdot, L/F) : \mathbb{A}_F^\times/(F^\times \cdot \mathrm{N}_{L/F}(\mathbb{A}_L^\times)) \xrightarrow{\cong} \mathrm{Gal}(L/F). \tag{B.1}$$

The above can also be thought of as an isomorphism $\mathbb{C}(F)/\mathrm{N}_{L/F}(\mathbb{C}(L)) \to \mathrm{Gal}(L/K)$, noting that the norm makes sense on $\mathbb{C}(L)$. Since the $(\cdot, L/F)$'s all come from a map ϕ, one can show the following commutative diagram for $F \subseteq F' \subseteq L$:

$$\begin{array}{ccccc}
F'^\times \cdot \mathrm{N}_{L/F'}(\mathbb{A}_L^\times) & \longrightarrow & \mathbb{A}_{F'}^\times & \xrightarrow{(\cdot, L/F')} & \mathrm{Gal}(L/F') \\
\Big\downarrow{\scriptstyle \mathrm{N}_{F'/F}} & & \Big\downarrow{\scriptstyle \mathrm{N}_{F'/F}} & & \Big\downarrow{\scriptstyle i} \\
F^\times \cdot \mathrm{N}_{L/F}(\mathbb{A}_L^\times) & \longrightarrow & \mathbb{A}_F^\times & \xrightarrow{(\cdot, L/F)} & \mathrm{Gal}(L/F)
\end{array}$$

Theorem B.2 (Existence Theorem)**.** *For every open subgroup N of $\mathbb{C}(F)$, there exists a unique abelian extension L of F such that $\mathrm{N}_{L/F}(\mathbb{C}(L)) = N$.*

Corollary B.3. *The assignment $L \mapsto \mathrm{N}_{L/F}(\mathbb{C}(L))$ is a bijection between finite abelian extensions of K to the set of open subgroups of $\mathbb{C}(K)$. Furthermore, for L_1, L_2 finite abelian extensions of F:*

$$L_1 \subseteq L_2 \iff \mathrm{N}_{L_1/F}(\mathbb{C}(L_1)) \supseteq \mathrm{N}_{L_2/F}(\mathbb{C}(L_2))$$

and

$$\begin{aligned}
\mathrm{N}_{L_1 \cdot L_2/F}(\mathbb{C}(L_1 \cdot L_2)) &= \mathrm{N}_{L_1/F}(\mathbb{C}(L_1)) \cap \mathrm{N}_{L_2/F}(\mathbb{C}(L_2)) \\
\mathrm{N}_{L_1 \cap L_2/F}(\mathbb{C}(L_1 \cap L_2)) &= \mathrm{N}_{L_1/F}(\mathbb{C}(L_1)) \cdot \mathrm{N}_{L_2/F}(\mathbb{C}(L_2)).
\end{aligned}$$

Proof. See II.4.2 in [Neu2]. □

Hence continuous finite quotients of the idele class group $\mathbb{C}(F)$ correspond to finite abelian extensions of F. Lastly, we explicity outline the translation between idelic and ideal-theoretic class field theory. The full details can be found in IV.8 of [Neu2]. Let $\mathfrak{m}$ be a modulus. Define $U(\mathfrak{m})$ to be the set of ideles $(a_\mathfrak{p})$ satsfying

(1) $a_\mathfrak{p} \equiv 1 \bmod \mathfrak{p}^{\nu_\mathfrak{p}(\mathfrak{m})}$ for finite primes $\mathfrak{p}$,
(2) $\sigma(a_\mathfrak{p}) > 0$ for real infinite $\mathfrak{p}|\mathfrak{m}$.

Note the similarity to the definition of $P_{F,1}(\mathfrak{m})$. We use $\mathbb{C}_F(\mathfrak{m})$ to denote its image $U(\mathfrak{m}) \cdot F^\times/F^\times$ in $\mathbb{C}(F)$.

Proposition B.4. *We have a surjective homomorphism:*

$$\begin{aligned}
\kappa : \mathbb{A}_F^\times &\to I_K(\mathfrak{m}) \\
(a_\mathfrak{p}) &\mapsto \prod_{\mathfrak{p} \text{ finite}} \mathfrak{p}^{\nu_\mathfrak{p}(a_\mathfrak{p})}
\end{aligned}$$

that descends to an isomorphism:

$$\kappa_\mathfrak{m} : (\mathbb{A}_F^\times/F^\times)/U(\mathfrak{m}) = \mathbb{C}(F)/\mathbb{C}_F(\mathfrak{m}) \to I_F(\mathfrak{m})/P_{F,1}(\mathfrak{m}).$$

Proof. See IV.8.1 in [Neu2]. □

Theorem B.5. *Let L/F be an abelian extension, $\mathfrak{m}$ a modulus for L. Let H be the kernel of the Artin map $((L/F)/\cdot)$. Then we have an exact commutative diagram:*

$$\begin{array}{ccccccccc} 1 & \longrightarrow & \mathrm{N}_{L/F}(\mathbb{C}_L) & \longrightarrow & \mathbb{C}(F) & \xrightarrow{((L/F)/\cdot)} & \mathrm{Gal}(L/F) & \longrightarrow & 1 \\ & & \downarrow{\scriptstyle \kappa_{\mathfrak{m}}} & & \downarrow{\scriptstyle \kappa_{\mathfrak{m}}} & & \downarrow{\scriptstyle i} & & \\ 1 & \longrightarrow & H/P_{F,1}(\mathfrak{m}) & \longrightarrow & I_F(\mathfrak{m})/P_{F,1}(\mathfrak{m}) & \xrightarrow{(\cdot, L/F)} & \mathrm{Gal}(L/F) & \longrightarrow & 1 \end{array}$$

Proof. See IV.8.2 in [Neu2]. □

References

[AM] M. Atiyah, I. MacDonald, *Introduction to Commutative Algebra*, Addison-Wesley Publishing Company, Reading, Masachusetts, 1969.

[BoSh] Z. Borevich, I. Shafarevich, *Number Theory*, Academic Press, New York, 1966.

[Cox] D. Cox, *Primes of the Form $x^2 + ny^2$*, John Wiley & Sons, New York, 1989.

[Gh] E. Ghate, *Complex Multipliction,* from Winter School on Elliptic Curves, HRI. 2001. http://www.math.tifr.res.in/~eghate/cm.pdf

[Ja] G. Janusz, *Algebraic Number Fields*, Academic Press, New York, 1973.

[Ke] K. Kedlaya, *Complex Multiplication and Explicit Class Field Theory*, April 1, 1996. http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.49.3926

[La] S. Lang, *Algebraic Number Theory* 2nd edition. Springer-Verlag, New York. 1994.

[La2] S. Lang, *Elliptic Functions* 2nd edition. Springer-Verlag, New York. 1987.

[Li] C. Li, *Complex multiplication and singular moduli*, March 23, 2013. http://www.math.harvard.edu/~chaoli/doc/MinorThesis3.html

[Mi] J. S. Milne, *Class Field Theory*, v4.02. March 2013. http://www.jmilne.org/math/CourseNotes/cft.html

[Neu] J. Neukirch, *Algebraic Number Theory*, Springer-Verlag, New York, 1999.

[Neu2] J. Neukirch, *Class Field Thepry*, Springer-Verlag, New York, 1986.

[Sa] P. Samuel, *Algebraic Theory of Numbers*, Hermann, Paris. 1970.

[Si] J. Silverman, *The Arithmetic of Elliptic Curves*, Springer-Verlag, New York, 2009.

[Si2] J. Silverman, *Advanced Topics in the Arithmetic of Elliptic Curves*, Springer-Verlag, New York, 1994.

E-mail address: gwynm@umich.edu

Department of Mathematics, University of Michigan, Ann Arbor, MI 48109