Complex Multiplication and Kronecker's Jugendtraum

Introduction

The Kronecker-Weber theorem states that every finite abelian extension of $\mathbb{Q}$ is contained in a cyclotomic extension $\mathbb{Q}(\zeta_n)$. *Kronecker's Jugendtraum* (the "dearest dream of [Kronecker]'s youth') asks the same question for any number field, and though the general problem is still open, the case for K an imaginary quadratic extension of $\mathbb{Q}$ is solved through the theory of elliptic curves with complex multiplication.

This essay will build up the basic theory of elliptic curves with complex multiplication, and explain how to generate the maximal abelian extension of an imaginary quadratic field from the value of the j-invariant and Weber functions related to elliptic curves. We will go via the *main theorem of complex multiplication*, which relates homomorphisms of torsion points on the curve with Galois actions on the elliptic curve. In the course of this, we will also see the statements of the main theorems of class field theory.

1 Elliptic curves over $\mathbb{C}$ with complex multiplication

Though we eventually want to study elliptic curves over number fields, we will first look at elliptic curves over $\mathbb{C}$ with complex multiplication. Over $\mathbb{C}$, elliptic curves can be converted into complex tori, where the description of isogenies and endomorphisms is very simple.

1.1 Complex tori

A complex torus is the Riemann surface obtained by quotienting $\mathbb{C}$ by a lattice $\Lambda \subseteq \mathbb{C}$. The surface obtained has genus 1, and has an additive structure, much like an elliptic curve. Indeed, we can find an elliptic curve that is complex analytic isomorphic to $\mathbb{C}/\Lambda$:

Definition 1.1. Given a complex torus $\mathbb{C}/\Lambda$, we obtain an elliptic curve

$$E_\Lambda : y^2 = 4x^3 - g_2(\Lambda)x - g_3(\Lambda)$$

and a complex analytic isomorphism of Riemann surfaces given by

$$f : \mathbb{C}/\Lambda \to E_\Lambda$$

$$[z] \mapsto (\wp(z), \wp'(z)).$$

Addition in $\mathbb{C}/\Lambda$ corresponds to the group law on E_Λ:

$$f([z]) + f([z']) = f([z] + [z']).$$

As it turns out, every elliptic curve is isomorphic to a complex torus. This result is known as the *uniformisation theorem* (see [4]).

Theorem 1.2 (Uniformisation theorem)**.** *Every elliptic curve over $\mathbb{C}$ is isomorphic to some E_Λ, where Λ is a lattice in $\mathbb{C}$.*

Because of this, we only need to study complex tori to learn about elliptic curves over $\mathbb{C}$.

Next, we quote the following:

Theorem 1.3.

- *A map $E \to E'$ between elliptic curves over $\mathbb{C}$ is an isogeny iff it is a complex analytic map sending 0 to 0.*
- *Every isogeny $\phi : E_\Lambda \to E_{\Lambda'}$ is obtained from a linear map φ of the form*

$$\varphi : \mathbb{C}/\Lambda \to \mathbb{C}/\Lambda'$$

$$z + \Lambda \mapsto \lambda z + \Lambda'$$

with $\lambda\Lambda \subseteq \Lambda'$.

Proof. See [4]. □

Note that

$$\ker \varphi \cong \frac{\Lambda'}{\lambda\Lambda}.$$

So the maps ϕ, φ will be isomorphisms iff $\Lambda' = \lambda\Lambda$.

Definition 1.4. Let $\vartheta_\lambda : \mathbb{C}/\Lambda \to \mathbb{C}/\lambda\Lambda$ be the map

$$z + \Lambda \mapsto \lambda z + \lambda\Lambda.$$

Then every isomorphism of complex tori is of the form ϑ_λ for some $\lambda \in \mathbb{C}^\times$.

Corollary 1.5. *E_Λ, $E_{\Lambda'}$ are isomorphic iff the lattices Λ, Λ' are homothetic, i.e. $\Lambda' = \lambda\Lambda$ for some $\lambda \in \mathbb{C}^\times$.*

Theorem 1.3 lets us easily describe the set of homomorphisms between two elliptic curves in terms of the lattices. Moreover, since the group law on the elliptic curve corresponds to addition on the complex torus, the group structure of the homomorphisms is also preserved.

Corollary 1.6. *Let $\Lambda, \Lambda' \subseteq \mathbb{C}$ be lattices.*

i)

$$\mathrm{Hom}(E_\Lambda, E_{\Lambda'}) \cong \{\alpha \in \mathbb{C} \mid \alpha\Lambda \subseteq \Lambda'\}$$

as groups.

ii)

$$\mathrm{End}(E_\Lambda) \cong \{\alpha \in \mathbb{C} \mid \alpha\Lambda \subseteq \Lambda\}$$

as rings.

1.2 Classifying elliptic curves with complex multiplication

We begin by determining what endomorphism rings are possible for an elliptic curve E_Λ. To describe them, we need to introduce a new definition.

Definition 1.7. Let K be a finite extension of $\mathbb{Q}$. A subring $R \subseteq K$ is an *order* of K if it is a finitely generated $\mathbb{Z}$-module and $R \otimes_{\mathbb{Z}} \mathbb{Q} = K$.

As it turns out, the only possible endomorphism rings are $\mathbb{Z}$ or an order of an imaginary quadratic extension of $\mathbb{Q}$. More specifically, we have:

Proposition 1.8. *Let $\Lambda = \mathbb{Z}\omega_1 \oplus \mathbb{Z}\omega_2$ be a lattice. If there is an imaginary quadratic extension $K/\mathbb{Q}$ containing ω_2/ω_1, then E_Λ has complex multiplication by an order of K. Otherwise, E_Λ does not have complex multiplication.*

Proof. Let $R = \{\alpha \in \mathbb{C} \mid \alpha\Lambda \subseteq \Lambda\} \cong \mathrm{End}(E_\Lambda)$. This is a subring of $\mathbb{C}$, so it's closed under addition and contains $\mathbb{Z}$. Indeed, one can easily see that $R \cap \mathbb{Q} = \mathbb{Z}$.

If $\alpha \in R$, then $\alpha\omega_1 \in \Lambda$. This tells us that

$$R \subseteq \omega_1^{-1}\Lambda = \mathbb{Z} \oplus \mathbb{Z}\omega_2/\omega_1.$$

So R is a $\mathbb{Z}$-submodule of a free $\mathbb{Z}$-module of rank 2, hence R is a free $\mathbb{Z}$-module of rank ≤ 2.

Moreover, we know that $R \cap \mathbb{Q} = \mathbb{Z}$, so either $R = \mathbb{Z}$ or $R = \mathbb{Z} \oplus \mathbb{Z}\alpha$ for some $\alpha = a\omega_2/\omega_1 + b$ with $a, b \in \mathbb{Z}, a \neq 0$.

Suppose R is strictly greater than $\mathbb{Z}$. Then it contains some $\alpha \notin \mathbb{Z}$. We get

$$R = \mathbb{Z} \oplus \mathbb{Z}\alpha \subseteq \mathbb{Z}[\alpha] \subseteq R,$$

so $\mathbb{Z}[\alpha] = \mathbb{Z} \oplus \mathbb{Z}\alpha$ has rank 2. Hence $\mathbb{Q}[\alpha] = \mathbb{Z}[\alpha] \otimes_{\mathbb{Z}} \mathbb{Q}$ is a 2-dimensional $\mathbb{Q}$-vector space, which tells us that $\mathbb{Q}(\alpha)/\mathbb{Q}$ is a degree 2 extension. But $\alpha = a\omega_2/\omega_2 + b$, so $\mathbb{Q}(\omega_2/\omega_1) = \mathbb{Q}(\alpha)$, and so ω_2/ω_1 is contained in a quadratic extension $K/\mathbb{Q}$. This extension must be imaginary because $\omega_2/\omega_1 \notin \mathbb{R}$.

Conversely, suppose that ω_2/ω_1 is contained in K, an imaginary quadratic extension of $\mathbb{Q}$. Note $\omega_2/\omega_1 \notin \mathbb{Q}$, so we have

$$\mathbb{Q} \oplus \mathbb{Q}\omega_2/\omega_1 = K = \mathbb{Q}(\omega_2/\omega_1).$$

Hence we can write

$$(\omega_2/\omega_1)^2 = \frac{a}{b}\omega_2/\omega_1 + \frac{c}{d}$$

for some $a, b, c, d \in \mathbb{Z}, b, d \neq 0$.

Then $bd(\omega_2/\omega_1)\omega_2 \in \mathbb{Z}\omega_1 \oplus \mathbb{Z}\omega_2$, so $bd(\omega_2/\omega_1) \in R$. This is an element of R not in $\mathbb{R}$, so R must have rank 2. Then $R \otimes_{\mathbb{Z}} \mathbb{Q}$ is a 2-dimensional $\mathbb{Q}$-vector subspace of K, so it equals K.

Therefore R is an order of K. □

If we look at the case where R is the maximal order, the ring of integers $\mathcal{O}_K$, then there is a particularly simple description of the lattice Λ.

Proposition 1.9. *E_Λ has complex multiplication by $\mathcal{O}_K$ iff Λ is homothetic to a fractional ideal of K.*

Proof. By Corollary 1.6, we have a ring homomorphism between the endomorphisms of E_Λ and the set $\{\alpha \in \mathbb{C} \mid \alpha\Lambda \subseteq \Lambda\}$.

By Proposition 1.8, if E_Λ has complex multiplication by $\mathcal{O}_K$, then Λ must be of the form $\mathbb{Z}\omega_1 + \mathbb{Z}\omega_2$ with $\omega_1/\omega_2 \in K$. We can find some integer $n > 0$ such that $n\omega_1/\omega_2 = \beta \in \mathcal{O}_K$. Then Λ is homothetic to the lattice $S = n\mathbb{Z} + \beta\mathbb{Z} \subseteq \mathcal{O}_K$.

Since E_Λ has complex multiplication by $\mathcal{O}_K$, we must have $\alpha S \subseteq S$ for all $\alpha \in \mathcal{O}_K$. This tells us that S is in fact an ideal of $\mathcal{O}_K$. So Λ is homothetic to a fractional ideal of K.

Conversely, if Λ is homothetic to a fractional ideal of K, the set $S = \{\alpha \in \mathbb{C} \mid \alpha\Lambda \subseteq \Lambda\}$ does not change under homothety, so we may assume WLOG that Λ is an ideal $\mathfrak{a} \triangleleft \mathcal{O}_K$.

S is clearly contained in K. Also, a theorem of number fields tells us that

$$\{\alpha \in K \mid \alpha\mathfrak{a} \subseteq \mathfrak{a}\} = \mathcal{O}_K,$$

so we can conclude that $\mathrm{End}(E_\Lambda) \cong S = \mathcal{O}_K$. □

Remark. For an order R of K, one can still prove by a similar argument that if E_Λ has complex multiplication by R, then Λ is homothetic to an ideal of R. However, the converse is not true - if I is an ideal of R, the elliptic curve E_I may have endomorphism ring strictly larger than R.

The set of all fractional ideals up to homothety should be very familiar, as it is just the ideal class group $\mathcal{Cl}(\mathcal{O}_K)$.

Corollary 1.10. *The set*

$$\mathcal{ELL}(\mathcal{O}_K) = \frac{\{\textit{elliptic curves over } \mathbb{C} \textit{ with complex multiplication by } \mathcal{O}_K\}}{\textit{isomorphism}}$$

is in one-to-one correspondence with $\mathcal{Cl}(\mathcal{O}_K)$, via

$$\mathcal{Cl}(\mathcal{O}_K) \to \mathcal{ELL}(\mathcal{O}_K)$$

$$\bar{\mathfrak{a}} \mapsto [E_\mathfrak{a}].$$

In particular, $\mathcal{ELL}(\mathcal{O}_K) = h_k$, the class number of K.

Proof. For well-definedness and injectivity, note that

$$\begin{aligned} E_\mathfrak{a} \cong E_{\mathfrak{a}'} &\iff \exists \lambda \in \mathbb{C}^\times \ \mathfrak{a}' = \lambda\mathfrak{a} \\ &\iff \mathfrak{a}, \mathfrak{a}' \text{ are in the same ideal class} \end{aligned}$$

Then Proposition 1.9 tells us that the above map is surjective. □

1.3 Multiplication by elements of $\mathcal{O}_K$

Let E be an elliptic curve over $\mathbb{C}$ with complex multiplication by $\mathcal{O}_K$. By uniformisation theorem, there exists a lattice $\Lambda \subseteq \mathbb{C}$ and a complex analytic isomorphism $f : \mathbb{C}/\Lambda \to E_\Lambda$.

Then, by Corollary 1.6, we have a bijection

$$[\cdot] : \mathcal{O}_K \to \mathrm{End}(E),$$

specified by

$$f^{-1}[\alpha]f : z + \Lambda \mapsto \alpha z + \Lambda.$$

Note that this map $[\cdot]_E$ extends the standard map $[\cdot] : \mathbb{Z} \to \mathrm{End}(E)$ representing multiplication by n.

To show this is independent of our choice of isomorphism, note the following property: $[\alpha]_E \in \mathrm{End}(E)$ is the unique endomorphism such that

$$[\alpha]_E^* \omega = \alpha\omega$$

for any invariant differential ω of E.

The map $[\cdot]_E$ makes E into an $\mathcal{O}_K$-module, via

$$\alpha \cdot P = [\alpha]_E(P).$$

Proposition 1.11. *Let $\phi : E \to E'$ be an isogeny between elliptic curves with complex multiplication by $\mathcal{O}_K$. Then, for all $\alpha \in \mathcal{O}_K$*

$$[\alpha]_{E'} \circ \phi = \phi \circ [\alpha]_E.$$

In other words, ϕ is an $\mathcal{O}_K$-module homomorphism.

Proof. Let ω be an invariant differential of E. Then $\phi^*\omega$ is an invariant differential of E', so

$$\begin{aligned} [\alpha]_{E'}^* \phi^* \omega &= \alpha \phi^* \omega \\ &= \phi^*(\alpha\omega) \\ &= \phi^* [\alpha]_E^* \omega. \end{aligned}$$

We're working in characteristic 0, so we can conclude from this $[\alpha]_{E'}\phi = \phi[\alpha]_E$. □

We will want to keep track of the kernels of the maps $[\alpha]_E$.

Definition 1.12. Let M be an $\mathcal{O}_K$-module (e.g. a curve E with complex multiplication by $\mathcal{O}_K$).

- Let $\alpha \in \mathcal{O}_K$. The *α-torsion* of M is
$$M[\alpha] = \{x \in M \mid \alpha \cdot x = 0\}.$$
- Let $\mathfrak{c} \lhd \mathcal{O}_K$. The *$\mathfrak{c}$-torsion* of M is
$$M[\mathfrak{c}] = \{x \in M \mid \alpha \cdot x = 0 \ \forall \alpha \in \mathfrak{c}\}.$$

1.4 Isogenies — Multiplication by ideals

Earlier, we looked at maps from a complex torus to itself: we fixed the lattice and changed the multiplier λ. Now, we fix the multiplier λ to be 1 and change the lattice.

Lemma 1.13. *Let $\mathbb{C}/\Lambda$ have complex multiplication by $\mathcal{O}_K$, and let $\mathfrak{a}$ be a fractional ideal of K. Then $\mathbb{C}/\mathfrak{a}\Lambda$ also has complex multiplication by $\mathcal{O}_K$.*

Proof. Proposition 1.9 tells us that there exists $\lambda \in \mathbb{C}^\times$ such that $\Lambda = \lambda\mathfrak{a}'$, where $\mathfrak{a}'$ is a fractional ideal of K. Then

$$\mathfrak{a}\Lambda = \lambda\mathfrak{a}\mathfrak{a}'$$

and $\mathfrak{a}\mathfrak{a}'$ is a fractional ideal. So $\mathfrak{a}\Lambda$ is homothetic to a fractional ideal, and so $\mathbb{C}/\mathfrak{a}\Lambda$ has complex multiplication by $\mathcal{O}_K$. □

This allows us to define an action of fractional ideals on complex tori:

Definition 1.14. Define an action of fractional ideals on complex tori by

$$\mathfrak{a} * \mathbb{C}/\Lambda = \mathbb{C}/\mathfrak{a}^{-1}\Lambda.$$

Next, note that if $\mathfrak{c}$ is an integral ideal, then we have $\mathcal{O}_K \subseteq \mathfrak{c}^{-1}$. So $\Lambda = \mathcal{O}_K\Lambda \subseteq \mathfrak{c}^{-1}\Lambda$ and so we get a natural map of complex tori

Definition 1.15. Given an ideal $\mathfrak{c}$ of $\mathcal{O}_K$ and a complex torux $\mathbb{C}/\Lambda$ with complex multiplication by $\mathcal{O}_K$, define

$$\varphi_{\mathfrak{c}} : \mathbb{C}/\Lambda \to \mathfrak{c} * \mathbb{C}/\Lambda$$
$$z + \Lambda \mapsto z + \mathfrak{c}^{-1}\Lambda.$$

Proposition 1.16. *The kernel of $\varphi_{\mathfrak{c}}$ is the $\mathfrak{c}$-torsion, i.e.*

$$\ker \varphi_{\mathfrak{c}} = (\mathbb{C}/\Lambda)[\mathfrak{c}].$$

Proof. Let $\Lambda' = \{x \in \mathbb{C} \mid x + \Lambda \in (\mathbb{C}/\Lambda)[\mathfrak{c}]\}$, so that $(\mathbb{C}/\Lambda)[\mathfrak{c}] = \Lambda'/\Lambda$. We wish to show that $\Lambda' = \mathfrak{c}^{-1}\Lambda$.

From the definition of $(\mathbb{C}/\Lambda)[\mathfrak{c}]$, we have that Λ' is the largest subset of $\mathbb{C}$ such that $\mathfrak{c}\Lambda' \subseteq \Lambda$.

We have $\mathfrak{c}(\mathfrak{c}^{-1}\Lambda) = \Lambda$, so $\mathfrak{c}^{-1}\Lambda \subseteq \Lambda'$.

Also, note that

$$\Lambda' \subseteq \mathcal{O}_K\Lambda' = \mathfrak{c}^{-1}(\mathfrak{c}\Lambda') \subseteq \mathfrak{c}^{-1}\Lambda.$$

So we have $\Lambda' = \mathfrak{c}^{-1}\Lambda$, and so we're done. □

Also note that φ respects the group law:

$$\varphi_{\mathfrak{c}'\mathfrak{c}} = \varphi_{\mathfrak{c}'}\varphi_{\mathfrak{c}}.$$

(This is technically an abuse of notation since $\varphi_{\mathfrak{c}'}$ is a map from $\mathfrak{c} * \mathbb{C}/\Lambda$.)

If $\mathfrak{c}$ is a principal ideal, say $\mathfrak{c} = (\alpha)$, then $\mathfrak{c}\Lambda = \alpha\Lambda$, so the complex tori $\mathfrak{c} * \mathbb{C}/\Lambda, \mathbb{C}/\Lambda$ are isomorphic via the map $\vartheta_\alpha : z \mapsto \alpha z$. Composing this with $\varphi_{\mathfrak{c}}$ then gives the endomorphism $E_\Lambda \to E_\Lambda$ given by $z \mapsto \alpha z$, which is $[\alpha]$.

2 Working over a number field

Our next step is to switch from working over $\mathbb{C}$ to working over a number field L. This will allow us to reduce modulo a prime ideal, which will prove important in finding isogenies later. However, we also need to make sure that everything we want to use, the elliptic curves and the isogenies between them, are defined over the number field L we work in.

2.1 Galois actions on elliptic curves

Suppose we have some elliptic curves and isogenies defined over a field L.

Let $\sigma \in \mathrm{Aut}(L)$ be a field automorphism. We can conjugate various things with with σ:

Elliptic curves Take an elliptic curve E defined over a field L. Suppose E has Weierstrass equation

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6.$$

We can conjugate E by σ to obtain the elliptic curve E^σ, defined by the equation

$$y^2 + a_1^\sigma xy + a_3^\sigma y = x^3 + a_2^\sigma x^2 + a_4^\sigma x + a_6^\sigma.$$

The associated quantites such as $b_2, \ldots, b_8, c_4, c_6, \Delta, \omega, j$ are all rational functions in the a_i with integer coefficients, so they are also conjugated by σ. In particular, we have

$$j(E^\sigma) = j(E)^\sigma.$$

Points on elliptic curves We can also conjugate points as well: there is a function

$$E \to E^\sigma$$

$$(x : y : z) \mapsto (x^\sigma : y^\sigma : z^\sigma).$$

However, this function is not a morphism, since the coordinates are not rational functions.

Isogenies between elliptic curves Finally, we can conjugate an isogeny $\phi : E \to E'$ by σ to obtain an isogeny $\phi^\sigma : E^\sigma \to E'^\sigma$. This gives a bijection

$$\mathrm{Hom}(E, E') \to \mathrm{Hom}(E^\sigma, E'^\sigma)$$

that respects composition. In particular, σ induces a ring isomorphism

$$\sigma : \mathrm{End}(E) \to \mathrm{End}(E^\sigma).$$

Note that if E has complex multiplication by $\mathcal{O}_K$, then both sides are canonically isomorphic to $\mathcal{O}_K$ via $[\cdot]$. What is the ring isomorphism σ in terms of $\mathcal{O}_K$?

Lemma 2.1. *Let E be an elliptic curve defined over a field $L \subseteq \mathbb{C}$ with complex multiplication by $\mathcal{O}_K$. Then the isomorphism $\sigma : \mathrm{End}(E) \to \mathrm{End}(E^\sigma)$ is given by*

$$([\alpha]_E)^\sigma = [\alpha^\sigma]_{E^\sigma}.$$

Proof. On the invariant differential ω^σ of E^σ, we have

$$\begin{aligned}([\alpha]_E^\sigma)^*\omega^\sigma &= ([\alpha]_E^*\omega)^\sigma \\ &= (\alpha\omega)^\sigma \\ &= \alpha^\sigma\omega^\sigma \\ &= [\alpha^\sigma]_{E^\sigma}^*\omega^\sigma\end{aligned}$$

Hence $[\alpha]_E^\sigma = [\alpha^\sigma]_{E^\sigma}$. □

So if σ fixes K, then σ gives an isomorphism of $\mathcal{O}_K$-modules $E \to E^\sigma$.

Lemma 2.2. *Let E be an elliptic curve over $\mathbb{C}$ with complex multiplication by $\mathcal{O}_K$. Then the j-invariant of E is algebraic.*

Proof. Corollary 1.10 tells us that $|\mathcal{ELL}(\mathcal{O}_K)| = h_K$. Therefore, the set

$$J = \{j(E) : E \text{ has complex multiplication by } \mathcal{O}_K\}$$

also has size h_K.

Let $\sigma \in \mathrm{Aut}(\mathbb{C})$. Then $\mathrm{End}(E^\sigma) \cong \mathrm{End}(E) \cong \mathcal{O}_K$, so

$$j(E)^\sigma = j(E^\sigma) \in J.$$

Thus $j(E)$ has at most h_K different Galois conjugates, which implies that $j(E)$ is algebraic over $\mathbb{Q}$ of degree at most h_K. □

2.2 Picking our favourite elliptic curves in $\mathcal{ELL}(\mathcal{O}_K)$

Given a complex torus $\mathbb{C}/\mathfrak{a}$, we obtain an elliptic curve

$$E_\mathfrak{a} : y^2 = 4x^3 - g_2(\mathfrak{a})x - g_3(\mathfrak{a}).$$

However, the coefficients $g_2(\mathfrak{a}), g_3(\mathfrak{a})$ might not be algebraic, so this elliptic curve is not defined over a number field. Another problem we have to bear in mind is that two elliptic curves defined over a field L can be isomorphic over $\mathbb{C}$ but not over L.

To deal with this, we construct a particular elliptic curve that is isomorphic to $E_\mathfrak{a}$ but with coefficients in some number field L, which we will use throughout the rest of this essay.

Lemma 2.3. *Given an elliptic curve E defined over $\mathbb{C}$ with j-invariant $j = j(E)$, the curve*

$$\mathrm{Ell}_j : \begin{cases} y^2 = x^3 - \frac{3j}{j-1728}x + \frac{2j}{j-1728} & j \neq 0, 1728 \\ y^2 = x^3 + 1 & j = 0 \\ y^2 = x^3 + x & j = 1728 \end{cases}$$

is an elliptic curve defined over $\mathbb{Q}(j)$ that is isomorphic to E over $\mathbb{C}$.

Proof. It's clear that Ell_j is defined over $\mathbb{Q}(j)$.

A calculation shows that the above equations give smooth curves and have j-invariant equal to j, so E, Ell_j are isomorphic over $\mathbb{C}$. □

Remark Note that Ell_j behaves nicely under Galois conjugation: we have

$$(\mathrm{Ell}_j)^\sigma = \mathrm{Ell}_{j^\sigma}$$

for all $\sigma \in \mathrm{Aut}(\mathbb{C})$.

We use this formula to define representatives for $\mathcal{ELL}(\mathcal{O}_K)$.

Definition 2.4. Suppose $\mathfrak{a}$ is a fractional ideal of K.

Define $E_{\bar{\mathfrak{a}}}$ to be the elliptic curve $\mathrm{Ell}_{j(E_\mathfrak{a})}$, which is defined over $\mathbb{Q}(j(E_\mathfrak{a}))$, a number field. Note that $j(E_\mathfrak{a})$ depends only on $\bar{\mathfrak{a}}$ the ideal class of $\mathfrak{a}$, so $E_{\bar{\mathfrak{a}}}$ depends only on $\bar{\mathfrak{a}}$.

In all cases, we have $j(E_{\bar{\mathfrak{a}}}) = j(E_\mathfrak{a})$, so $E_{\bar{\mathfrak{a}}}$ is isomorphic to $E_\mathfrak{a}$ over $\mathbb{C}$. So, for each $\mathfrak{a}$, we also define

$$f_\mathfrak{a} : \mathbb{C}/\mathfrak{a} \to E_{\bar{\mathfrak{a}}}$$

a complex analytic isomorphism.

Definition 2.5. Define the set

$$\mathrm{Ell}(\mathcal{O}_K) = \{E_{\bar{\mathfrak{a}}} : \bar{\mathfrak{a}} \in \mathcal{Cl}(\mathcal{O}_K)\}$$

This is a set of representatives for $\mathcal{ELL}(\mathcal{O}_K)$.

As discussed before, a Galois conjugate of an elliptic curve with complex multiplication by $\mathcal{O}_K$ also has complex multiplication by $\mathcal{O}_K$. This, combined with the fact that all curves in $\mathrm{Ell}(\mathcal{O}_K)$ are of the form given in Lemma 2.3, implies that for all $\sigma \in \mathrm{Aut}(\mathbb{C})$ and all $E \in \mathrm{Ell}(\mathcal{O}_K)$ we have $E^\sigma \in \mathrm{Ell}(\mathcal{O}_K)$ — the set $\mathrm{Ell}(\mathcal{O}_K)$ is closed under Galois conjugation.

Recall we had an action of fractional ideals on elliptic curves E_Λ with complex multiplication by $\mathcal{O}_K$. When we move to using representatives of each isomorphism class, this descends to an action of ideal classes:

Definition 2.6. Define an action of $\mathcal{Cl}(\mathcal{O}_K)$ on $\mathrm{Ell}(\mathcal{O}_K)$ by

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

We can also define the isogenies $\phi_\mathfrak{c} : E_{\bar{\mathfrak{a}}} \to \bar{\mathfrak{c}} * E_{\bar{\mathfrak{a}}}$ corresponding to the maps $\varphi_\mathfrak{c} : \mathbb{C}/\mathfrak{a} \to \mathbb{C}/\mathfrak{c}^{-1}\mathfrak{a}$.

Definition 2.7. Let $\mathfrak{a}$ be a fractional ideal of K and let $\mathfrak{c}$ be an ideal of $\mathcal{O}_K$. Then $\phi_\mathfrak{c} : E_{\bar{\mathfrak{a}}} \to \bar{\mathfrak{c}} * E_{\bar{\mathfrak{a}}}$ is the isogeny

$$\phi_\mathfrak{c} = f_{\mathfrak{c}^{-1}\mathfrak{a}} \circ \varphi_\mathfrak{c} \circ f_\mathfrak{a}^{-1},$$

i.e. the isogeny making the following diagram commute:

$$\begin{array}{ccc} \mathbb{C} & \xrightarrow[\sim]{\times 1} & \mathbb{C} \\ \downarrow & & \downarrow \\ \mathbb{C}/\mathfrak{a} & \xrightarrow{\varphi_\mathfrak{c}} & \mathbb{C}/\mathfrak{c}^{-1}\mathfrak{a} \\ \downarrow{\scriptstyle f_\mathfrak{a}} & & \downarrow{\scriptstyle f_{\mathfrak{c}^{-1}\mathfrak{a}}} \\ E_{\bar{\mathfrak{a}}} & \xrightarrow{\phi_\mathfrak{c}} & \bar{\mathfrak{c}} * E_{\bar{\mathfrak{a}}} \end{array}$$

Lemma 2.8.

$$\deg \phi_{\mathfrak{c}} = \mathrm{Nm}(\mathfrak{c}).$$

Proof. It suffices to show that $\ker \phi_{\mathfrak{c}}$ has size $\mathrm{Nm}(\mathfrak{c}) = |\mathcal{O}_K/\mathfrak{c}|$. We have $\ker \phi_{\mathfrak{c}} = f_{\mathfrak{a}}(\ker \varphi_{\mathfrak{c}})$, and $f_{\mathfrak{a}}$ is an isomorphism, so $\ker \phi_{\mathfrak{c}}$ and $\ker \varphi_{\mathfrak{c}}$ have the same size.

Next, $\ker \varphi_{\mathfrak{c}} = \mathfrak{c}^{-1}\Lambda/\Lambda$, so it suffices to prove

$$|\mathfrak{c}^{-1}\Lambda/\Lambda| = |\mathcal{O}_K/\mathfrak{c}|.$$

We will later see in Section 5 that $\mathfrak{c}^{-1}\Lambda/\Lambda$ and $\mathcal{O}_K/\mathfrak{c}$ are isomorphic as $\mathcal{O}_K$-modules, which implies the above fact. □

2.3 A field of definition for isogenies

We've seen that our representatives $E_{\bar{\mathfrak{a}}}$ are defined over suitable number fields. We now want to extend the number field so that the isogenies between these elliptic curves are also defined.

First, we look at isogenies from $E_{\bar{\mathfrak{a}}}$ to itself, i.e. we study the endomorphism ring $\mathrm{End}(E_{\bar{\mathfrak{a}}})$.

Lemma 2.9. *Let E be an elliptic curve defined over a field $L \subseteq \mathbb{C}$ with complex multiplication by $\mathcal{O}_K$. Then every endomorphism of E is defined over the field LK.*

Proof. Take an endomorphism of E. It will be $[\alpha]_E$ for some $\alpha \in \mathcal{O}_K$.

Let σ be an automorphism of $\mathbb{C}$ fixing LK. σ fixes L, so $E = E^\sigma$. So we have

$$\begin{aligned} [\alpha]_E^\sigma &= [\alpha^\sigma]_E \\ &= [\alpha]_E && \text{because } \sigma \text{ fixes } K \end{aligned}$$

This tells us $[\alpha]_E$ is fixed by all $\sigma \in \mathrm{Aut}(\mathbb{C})$ fixing LK. Therefore $[\alpha]_E$ is defined over LK. □

This tells us that every endomorphism of $E_{\bar{\mathfrak{a}}}$ is defined over the number field $K(j(E_{\mathfrak{a}}))$.

Next, we look at isogenies between the elliptic curves $E_{\bar{\mathfrak{a}}}$ for different $\bar{\mathfrak{a}} \in \mathcal{Cl}(\mathcal{O}_K)$.

Lemma 2.10. *Let L be a number field such that $E_{\bar{\mathfrak{a}}}, E_{\bar{\mathfrak{a}}'}$ are defined over L. Let $\phi : E_{\bar{\mathfrak{a}}} \to E_{\bar{\mathfrak{a}}'}$ be an isogeny. Then ϕ is defined over a finite extension of L.*

Proof. Let $\sigma \in \mathrm{Aut}(\mathbb{C})$ be an automorphism fixing L. Then σ fixes $E_{\bar{\mathfrak{a}}}, E_{\bar{\mathfrak{a}}'}$, so ϕ^σ is also an isogeny $E_{\bar{\mathfrak{a}}} \to E_{\bar{\mathfrak{a}}'}$, i.e.

$$\phi^\sigma \in \mathrm{Hom}(E_{\bar{\mathfrak{a}}}, E_{\bar{\mathfrak{a}}'}).$$

Also, $\deg \phi^\sigma = \deg \phi$.

But now note that $\mathrm{Hom}(E_{\bar{\mathfrak{a}}}, E_{\bar{\mathfrak{a}}'})$ is a free $\mathbb{Z}$-module of finite rank, and deg is a positive definite quadratic form on $\mathrm{Hom}(E_{\bar{\mathfrak{a}}}, E_{\bar{\mathfrak{a}}'})$. So there are only finitely many isogenies of a given degree.

Therefore ϕ has only finitely images under conjugation by the automorphisms of $\mathbb{C}$ fixing L. So ϕ is defined over a finite extension of L. □

Proposition 2.11. *There exists a finite extension $L/K \subseteq \mathbb{C}$ such that every elliptic curve $E_{\bar{\mathfrak{a}}}$ and every isogeny $E_{\bar{\mathfrak{a}}} \to E_{\bar{\mathfrak{a}}'}$ is defined over L.*

Proof. There are only finitely many $E_{\bar{\mathfrak{a}}}$. So we only need to extend L a finite number of times to ensure that every $E_{\bar{\mathfrak{a}}}$ is defined over L.

Also, for every pair $\bar{\mathfrak{a}}, \bar{\mathfrak{a}}'$, the $\mathbb{Z}$-module $\mathrm{Hom}(E_{\bar{\mathfrak{a}}}, E_{\bar{\mathfrak{a}}'})$ is finitely generated (by Corollary 1.6), and there are only finitely many of these pairs. So we only need to extend L a finite number of times to have generators for every $\mathrm{Hom}(E_{\bar{\mathfrak{a}}}, E_{\bar{\mathfrak{a}}'})$ be defined over L. This then implies that every isogeny in every $\mathrm{Hom}(E_{\bar{\mathfrak{a}}}, E_{\bar{\mathfrak{a}}'})$ is defined over L. □

This gives us a suitable number field to work in for the next section.

3 Reduction modulo $\mathfrak{P}$

Let L/K be an extension of number fields. We will use the following notation:

- $\mathfrak{P}$ is a prime ideal of L.
- $\mathfrak{p}$ is a the prime ideal of K that $\mathfrak{P}$ lies over.
- $k_{\mathfrak{P}}, k_{\mathfrak{p}}$ are the residue fields $\mathcal{O}_L/\mathfrak{P}, \mathcal{O}_K/\mathfrak{p}$ respectively.
- p is the prime of $\mathbb{Q}$ that $\mathfrak{P}, \mathfrak{p}$ lie over, i.e. $p = \operatorname{char} k_{\mathfrak{p}} = \operatorname{char} k_{\mathfrak{P}}$.
- $L_{\mathfrak{P}}, K_{\mathfrak{p}}$ are the completions of L, K with respect to the valuations $v_{\mathfrak{P}}, v_{\mathfrak{p}}$.
- $\mathcal{O}_{\mathfrak{P}}, \mathcal{O}_{\mathfrak{p}}$ are the rings of integers of $L_{\mathfrak{P}}, K_{\mathfrak{p}}$.

In this section, we move between working over a number field L and working over the finite field $k_{\mathfrak{P}}$. We look at reducing elliptic curves and isogenies modulo a prime ideal $\mathfrak{P}$, as well as lifting isogenies between curves modulo $\mathfrak{P}$ back up to isogenies between the original curves.

The most important advantage of working over a finite field is that Galois actions can have a geometric meaning as well: the Frobenius element of $\operatorname{Aut}(k_{\mathfrak{P}})$ has a polynomial formula $x \mapsto x^p$, so conjugating by the Frobenius element is an isogeny. When we lift this isogeny back up to L, the isogeny we get will then have a close relationship with the lift of the Frobenius element up to $\operatorname{Aut}(L)$.

3.1 The Frobenius element for an unramified prime

Let L be a Galois extension of K. Let $\mathfrak{p}$ be an unramified prime of K, and $\mathfrak{P}$ a prime of L lying over $\mathfrak{p}$. Then the Galois extension L/K gives rise to a Galois extension of local fields $L_{\mathfrak{P}}/K_{\mathfrak{p}}$, and the Galois groups are related by restriction:

$$\operatorname{Gal}(L_{\mathfrak{P}}/K_{\mathfrak{p}}) \hookrightarrow \operatorname{Gal}(L/K).$$

The image of $\operatorname{Gal}(L_{\mathfrak{P}}/K_{\mathfrak{p}})$ in $\operatorname{Gal}(L/K)$ is the *decomposition group*.

Consider an automorphism $\sigma \in \operatorname{Gal}(L_{\mathfrak{P}}/K_{\mathfrak{p}})$. σ sends $\mathcal{O}_{\mathfrak{P}}$, the integral closure of $\mathcal{O}_{\mathfrak{p}}$ in $L_{\mathfrak{P}}$, to itself, and it sends $\mathfrak{P}\mathcal{O}_{\mathfrak{P}}$ the maximal ideal of $\mathcal{O}_{\mathfrak{P}}$ to itself too. Therefore, σ descends to a field automorphism of $\operatorname{Gal}(k_{\mathfrak{P}}/k_{\mathfrak{p}})$.

This therefore defines a natural group homomorphism

$$\operatorname{Gal}(L_{\mathfrak{P}}/K_{\mathfrak{p}}) \to \operatorname{Gal}(k_{\mathfrak{P}}/k_{\mathfrak{p}}).$$

Since $\mathfrak{p}$ is an unramified prime, the corresponding extension of local fields $L_{\mathfrak{P}}/K_{\mathfrak{p}}$ is unramified, and so the above map is an isomorphism.

Definition 3.1. Let L/K be a Galois extension of number fields, and let $\mathfrak{P}$ be a prime of L lying over an unramified prime $\mathfrak{p}$ of K.

The *Frobenius element* for the unramified extension $L_{\mathfrak{P}}/K_{\mathfrak{p}}$, written $\operatorname{Fr}_{L_{\mathfrak{P}}/K_{\mathfrak{p}}}$, is the unique element of $\operatorname{Gal}(L_{\mathfrak{P}}/K_{\mathfrak{p}})$ that descends to the Frobenius element $x \mapsto x^{\operatorname{Nm}(\mathfrak{p})}$ of $\operatorname{Gal}(k_{\mathfrak{P}}/k_{\mathfrak{p}})$.

The *Frobenius element* for $\mathfrak{P}$ in L/K, written $(\mathfrak{P}, L/K)$, is the restriction of the Frobenius element for $L_{\mathfrak{P}}/K_{\mathfrak{p}}$ to L.

In other words, $(\mathfrak{P}, L/K)$ is the unique element of $\operatorname{Gal}(L/K)$ such that

$$\forall x \in \mathcal{O}_L \quad (\mathfrak{P}, L/K)(x) \equiv x^{\operatorname{Nm}(\mathfrak{p})} \mod \mathfrak{P}.$$

We'll see more about the Frobenius element later in Section 6, where we use it to describe the local and global reciprocity maps. We'll also see the Chebotarev density theorem, which tells us that every element of $\operatorname{Gal}(L/K)$ is the Frobenius element for infinitely many primes $\mathfrak{P}$. So understanding how a Frobenius element acts on an elliptic curve E will be enough to understand how each element of $\operatorname{Gal}(L/K)$ acts on E.

3.2 Reducing elliptic curves modulo $\mathfrak{P}$

Let E be an elliptic curve defined over a number field L, and let $\mathfrak{P}$ be a prime of L. Let $\mathfrak{p} = \mathfrak{P} \cap K$ be the prime of K that $\mathfrak{P}$ lies over.

We now look at reduction modulo $\mathfrak{P}$. Like with Galois conjugation, there are multiple things we can reduce:

Elliptic curves Given an integral Weierstrass equation for an elliptic curve E, we can reduce all the coefficients modulo $\mathfrak{P}$ to obtain a Weierstrass equation over the field $k_{\mathfrak{P}}$. This then defines a curve $\widetilde{E}$ over $k_{\mathfrak{P}}$. The associated quantities $b_2, \ldots, b_8, c_4, c_6, \Delta, \omega$ for the reduced equation are then just the reductions of the original quantities modulo $\mathfrak{P}$.

Note however that if $\mathfrak{P}|\Delta$, then $\widetilde{\Delta} = 0$, so the reduced equation does not define an elliptic curve. If $\mathfrak{P}|\Delta$, then this won't be a problem. In this case we have *good reduction*, and the j-invariant of $\widetilde{E}$ will be the reduction of $j(E)$ modulo $\mathfrak{P}$.

Only finitely many primes divide Δ, so all but finitely many primes give good reduction.

Points on elliptic curves We can reduce points: we have a reduction map

$$E \to \widetilde{E}$$

$$(x : y : z) \mapsto (\widetilde{x} : \widetilde{y} : \widetilde{z}),$$

where we pick x, y, z such that $\min(v_{\mathfrak{P}}(x), v_{\mathfrak{P}}(y), v_{\mathfrak{P}}(z)) = 0$. Here $\widetilde{x}$ represents the residue class of x modulo $\mathfrak{P}$.

Isogenies between elliptic curves In a similar way, if $\mathfrak{P}$ is a prime of good reduction for E, E', and $\phi : E \to E'$ is an isogeny, then we can reduce the isogeny modulo $\mathfrak{P}$ to get an isogeny $\widetilde{\phi} : \widetilde{E} \to \widetilde{E'}$ such that the following diagram commutes:

$$\begin{array}{ccc} E & \xrightarrow{\phi} & E' \\ \downarrow & & \downarrow \\ \widetilde{E} & \xrightarrow{\widetilde{\phi}} & \widetilde{E'} \end{array}$$

3.3 The Frobenius isogenies

In finite fields such as $k_{\mathfrak{P}}$, the Galois group $\mathrm{Gal}(k_{\mathfrak{P}}/\mathbb{F}_p)$ consists of Frobenius elements $\mathrm{Fr}_{p^n} \in \mathrm{Gal}(k_{\mathfrak{P}}/\mathbb{F}_p)$:

$$\mathrm{Fr}_{p^n} : x \mapsto x^{p^n}.$$

So the function $\mathrm{Fr}_{p^n} : \widetilde{E} \to \widetilde{E}^{\mathrm{Fr}_{p^n}}$ is actually an isogeny, which we will denote ψ_{p^n}:

$$\psi_{p^n} : \widetilde{E} \to \widetilde{E}^{\mathrm{Fr}_{p^n}}$$

$$(x : y : z) \mapsto (x^{p^n} : y^{p^n} : z^{p^n}).$$

This isogeny has degree p^n, and is called the *p^n-Frobenius isogeny.*

These maps ψ_{p^n} are the 'fundamental' inseparable morphisms: any morphism $\phi : \widetilde{E} \to \widetilde{E'}$ can be written as $\phi = \psi_{p^n} \circ \chi$, for some n, where χ is a separable morphism.

3.4 Lifitng the p-Frobenius isogeny

In this section, L will be a finite Galois extension of K satisfying the conditions of Proposition 2.11.

Let $E \in \mathrm{Ell}(\mathcal{O}_K)$, and let $\mathfrak{P}$ be a prime of L. If $\mathfrak{p}$ *has degree 1*, i.e. $\mathrm{Nm}(\mathfrak{p}) = p$, then $k_\mathfrak{p} = \mathbb{F}_p$, and so $(\mathfrak{P}, L/K)$ restricts to Fr_p.

We will try to construct an isogeny $E \to E^{(\mathfrak{P}, L/K)}$ that descends to the isogeny ψ_p modulo $\mathfrak{P}$.

First, we need some lemmas, which we will quote:

Lemma 3.2. *Let χ be an isogeny $\widetilde{E} \to \widetilde{E}$. Then there exists $\hat{\chi} : E \to E$ reducing to χ modulo $\mathfrak{P}$ iff χ commutes with $\widetilde{\phi}$ for all isogenies $\phi : E \to E$.*

Lemma 3.3. *Let $\widetilde{\cdot}$ represent reduction modulo $\mathfrak{P}$. Given $E, E'/L$ elliptic curves with good reduction modulo $\mathfrak{P}$, and an isogeny $\phi : E \to E'$, we get an isogeny*

$$\widetilde{\phi} : \widetilde{E} \to \widetilde{E'}.$$

Then

$$\deg(\phi) = \deg\left(\widetilde{\phi}\right).$$

Proof. See [3]. □

Our approach to obtaining the Frobenius isogeny will be to construct some isogenies that reduce to inseparable isogenies modulo $\mathfrak{P}$. First, we give a criterion for checking whether the isogeny $\phi_\mathfrak{c}$ is inseparable:

Lemma 3.4. *Let $\mathfrak{P}$ be a prime of L of good reduction for E, and let $\mathfrak{p}$ be the prime of K that $\mathfrak{P}$ lies over. Let $\mathfrak{c}$ be an ideal of $\mathcal{O}_K$. Let $\widetilde{\phi_\mathfrak{c}}$ be the reduction of the isogeny*

$$\phi_\mathfrak{c} : E \to \bar{\mathfrak{c}} * E$$

modulo $\mathfrak{P}$. Then $\widetilde{\phi_\mathfrak{c}}$ is inseparable iff $\mathfrak{p}$ divides $\mathfrak{c}$.

Proof. First we prove it in the case where $\mathfrak{c} = (\alpha)$ is a principal ideal. Then $\phi_\mathfrak{c}$ differs from the isogeny $[\alpha]$ by an isomorphism, so $\phi_\mathfrak{c}$ is inseparable iff $[\alpha]$ is.

We check separability using the invariant differential. By definition of $[\cdot]$, we have

$$\phi_\mathfrak{c}^* \omega = [\alpha]^* \omega = \alpha\omega.$$

Reducing this modulo $\mathfrak{P}$ then gives

$$\widetilde{\phi_\mathfrak{c}}^* \widetilde{\omega} = \widetilde{\alpha}\widetilde{\omega}.$$

Note that $\widetilde{\omega}$ is an invariant differential for $\widetilde{E}$. The RHS is zero iff $\alpha = 0$ in $\mathcal{O}_L/\mathfrak{P}$, which holds precisely when $\mathfrak{p}$ divides $(\alpha) = \mathfrak{c}$. So this proves the lemma for $\mathfrak{c}$ principal.

Next, let $\mathfrak{c}$ be any ideal of $\mathcal{O}_K$. We can find some ideal $\mathfrak{c}'$ with norm not divisible by p in the inverse ideal class to $\mathfrak{c}$. Then $\mathfrak{c}'\mathfrak{c}$ is principal. Now we have

$$\widetilde{\phi_{\mathfrak{c}'\mathfrak{c}}} = \widetilde{\phi_{\mathfrak{c}'}} \circ \widetilde{\phi_\mathfrak{c}}.$$

Also,

$$\begin{aligned} \deg \widetilde{\phi_{\mathfrak{c}'}} &= \deg \phi_{\mathfrak{c}'} && \text{by Lemma 3.3} \\ &= \mathrm{Nm}(\mathfrak{c}') && \text{by Lemma 2.8} \end{aligned}$$

which we have chosen to be coprime to $p = \mathrm{char}\, k_\mathfrak{P}$. Therefore $\widetilde{\phi_{\mathfrak{c}'}}$ is separable, and so $\widetilde{\phi_\mathfrak{c}}$ is inseparable iff $\widetilde{\phi_{\mathfrak{c}'\mathfrak{c}}}$ is.

But $\mathfrak{c}'\mathfrak{c}$ is principal, and $\mathfrak{p}$ does not divide $\mathfrak{c}'$, so we can conclude that $\widetilde{\phi_\mathfrak{c}}$ is inseparable iff $\mathfrak{p}$ divides $\mathfrak{c}$. □

Now we are ready to prove the following lemma, which relates $\phi_{\mathfrak{p}}$ with the p-power Frobenius isogeny, provided that certain conditions are satisfied.

Lemma 3.5. *Let $E \in \mathrm{Ell}(\mathcal{O}_K)$.*

Let $\mathfrak{P}$ be a prime of L satisfying:

i) $\mathfrak{P}$ is a prime of good reduction for E.

ii) $\mathfrak{p} = \mathfrak{P} \cap K$ is a degree 1 prime.

iii) For all $\bar{\mathfrak{a}} \neq \bar{\mathfrak{a}}' \in \mathcal{Cl}(\mathcal{O}_K)$, we have $v_{\mathfrak{P}}(j(E_{\bar{\mathfrak{a}}}) - j(E_{\bar{\mathfrak{a}}'})) = 0$.

Then there exists an isomorphism $\theta : \bar{\mathfrak{p}} * E \to E^{(\mathfrak{P}, L/K)}$ such that the composition

$$\theta \circ \phi_{\mathfrak{p}} : E \to E^{(\mathfrak{P}, L/K)}$$

reduces to the p-power Frobenius isogeny ψ_p when taken modulo $\mathfrak{P}$.

Proof. To ease notation, write σ for $(\mathfrak{P}, L/K)$.

First note that $\phi_{\mathfrak{p}}$ has degree p. So by Lemma 3.3, $\widetilde{\phi_{\mathfrak{p}}}$ also has degree p. Next, by Lemma 3.4, we know that $\widetilde{\phi_{\mathfrak{p}}}$ is inseparable.

So if we write $\phi_{\mathfrak{p}}$ as a composition of purely inseparable and separable morphisms, we get

$$\phi_{\mathfrak{p}} = \psi_p \circ \chi.$$

Counting degrees, we find $\deg \chi = 1$, i.e. χ is an isomorphism $\widetilde{E^\sigma} \to \widetilde{\bar{\mathfrak{p}} * E}$. Hence

$$j(\widetilde{E^\sigma}) = j(\widetilde{\bar{\mathfrak{p}} * E}),$$

and so

$$j(E^\sigma) \equiv j(\bar{\mathfrak{p}} * E) \mod \mathfrak{P},$$

i.e.

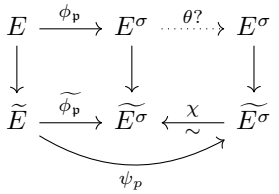
$$v_{\mathfrak{P}}(j(E^\sigma) \equiv j(\bar{\mathfrak{p}} * E)) > 0.$$

Now, by condition (iii) on $\mathfrak{P}$, we deduce that

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

and so $E^\sigma = \bar{\mathfrak{p}} * E$.

Thus, we have the following diagram:



Next, we show that χ has a lift to an isogeny $E^\sigma \to E^\sigma$. To check this, we use Lemma 3.2. First note that for all isogenies $[\alpha]_E$ and all points $T \in \widetilde{E}$, we have

$$\mathrm{Fr}_p\left(\widetilde{[\alpha]_E}(T)\right) = \widetilde{[\alpha]_E}^{\mathrm{Fr}_p}(\mathrm{Fr}_p(T)).$$

Therefore

$$\begin{aligned}
\psi_p \circ \widetilde{[\alpha]_E} &= \widetilde{[\alpha]_E}^{\mathrm{Fr}_p} \circ \psi_p \\
&= \widetilde{[\alpha]_E^\sigma} \circ \psi_p \\
&= \widetilde{[\alpha]_{E^\sigma}} \circ \psi_p
\end{aligned}$$

and so

$$\begin{aligned}
[\alpha]_{E^\sigma} \circ \phi_{\mathfrak{p}} &= \phi_{\mathfrak{p}} \circ [\alpha]_E && \text{by Proposition 1.11} \\
\widetilde{[\alpha]_{E^\sigma}} \circ \widetilde{\phi_{\mathfrak{p}}} &= \widetilde{\phi_{\mathfrak{p}}} \circ \widetilde{[\alpha]_E} \\
\widetilde{[\alpha]_{E^\sigma}} \circ \chi \circ \psi_p &= \chi \circ \psi_p \circ \widetilde{[\alpha]_E} \\
&= \chi \circ \widetilde{[\alpha]_{E^\sigma}} \circ \psi_p && \text{by above.}
\end{aligned}$$

ψ_p is surjective, so we conclude that χ commutes with $\widetilde{[\alpha]_{E^\sigma}}$ for all $\alpha \in \mathcal{O}_K$. So, by Lemma 3.2, χ lifts to an isogeny $\hat{\chi} : E^\sigma \to E^\sigma$.

We have $\deg \hat{\chi} = \deg \chi = 1$ by Lemma 3.3, so $\hat{\chi}$ is an isomorphism, and therefore has an inverse θ. This θ then completes the commutative diagram, giving

$$\widetilde{\theta \circ \phi_{\mathfrak{p}}} = \psi_p.$$

□

4 Adeles and ideles

4.1 Definition

Given a prime $\mathfrak{p}$ of K, we can 'work locally' and only look at things modulo powers of $\mathfrak{p}$. When moving from working modulo $\mathfrak{p}^n$ to modulo $\mathfrak{p}^{n+1}$, there is a compatiblity condition. Local fields are a way to work modulo $\mathfrak{p}^n$ for all n simultaneously, satisfying all the compatibility conditions.

An element of the completion $\mathcal{O}_{\mathfrak{p}}$ can be thought of as a sequence $(x_1, x_2, x_3, \ldots)$, where each x_i is a residue class modulo $\mathfrak{p}^i$, and the x_i are compatible:

$$x_i \equiv x_{i+1} \mod \mathfrak{p}^i \quad \forall i.$$

(If we want to talk about $K_{\mathfrak{p}}$ instead of $\mathcal{O}_{\mathfrak{p}}$, we should replace '$x \equiv y \mod \mathfrak{p}^n$' with $v_{\mathfrak{p}}(x-y) \geq n$.)

Consider working modulo $\mathfrak{c}$ for a general ideal $\mathfrak{c} \triangleleft \mathcal{O}_K$. When moving from working modulo $\mathfrak{c}$ to working modulo $\mathfrak{c}' \subseteq \mathfrak{c}$, there will be a compatibility condition. Adeles and ideles are a way to work modulo $\mathfrak{c}$ for all $\mathfrak{c}$ simultaneously, satisfying all the compatibility conditions.

What will we use these for?

- In Section 5, we will use ideles to describe the isomorphisms $K/\mathfrak{a} \to K/\mathfrak{a}'$ for $\mathfrak{a}, \mathfrak{a}'$ fractional ideals of $\mathfrak{a}$. These modules are the union of the $\mathfrak{c}$-torsion submodules of $\mathbb{C}/\mathfrak{a}, \mathbb{C}/\mathfrak{a}'$ over all integral ideals $\mathfrak{c} \triangleleft \mathcal{O}_K$, and correspondingly, the ideles are the inverse limits of the 'data modulo $\mathfrak{c}$' over all ideals $\mathfrak{c}$.
- In Section 6 we will use ideles to formulate global class field theory. There is a formulation of the main results of global class field theory without ideles, through the use of *conductors* $\mathfrak{c}$, but the idelic formulation wraps this up through its topology, which tells us that when we quotient out by an open subgroup we work modulo $\mathfrak{c}$ for some ideal $\mathfrak{c}$.

First, we set up some notation.

- Let V be the set of all nontrivial places of K (both finite and infinite).
- Let V_f be the set of all finite places of K.
- Let K_v be the completion of K with respect to the place v.
- For $v = \mathfrak{p}$ finite, let $\mathcal{O}_{\mathfrak{p}}$ denote the ring of integers of $K_{\mathfrak{p}}$.

$$\mathcal{O}_{\mathfrak{p}} = \{x \in K_{\mathfrak{p}} : v_{\mathfrak{p}}(x) \geq 0\}.$$

- For $v = \mathfrak{p}$ finite, let $U_{K_{\mathfrak{p}}}$ denote the group of units of $O_{K_{\mathfrak{p}}}$.

$$U_{K_{\mathfrak{p}}} = \{x \in K_{\mathfrak{p}} : v_{\mathfrak{p}}(x) = 0\}.$$

Here are the definitions.

Definition 4.1. The *ring of adeles* of a number field K, written $\mathbb{A}_K$ or just $\mathbb{A}$, is the *restricted product* of the completions K_v with respect to the open subrings $\mathcal{O}_\mathfrak{p}$.

In other words,

$$\mathbb{A}_K = \{(x_v)_v \mid x_v \in K_v \ \forall v,\ x_\mathfrak{p} \in \mathcal{O}_\mathfrak{p} \text{ for all but finitely many finite places } \mathfrak{p}\}.$$

We write this as

$$\mathbb{A}_K = \prod_{v \in V}{}' K_v,$$

where the dash symbol indicates the restricted product.

We can also define the *group of finite adeles*, written $\mathbb{A}_f$, by only taking the restricted product over the finite places:

$$\mathbb{A}_f = \prod_{\mathfrak{p} \in V_f}{}' K_\mathfrak{p}.$$

This can also be viewed as the quotient of $\mathbb{A}$ by the infinite places.

Definition 4.2. The *group of ideles* of a number field K, written $\mathbb{I}_K$ or just $\mathbb{I}$, is defined as

$$\mathbb{I}_K = \mathbb{A}_K^\times.$$

It is the restricted product of the multiplicative groups $K_v^\times$ with respect to the subgroups $U_{K_\mathfrak{p}} = \mathcal{O}_\mathfrak{p}^\times$:

$$\mathbb{I}_K = \prod_{v \in V}{}' K_v^\times.$$

Similarly, the *group of finite ideles* is

$$\mathbb{I}_f = \mathbb{A}_f^\times = \prod_{\mathfrak{p} \in V_f}{}' K_\mathfrak{p}^\times.$$

The adele ring contains K, as well as all the completions of K.

- Given a place v, there is a natural injection $K_v \hookrightarrow \mathbb{A}_K$, given by

  $$x \mapsto (\ldots, 1, 1, x, 1, \ldots)$$

  where the x is in the v position.

- There is also a natural injection $K \hookrightarrow \mathbb{A}_K$, given by

  $$x \mapsto (x)_v.$$

  So we can view K as a subring of $\mathbb{A}_K$.

In a similar manner, we can view $K^\times$, $K_v^\times$ as subgroups of $\mathbb{I}_K$.

4.2 Ideal of an idele

Given any prime $\mathfrak{p}$ of K, we can talk about the $\mathfrak{p}$-adic valuation of an idele x by looking at the $\mathfrak{p}$-adic valuation of $x_\mathfrak{p}$. Because we have taken the restricted product, we have

$$v_\mathfrak{p}(x_\mathfrak{p}) = 0 \quad \text{for all but finitely many } \mathfrak{p}.$$

Therefore, we may define the ideal of an idele:

Definition 4.3. The *ideal* of an idele $x \in \mathbb{I}$, written $i(x)$ or just (x), is the fractional ideal

$$i(x) = \prod_{\mathfrak{p}} \mathfrak{p}^{v_{\mathfrak{p}}(x_{\mathfrak{p}})}.$$

So we have

$$v_{\mathfrak{p}}(i(x)) = v_{\mathfrak{p}}(x_{\mathfrak{p}})$$

for all $\mathfrak{p}$.

This gives a homomorphism from $\mathbb{I}$ to the group of fractional ideals of K. Let W be the kernel of i, i.e.

Definition 4.4. W is the subgroup

$$W = \{(x_v)_v \in \mathbb{I} \mid x \in U_{K_{\mathfrak{p}}} \text{ for all finite places } \mathfrak{p}\}.$$

One could think of the ideles $\mathbb{I}$ as the subset of the direct product $\prod_v K_v^\times$ where the ideal is well-defined.

If L/K is an extension of number fields, then we have maps $K \hookrightarrow L$ and $\mathrm{Nm} : L \to K$. We can extend these to maps between the idele groups.

Definition 4.5. The *norm map* $\mathrm{Nm} : \mathbb{I}_L \to \mathbb{I}_K$ is defined by

$$\mathrm{Nm}(s)_v = \prod_{w|v} \mathrm{Nm}_{L_w/K_v}(s_w).$$

This then has the property that $\mathrm{Nm}(i(s)) = i(\mathrm{Nm}(s))$ for all $s \in \mathbb{I}_L$.

4.3 Topology of $\mathbb{A}$

The topology of $\mathbb{A}$ is given by the restricted product topology:

Definition 4.6. $\mathbb{A}$ has a basis of open sets given by the sets

$$\prod_v S_v,$$

where each S_v is an open subset of K_v, and $S_{\mathfrak{p}} = \mathcal{O}_{\mathfrak{p}}$ for all but finitely many finite places $\mathfrak{p}$.

This makes $\mathbb{A}$ into a topological ring, i.e. addition and multiplication are continuous maps $\mathbb{A} \times \mathbb{A} \to \mathbb{A}$.

The image of K in $\mathbb{A}$ is not dense, but if we quotient $\mathbb{A}$ by any one component local field K_v then the image of K in that is dense. This can be phrased more explicitly as the following:

Theorem 4.7 (Strong approximation theorem)**.** *Let v_0 be a place of K. Let S be a finite subset of $V \setminus \{v_0\}$. For each $v \in S$, pick $\alpha_v \in K_v$ and $\epsilon_v > 0$. Then there exists $x \in K$ such that*

- $|x - \alpha_v|_v < \epsilon_v$ *for all* $v \in S$
- $x \in \mathcal{O}_{\mathfrak{p}}$ *for all finite places* $\mathfrak{p} \notin S, \mathfrak{p} \neq v_0$

Proof. See [1] II.15. □

Remark The subring $K \subseteq \mathbb{A}$ has several other nice topological properties, such as

- K is discrete.
- $\mathbb{A}^+/K^+$ (the quotient of additive groups) is compact.

4.4 Open subgroups of $\mathbb{I}$

We want to make $\mathbb{I}$ into a topological group. Unfortunately, taking the subset topology from $\mathbb{A}$ does not work, since inversion would not be continuous. Instead, we use the topology from the restricted product for $\mathbb{I}$:

Definition 4.8. $\mathbb{I}$ has a basis of open sets given by the sets

$$\prod_v S_v,$$

where each S_v is an open subset of $K_v^\times$, and $S_{\mathfrak{p}} = U_{K_{\mathfrak{p}}}$ for all but finitely many finite places $\mathfrak{p}$.

Next, we want to look at open subgroups of $\mathbb{I}$, because any continuous group homomorphism to a discrete group will have kernel an open subgroup.

First, we describe the open subgroups of a local field $\mathcal{K}$.

Definition 4.9. We define some open subgroups of $\mathcal{K}$ and index them.

- If $\mathcal{K} = \mathbb{C}$, let
$$U_{\mathbb{C}}^{(0)} = \mathbb{C}^\times.$$
- If $\mathcal{K} = \mathbb{R}$, let
$$U_{\mathbb{R}}^{(0)} = \mathbb{R}^\times, \quad U_{\mathbb{R}}^{(1)} = \mathbb{R}_{>0}.$$
- If $\mathcal{K}$ is non-archimedean, then let
$$U_{\mathcal{K}}^{(0)} = \mathcal{O}_{\mathcal{K}}^\times$$
$$U_{\mathcal{K}}^{(n)} = 1 + \pi^n \mathcal{O}_{\mathcal{K}} = \{x \in \mathcal{K}^\times : v_{\mathcal{K}}(x-1) \geq n\}.$$

The open subgroups of $\mathcal{K}$ are

- If $\mathcal{K} = \mathbb{C}$, then the only open subgroup of $\mathcal{K}^\times = \mathbb{C}^\times$ is $\mathbb{C}^\times = U_{\mathbb{C}}^{(0)}$ itself.
- If $\mathcal{K} = \mathbb{R}$, then the only open subgroups of $\mathcal{K}^\times = \mathbb{R}^\times$ are $\mathbb{R}^\times$ and $\mathbb{R}_{>0}$, i.e. $U_{\mathbb{R}}^{(0)}, U_{\mathbb{R}}^{(1)}$.
- If $\mathcal{K}$ is non-archimedean, then a basis of open neighbourhoods of 1 in $\mathcal{K}^\times$ is $U_{\mathcal{K}}^{(n)} (n \geq 0)$. Therefore, every open subgroup of $\mathcal{K}^\times$ contains $U_{\mathcal{K}}^{(n)}$ for some $n \geq 0$.

Motivated by this, we define a way to index a basis of open subgroups:

Definition 4.10. A *modulus* $\mathfrak{m}$ is a function from places of K to $\mathbb{Z}_{\geq 0}$, subject to the following:

- $\mathfrak{m}(v) = 0$ for all but finitely many places.
- If v is a complex place, then $\mathfrak{m}(v) = 0$.
- If v is a real place, then $\mathfrak{m}(v) = 0$ or 1.

We write it as a product of places:

$$\mathfrak{m} = \prod_v v^{\mathfrak{m}(v)}.$$

We say v *divides* $\mathfrak{m}$ if $\mathfrak{m}(v) > 0$.

We can write $\mathfrak{m}$ as a product of the infinite and finite parts: $\mathfrak{m} = \mathfrak{m}_\infty \mathfrak{m}_0$.

Note that $\mathfrak{m}_0$ can be identified with an ideal of $\mathcal{O}_K$. Also, if K is totally imaginary (i.e. has no real embeddings) then $\mathfrak{m}_\infty$ is always trivial.

Definition 4.11. Let $\mathfrak{m}$ be a modulus.

Define $\mathbb{I}_{\mathfrak{m}}$ to be the subgroup consisting of all $s \in \mathbb{I}_K$ such that $s_v \in U_{K_v}^{(\mathfrak{m}(v))}$ for all places v with $\mathfrak{m}(v) \geq 1$.

Define $W_{\mathfrak{m}}$ to be the subgroup consisting of all $s \in \mathbb{I}_K$ such that $s_v \in U_{K_v}^{(\mathfrak{m}(v))}$ for all places v (including those with $\mathfrak{m}(v) = 0$). Note that this means that $s_{\mathfrak{p}} \in U_{K_{\mathfrak{p}}}$ for all primes $\mathfrak{p}$.

In other words, $W_{\mathfrak{m}} = W \cap \mathbb{I}_{\mathfrak{m}}$.

Then $W_{\mathfrak{m}}$ is an open subgroup of $\mathbb{I}$, and every open subgroup of $\mathbb{I}$ contains $W_{\mathfrak{m}}$ for some modulus $\mathfrak{m}$.

The largest such subgroup is when $\mathfrak{m} = (1)$: this gives $\mathbb{I}_{(1)} = \mathbb{I}$ and $W_{(1)} = W$.

5 Torsion

5.1 $\mathfrak{c}$-torsion

The $\mathfrak{c}$-torsion points of $\mathbb{C}/\Lambda$ are given by

$$\{a + \Lambda \in \mathbb{C}/\Lambda \mid a \in \mathfrak{c}^{-1}\Lambda\} = \mathfrak{c}^{-1}\Lambda/\Lambda.$$

Note that these form an $O_K/\mathfrak{c}$-module.

As is often the case, understanding the structure of the $\mathfrak{c}$-torsion points of $\mathbb{C}/\Lambda$ can be reduced to understanding the structure of $\mathfrak{p}^e$-torsion points of $\mathbb{C}/\Lambda$, where $\mathfrak{p}$ is a prime of K.

Lemma 5.1. *Let $\mathfrak{c} = \mathfrak{p}_1^{e_1} \dots \mathfrak{p}_k^{e_k}$ be an integral ideal of $\mathcal{O}_K$.*

Let $\Lambda \subseteq \mathbb{C}$ be a lattice satisfying $\mathcal{O}_K\Lambda = \Lambda$. Then

$$\bigoplus_i \frac{\mathfrak{p}_i^{-e_i}\Lambda}{\Lambda} = \frac{\mathfrak{c}^{-1}\Lambda}{\Lambda}$$

as a direct sum of submodules.

Proof. Write $\mathfrak{q}_i = \mathfrak{p}_i^{e_i}$.

We have $\mathfrak{c} = \mathfrak{q}_1\mathfrak{q}_2 \dots \mathfrak{q}_k$, with the $\mathfrak{q}_i$ pairwise coprime. Define $\mathfrak{b}_i = \mathfrak{c}\mathfrak{q}_i^{-1} = \prod_{j\neq i} \mathfrak{q}_j$.

We wish to show that the map

$$\bigoplus_i \frac{\mathfrak{q}_i^{-1}\Lambda}{\Lambda} \to \frac{\mathfrak{c}^{-1}\Lambda}{\Lambda}$$

$$(z_i + \Lambda)_i \mapsto \sum_i z_i + \Lambda$$

is an isomorphism.

Injectivity: Suppose we have $z_i \in \mathfrak{q}_i^{-1}\Lambda$ such that $z = \sum_i z_i \in \Lambda$. Then, for each i, we have

$$z_i = z - \sum_{j\neq i} z_j.$$

For all $j \neq i$, $z_j \in \mathfrak{q}_j^{-1}\Lambda \subseteq \mathfrak{b}_i^{-1}\Lambda$. Also, $z \in \Lambda \subseteq \mathfrak{b}_i^{-1}\Lambda$. So the RHS is in $\mathfrak{b}_i^{-1}\Lambda$.

This shows that $z_i \in \mathfrak{b}_i^{-1}\Lambda$, which tells us that $\beta z_i \in \Lambda$ for all $\beta \in \mathfrak{b}_i$. Similarly, $z_i \in \mathfrak{q}_i^{-1}\Lambda$ tells us that $\alpha z_i \in \Lambda$ for all $\alpha \in \mathfrak{q}_i$. But $\mathfrak{q}_i + \mathfrak{b}_i = (1)$, so we can find $\alpha \in \mathfrak{q}_i, \beta \in \mathfrak{b}_i$ such that $\alpha + \beta = 1$. So

$$z_i = \alpha z_i + \beta z_i \in \Lambda,$$

i.e. $z_i + \Lambda$ is the identity element.

This holds for all i, so we've shown injectivity.

Surjectivity: We have

$$\mathfrak{b}_1 + \ldots + \mathfrak{b}_k = (1).$$

Therefore there exist $b_i \in \mathfrak{b}_i$ such that

$$b_1 + \ldots + b_k = 1.$$

Now, given $z \in \mathfrak{c}^{-1}\Lambda$, we will have

$$b_i z \in \mathfrak{b}_i\mathfrak{c}^{-1}\Lambda = \mathfrak{q}_i^{-1}\Lambda.$$

So $(b_i z + \Lambda)_i$ is an element of the direct sum, and it maps to

$$(b_i z + \Lambda)_i \mapsto \sum_i b_i z + \Lambda = z + \Lambda.$$

Hence $z + \Lambda$ is in the image, which shows surjectivity. □

The above lemma allows us to break down a torsion submodule into its primary components. Next, we study each primary component on its own. For this, we will be able to say more about the torsion submodule if we restrict to the case where $\Lambda = \mathfrak{a}$ a fractional ideal.

Lemma 5.2. *Let $\mathfrak{a}$ be a fractional ideal of $\mathcal{O}_K$, and let $\mathfrak{p}$ be a prime ideal of $\mathcal{O}_K$. Let $\pi \in K_\mathfrak{p}$ be a uniformiser of the completion $K_\mathfrak{p}$, and let $d = v_\mathfrak{p}(\mathfrak{a})$ be the exponent of $\mathfrak{p}$ in the prime factorisation of $\mathfrak{a}$.*
Note we have a natural inclusion map

$$\mathfrak{p}^{-e}\mathfrak{a} \hookrightarrow \mathfrak{p}^{-e}\mathfrak{a}\mathcal{O}_\mathfrak{p} = \pi^{d-e}\mathcal{O}_\mathfrak{p}.$$

Then, for all $e > 1$, this induces a map

$$\frac{\mathfrak{p}^{-e}\mathfrak{a}}{\mathfrak{a}} \to \frac{\mathfrak{p}^{-e}\mathfrak{a}\mathcal{O}_\mathfrak{p}}{\mathfrak{a}\mathcal{O}_\mathfrak{p}} = \frac{\pi^{d-e}\mathcal{O}_\mathfrak{p}}{\pi^d\mathcal{O}_\mathfrak{p}},$$

and this is an isomorphism of $\mathcal{O}_K$-modules.

Proof. To show well-definedness and injectivity, we need to show that

$$\mathfrak{p}^{-e}\mathfrak{a} \cap \mathfrak{a}\mathcal{O}_\mathfrak{p} = \mathfrak{a}.$$

To do this, note that

$$\begin{aligned}
\mathfrak{a}\mathcal{O}_\mathfrak{p} \cap \mathfrak{p}^{-e}\mathfrak{a} &= \pi^d\mathcal{O}_\mathfrak{p} \cap \mathfrak{p}^{-e}\mathfrak{a} \\
&= \{x \in \mathfrak{p}^{-e}\mathfrak{a} : v_\mathfrak{p}(x) \geq d\} \\
&= \mathfrak{p}^d \cap \mathfrak{p}^{-e}\mathfrak{a} \\
&= \mathfrak{p}^d \cap (\mathfrak{p}^{d-e}(\mathfrak{a}\mathfrak{p}^{-d}))
\end{aligned}$$

The intersection of two fractional ideals is equal to their LCM, i.e. take the highest exponent of each prime. $\mathfrak{a}\mathfrak{p}^{-d}$ is coprime to $\mathfrak{p}$, so the above is equal to

$$= \mathfrak{p}^d(\mathfrak{a}\mathfrak{p}^{-d}) = \mathfrak{a},$$

which proves well-definedness and injectivity.

For surjectivity: let y be an element of $\pi^{d-e}\mathcal{O}_\mathfrak{p}$. We wish to find $x \in \mathfrak{p}^{-e}\mathfrak{a}$ such that

$$x \equiv y \mod \pi^d,$$

i.e.

$$v_\mathfrak{p}(x - y) \geq d.$$

First, we can find $y' \in \mathfrak{p}^{d-e}\mathcal{O}_K$ such that $v_\mathfrak{p}(y' - y) \geq d$, so we may assume WLOG that $y \in \mathfrak{p}^{d-e}\mathcal{O}_K$. Next, by strong approximation theorem, we can find $x \in K$ such that

$$\begin{cases} v_\mathfrak{p}(x - y) \geq d & \\ v_\mathfrak{q}(x) \geq v_\mathfrak{q}(\mathfrak{a}) & \forall \mathfrak{q} \neq \mathfrak{p} \text{ prime}, \mathfrak{q} | \mathfrak{a} \\ v_\mathfrak{q}(x) \geq 0 & \forall \mathfrak{q} \neq \mathfrak{p} \text{ prime}, \mathfrak{q} \nmid \mathfrak{a} \end{cases}.$$

Note that since $e \geq 1$ and $v_\mathfrak{p}(y) \geq d - e$, the first condition here implies a fourth condition:

$$v_\mathfrak{p}(x) \geq d - e.$$

But the second to fourth conditions are equivalent to $x \in \mathfrak{p}^{-e}\mathfrak{a}$, while the first condition says that x maps to y. So this shows surjectivity.

□

In the case where Λ is homothetic to $\mathcal{O}_K$ as a lattice, one can easily see that the $\mathfrak{c}$-torsion is isomorphic to $\mathcal{O}_K/\mathfrak{c}$ as an $\mathcal{O}_K$-module. We can now use the previous two lemmas to show that this is true for Λ in general:

Corollary 5.3. *Let $\Lambda \subseteq \mathbb{C}$ be a lattice s.t. $\mathcal{O}_K\Lambda = \Lambda$. Then $\mathfrak{c}^{-1}\Lambda/\Lambda$ is a free $\mathcal{O}_K/\mathfrak{c}$-module of rank 1.*

Proof. We have

$$\mathcal{O}_K/\mathfrak{c} \cong \bigoplus_i \mathcal{O}_K/\mathfrak{p}_i^{e_i}$$

and

$$\frac{\mathfrak{c}^{-1}\Lambda}{\Lambda} = \bigoplus_i \frac{(\mathfrak{p}_i^{e_i})^{-1}\Lambda}{\Lambda}.$$

So it suffices to show that $\mathfrak{p}_i^{-e_i}\Lambda/\Lambda$ is a free $\mathcal{O}_K/\mathfrak{p}_i^{e_i}$-module of rank 1 for each i.

Next, note that Λ is homothetic to a fractional ideal $\mathfrak{a}$ of K, so it suffices to show that $\mathfrak{p}^{-e}\mathfrak{a}/\mathfrak{a}$ is a free $\mathcal{O}_K/\mathfrak{p}^e$-module for any fractional ideal $\mathfrak{a}$.

But now observe

$$\begin{aligned}
\mathfrak{p}^{-e}\mathfrak{a}/\mathfrak{a} &\cong \frac{\pi^{d-e}\mathcal{O}_\mathfrak{p}}{\pi^d\mathcal{O}_\mathfrak{p}} && \text{by Lemma 5.2} \\
&\cong \frac{\mathcal{O}_\mathfrak{p}}{\pi^e\mathcal{O}_\mathfrak{p}} && \text{by the map } x \mapsto \pi^{e-d}x \\
&\cong \mathcal{O}_K/\mathfrak{p}^e && \text{by Lemma 5.2 on the ideal } \mathfrak{p}^e
\end{aligned}$$

which completes the proof. □

5.2 All the torsion

Let λ be a nonzero element of Λ. The torsion subgroup of $\mathbb{C}/\Lambda$ is

$$\begin{aligned}
(\mathbb{C}/\Lambda)_{tors} &= \{z + \Lambda \mid z \in \mathbb{C}, mz \in \Lambda \text{ for some } m \in \mathbb{N}\} \\
&= \{z + \Lambda \mid z \in \mathbb{C}, z/\lambda \in m^{-1}\lambda^{-1}\Lambda \text{ for some } m \in \mathbb{N}\} \\
&= \{z + \Lambda \mid z/\lambda \in K\} \\
&= (\lambda K)/\Lambda
\end{aligned}$$

Once again, we'll focus on the case where $\Lambda = \mathfrak{a}$ a fractional ideal. Then $\lambda \in K$, so the torsion subgroup is simply $K/\mathfrak{a}$.

The torsion subgroup $K/\mathfrak{a}$ is the union of the $\mathfrak{c}$-torsion subgroups $(\mathbb{C}/\mathfrak{a})[\mathfrak{c}]$ for all integral ideals $\mathfrak{c}$ of O_K. We can write this as the colimit (i.e. direct limit) of the diagram with directed set

$$\{\mathfrak{c}^{-1}\mathfrak{a}/\mathfrak{a} \mid \mathfrak{c} \trianglelefteq \mathcal{O}_K\}$$

$$\mathfrak{c} \leq \mathfrak{c}' \iff \mathfrak{c} \supseteq \mathfrak{c}'$$

and inclusion maps

$$\iota_{\mathfrak{c}\mathfrak{c}'} : \mathfrak{c}^{-1}\mathfrak{a}/\mathfrak{a} \hookrightarrow \mathfrak{c}'^{-1}\mathfrak{a}/\mathfrak{a}$$

for $\mathfrak{c} \supseteq \mathfrak{c}'$.

Definition 5.4. For $\mathfrak{p}$ a prime of K, let

$$(\mathbb{C}/\mathfrak{a})[\mathfrak{p}^\infty] = \{z \in \mathbb{C}/\mathfrak{a} \mid z\mathfrak{p}^n = 0 \text{ for some } n \geq 0\}.$$

Note

$$(\mathbb{C}/\mathfrak{a})[\mathfrak{p}^\infty] = K_\mathfrak{p}/\mathfrak{a}\mathcal{O}_\mathfrak{p}.$$

By Lemma 5.1, the module $\mathfrak{c}^{-1}\mathfrak{a}/\mathfrak{a}$ is the coproduct of $\mathfrak{p}_i^{-e_i}\mathfrak{a}/\mathfrak{a}$, where $\mathfrak{c} = \prod_i \mathfrak{p}_i^{e_i}$. Hence we can decompose into primes: the above colimit is equal to

$$\bigoplus_\mathfrak{p} \varinjlim \mathfrak{p}^{-n}\mathfrak{a}/\mathfrak{a} \cong \bigoplus_\mathfrak{p} \varinjlim \mathfrak{p}^{-n}\mathfrak{a}\mathcal{O}_\mathfrak{p}/\mathfrak{a}\mathcal{O}_\mathfrak{p} \cong \bigoplus_\mathfrak{p} K_\mathfrak{p}/\mathfrak{a}\mathcal{O}_\mathfrak{p}$$

as $\mathcal{O}_K$-modules.

5.3 Isomorphisms of torsion submodules

We now look at the isomorphisms between the two torsion subgroups $K/\mathfrak{a}, K/\mathfrak{a}'$. Once again, we can do this prime by prime.

Proposition 5.5. *There is an isomorphism*

$$F : \mathfrak{a}^{-1}\mathfrak{a}'\mathcal{O}_\mathfrak{p} \to \mathrm{Hom}_{\mathcal{O}_K}(K_\mathfrak{p}/\mathfrak{a}\mathcal{O}_\mathfrak{p}, K_\mathfrak{p}/\mathfrak{a}'\mathcal{O}_\mathfrak{p})$$

given by

$$F(t) : x + \mathfrak{a}\mathcal{O}_\mathfrak{p} \mapsto tx + \mathfrak{a}'\mathcal{O}_\mathfrak{p}.$$

The module on the right describes all homomorphisms between the $\mathfrak{p}^\infty$-torsion components of $K/\mathfrak{a}$ and $K/\mathfrak{a}'$. The key idea is that any such homomorphism can be thought of as a collection of homomorphisms between the $\mathfrak{p}^e$-torsion components, with some compatibility conditions. Meanwhile, an element of the module $\mathfrak{a}^{-1}\mathfrak{a}'\mathcal{O}_\mathfrak{p}$ can be thought of as a collection of values $t_e \in \mathfrak{a}^{-1}\mathfrak{a}'$ modulo some power of $\mathfrak{p}$, again with some compatibility conditions. The map F then precisely relates these two things.

Proof. Let $d = v_\mathfrak{p}(\mathfrak{a}),\ d' = v_\mathfrak{p}(\mathfrak{a}')$.
Then $\mathfrak{a}\mathcal{O}_\mathfrak{p} = \pi^d\mathcal{O}_\mathfrak{p},\ \mathfrak{a}'\mathcal{O}_\mathfrak{p} = \pi^{d'}\mathcal{O}_\mathfrak{p},\ \mathfrak{a}^{-1}\mathfrak{a}\mathcal{O}_\mathfrak{p} = \pi^{d'-d}\mathcal{O}_\mathfrak{p}$.

For $f \in \mathrm{Hom}_{\mathcal{O}_K}(K_\mathfrak{p}/\mathfrak{a}\mathcal{O}_\mathfrak{p}, K_\mathfrak{p}/\mathfrak{a}'\mathcal{O}_\mathfrak{p})$ and $e \geq 0$, write $f|_e$ for the restriction of f to the $\mathfrak{p}^e$-torsion:

$$f|_e :\ \pi^{d-e}\mathcal{O}_\mathfrak{p}/\pi^d\mathcal{O}_\mathfrak{p} \to \pi^{d'-e}\mathcal{O}_\mathfrak{p}/\pi^{d'}\mathcal{O}_\mathfrak{p}$$

Note that $f = f'$ iff $f|_e = f'|_e$ for all e.

We have $F(t)|_e = F(t')|_e$ iff t, t' give the same map on $\mathfrak{p}^e$-torsion. This happens iff $tx - t'x \in \pi^{d'}\mathcal{O}_\mathfrak{p}$ for all $x \in \pi^{d-e}\mathcal{O}_\mathfrak{p}$, i.e.

$$v_\mathfrak{p}(t - t') \geq d' - d + e.$$

Therefore, $F(t)|_e = F(t')|_e$ for all e iff $v_\mathfrak{p}(t - t') = \infty$, i.e. iff $t = t'$. So F is injective.

Next, pick $f \in \mathrm{Hom}_{\mathcal{O}_K}(K_\mathfrak{p}/\mathfrak{a}\mathcal{O}_\mathfrak{p}, K_\mathfrak{p}/\mathfrak{a}'\mathcal{O}_\mathfrak{p})$.

For a given e, pick an element x_e with valuation $v_\mathfrak{p}(x_e) = d - e$. This generates $\pi^{d-e}\mathcal{O}_\mathfrak{p}/\pi^d\mathcal{O}_\mathfrak{p}$ as an $\mathcal{O}_K$-module.
Then pick a representative $y_e \in \pi^{d'-e}\mathcal{O}_\mathfrak{p}$ such that

$$f(x_e + \pi^d\mathcal{O}_\mathfrak{p}) = y_e + \pi^{d'}\mathcal{O}_\mathfrak{p}.$$

Let $t_e = y_e/x_e \in \pi^{d'-d}\mathcal{O}_\mathfrak{p}$. We get

$$t_e x_e + \pi^{d'}\mathcal{O}_\mathfrak{p} = f(x_e + \pi^d\mathcal{O}_\mathfrak{p}).$$

Then we will have

$$t_e x + \pi^{d'}\mathcal{O}_\mathfrak{p} = f(x + \pi^d\mathcal{O}_\mathfrak{p})$$

for all $x \in \pi^{d-e}\mathcal{O}_\mathfrak{p}$, i.e.

$$F(t_e)|_e = f|_e.$$

This gives a sequence $t_1, t_2, \ldots$ that describes how f acts on $\mathfrak{p}^e$-torsion for each e. The t_e must be compatible with each other: for all e, we must have $F(t_{e+1})|_e = F(t_e)|_e$, which gives

$$v_\mathfrak{p}(t_{e+1} - t_e) \geq d' - d + e.$$

Hence the sequence (t_e) is Cauchy, and so it converges to a limit $t \in \pi^{d'-d}\mathcal{O}_\mathfrak{p}$. This t then satisfies $F(t)|_e = F(t_e)|_e = f|_e$ for all e, so $F(t) = f$. So we have shown surjectivity. □

To define an isomorphism of $\mathcal{O}_K$-modules

$$f : K/\mathfrak{a} \to K/\mathfrak{a}',$$

note that the $\mathfrak{p}$-primary parts must be sent to $\mathfrak{p}$-primary parts: if $x \in \mathfrak{p}^{-n}\mathfrak{a}/\mathfrak{a}$ then $f(x) \in \mathfrak{p}^{-n}\mathfrak{a}'/\mathfrak{a}'$. So we just need to give isomorphisms $f_\mathfrak{p}$ for each $\mathfrak{p}$ to give an isomorphism

$$f : \bigoplus_\mathfrak{p} K_\mathfrak{p}/\mathfrak{a}\mathcal{O}_\mathfrak{p} \to \bigoplus_\mathfrak{p} K_\mathfrak{p}/\mathfrak{a}'\mathcal{O}_\mathfrak{p}.$$

In other words, specifying f is the same as specifying an $c_\mathfrak{p} \in \{c \in K_\mathfrak{p} : v_\mathfrak{p}(c) = v_\mathfrak{p}(\mathfrak{b})\}$ for each prime $\mathfrak{p}$ of K.

So we can identify the set of all isomorphisms $f : K/\mathfrak{a} \to K/\mathfrak{a}'$ with the set

$$\{(c_\mathfrak{p})_\mathfrak{p} : c_\mathfrak{p} \in K_\mathfrak{p}, v_\mathfrak{p}(c_\mathfrak{p}) = v_\mathfrak{p}(\mathfrak{b})\}.$$

This is precisely the subgroup of the finite ideles given by

$$\{s \in \mathbb{I}_f : (s) = \mathfrak{b}\},$$

or the subgroup of the ideles given by $(s) = \mathfrak{b}$ after quotienting out by the infinite places.

Therefore, given a fractional ideal $\mathfrak{a}$ and any idele $s \in \mathbb{I}_K$, we get an isomorphism of torsion subgroups $K/\mathfrak{a} \to K/s\mathfrak{a}$, where $s\mathfrak{a} = (s)\mathfrak{a}$. We will denote this map $s\cdot$.

Definition 5.6. Given a fractional ideal $\mathfrak{a}$ and an idele $s \in \mathbb{I}_K$, the isomorphism of $\mathcal{O}_K$-modules

$$s\cdot : K/\mathfrak{a} \to K/s\mathfrak{a}$$

is defined by

$$s\cdot : \bigoplus_\mathfrak{p} K_\mathfrak{p}/\mathfrak{a}\mathcal{O}_\mathfrak{p} \to \bigoplus_\mathfrak{p} K_\mathfrak{p}/s_\mathfrak{p}\mathfrak{a}\mathcal{O}_\mathfrak{p}$$
$$(x_\mathfrak{p} + \mathfrak{a}\mathcal{O}_\mathfrak{p})_\mathfrak{p} \mapsto (s_\mathfrak{p}x_\mathfrak{p} + s_\mathfrak{p}\mathfrak{a}\mathcal{O}_\mathfrak{p})_\mathfrak{p}.$$

Remark.

- Note that this respects multiplication: we have
$$(s\cdot) \circ (t\cdot) = (st)\cdot.$$
- If $\alpha \in K^\times$, then the map we get from the idele α is just ϑ_α.
$$\alpha\cdot : \ z + \mathfrak{a} \mapsto \alpha z + \alpha\mathfrak{a}.$$

The next proposition will allow us to recover how this map $s\cdot$ acts on the $\mathfrak{c}$-torsion:

Proposition 5.7. *Let $\mathfrak{a}$ be a fractional ideal, and $\mathfrak{c}, \mathfrak{d}$ integral ideals.*
Recall that $\varphi_\mathfrak{d}$ is the map $\mathbb{C}/\mathfrak{a} \to \mathbb{C}/\mathfrak{d}^{-1}\mathfrak{a}$ given by

$$\varphi_\mathfrak{d} : z + \mathfrak{a} \mapsto z + \mathfrak{d}^{-1}\mathfrak{a}.$$

Then

i) $\varphi_\mathfrak{d}$ is an isomorphism on $\mathfrak{c}$-torsion iff $\mathfrak{c}, \mathfrak{d}$ are coprime.

ii) Suppose $\mathfrak{c}, \mathfrak{d}$ are coprime. Let $s \in \mathbb{I}$ is an idele such that $(s) = \mathfrak{d}^{-1}$, so that $s\cdot$ is an isomorphism

$$\mathbb{C}/\mathfrak{a} \to \mathbb{C}/\mathfrak{d}^{-1}\mathfrak{a}.$$

Then $s\cdot$ and $\varphi_\mathfrak{d}$ agree on $\mathfrak{c}$-torsion iff $s \in \mathbb{I}_\mathfrak{c}$.

Proof. Write $\mathfrak{c} = \mathfrak{p}_1^{e_1} \dots \mathfrak{p}_r^{e_r}$ as a product of prime powers, where each $e_i > 0$. Also, we will write φ for $\varphi_\mathfrak{d}$.

(i) The kernel of the map φ is

$$\mathfrak{d}^{-1}\mathfrak{a}/\mathfrak{a},$$

while the $\mathfrak{c}$-torsion of $\mathbb{C}/\mathfrak{a}$ is

$$\mathfrak{c}^{-1}\mathfrak{a}/\mathfrak{a}.$$

Note that the $\mathfrak{c}$-torsion subgroups of $\mathbb{C}/\mathfrak{a}, \mathbb{C}/\mathfrak{d}^{-1}\mathfrak{a}$ both have size $|\mathcal{O}_K/\mathfrak{c}|$, so φ being injective is equivalent to it being an isomorphism.

The kernel of the map φ on $\mathfrak{c}$-torsion is

$$\begin{aligned}\mathfrak{d}^{-1}\mathfrak{a}/\mathfrak{a} \cap \mathfrak{c}^{-1}\mathfrak{a}/\mathfrak{a} &= (\mathfrak{d}^{-1}\mathfrak{a} \cap \mathfrak{c}^{-1}\mathfrak{a})/\mathfrak{a} \\ &= (\mathfrak{d}^{-1} \cap \mathfrak{c}^{-1})\mathfrak{a}/\mathfrak{a}\end{aligned}$$

which is trivial iff $\mathfrak{d}^{-1} \cap \mathfrak{c}^{-1} = \mathcal{O}_K$, i.e. iff $\mathfrak{c}, \mathfrak{d}$ are coprime.

(ii) Let $d_i = v_{\mathfrak{p}_i}(\mathfrak{a})$. Then, since $\mathfrak{c}, \mathfrak{d}$ are coprime, we have $v_{\mathfrak{p}_i}(\mathfrak{a}') = d_i$.

The map φ restricted to $\mathfrak{c}$-torsion is

$$\varphi : \bigoplus_i \frac{\pi^{d_i - e_i}\mathcal{O}_{\mathfrak{p}_i}}{\pi^{d_i}\mathcal{O}_{\mathfrak{p}_i}} \to \bigoplus_i \frac{\pi^{d_i - e_i}\mathcal{O}_{\mathfrak{p}_i}}{\pi^{d_i}\mathcal{O}_{\mathfrak{p}_i}}$$

$$(x_{\mathfrak{p}_i} + \pi^{d_i}\mathcal{O}_{\mathfrak{p}_i})_i \mapsto (x_{\mathfrak{p}_i} + \pi^{d_i}\mathcal{O}_{\mathfrak{p}_i})_i,$$

while the map $s\cdot$ restricted to $\mathfrak{c}$-torsion is

$$s : \bigoplus_i \frac{\pi^{d_i - e_i}\mathcal{O}_{\mathfrak{p}_i}}{\pi^{d_i}\mathcal{O}_{\mathfrak{p}_i}} \to \bigoplus_i \frac{\pi^{d_i - e_i}\mathcal{O}_{\mathfrak{p}_i}}{\pi^{d_i}\mathcal{O}_{\mathfrak{p}_i}}$$

$$(x_{\mathfrak{p}_i} + \pi^{d_i}\mathcal{O}_{\mathfrak{p}_i})_i \mapsto (s_{\mathfrak{p}_i} x_{\mathfrak{p}_i} + \pi^{d_i}\mathcal{O}_{K_{\mathfrak{p}_i}})_i.$$

For these to agree, we need for all i

$$x_{\mathfrak{p}_i} \equiv s_{\mathfrak{p}_i} x_{\mathfrak{p}_i} \mod \pi^{d_i} \text{ for all } x_{\mathfrak{p}_i} \in \pi^{d_i - e_i}\mathcal{O}_{\mathfrak{p}},$$

which is equivalent to

$$v_{\mathfrak{p}_i}((s_{\mathfrak{p}_i} - 1)x_{\mathfrak{p}_i}) \geq d \text{ for all } x_{\mathfrak{p}_i} \text{ such that } v_{\mathfrak{p}_i}(x_{\mathfrak{p}_i}) \geq d - e,$$

i.e.

$$v_{\mathfrak{p}_i}(s_{\mathfrak{p}_i} - 1) \geq e.$$

Therefore $s\cdot, \varphi$ are isomorphic on $\mathfrak{c}$-torsion iff $v_{\mathfrak{p}}(s_{\mathfrak{p}} - 1) \geq v_{\mathfrak{p}}(\mathfrak{c})$ for all $\mathfrak{p}$ dividing $\mathfrak{c}$, which is equivalent to $s \in \mathbb{I}_{\mathfrak{c}}$. □

Remark Given an idele s and an ideal $\mathfrak{c}$, we can always find $\alpha \in K$ such that $s\alpha^{-1} \in \mathbb{I}_{\mathfrak{c}}$:

- $\alpha \equiv s_{\mathfrak{p}} \mod \mathfrak{p}^e$ for all $\mathfrak{p}$ dividing $\mathfrak{c}$
- $\alpha \in \mathcal{O}_{\mathfrak{p}}$ for all $\mathfrak{p}$ not dividing $\mathfrak{c}$

By strong approximation theorem, we can find a $\alpha \in K$ that satisfies all the congruence relations at the same time. This then gives the α we want. So $s\alpha^{-1}\cdot$ acts as multiplication by 1 on $\mathfrak{c}$-torsion, and so $s\cdot$ acts as multiplication by α. (Note that the multiplication-by-1 map need not be an isomorphism of complex tori, as the lattices $\mathfrak{a}, \mathfrak{d}^{-1}\mathfrak{a}$ may differ. However, it is an isomorphism when we reduce to the $\mathfrak{c}$-torsion.)

6 Class field theory

6.1 Frobenius elements

Let L/K be a finite Galois extension of number fields. Let $\mathfrak{p}$ be an unramified prime of K, and $\mathfrak{P}$ a prime of L lying over $\mathfrak{p}$. Recall that we get a Frobenius element $(\mathfrak{P}, L/K) \in \mathrm{Gal}(L/K)$, characterised as the unique element such that

$$(\mathfrak{P}, L/K)(x) \equiv x^{\mathrm{Nm}\,\mathfrak{p}} \mod \mathfrak{P} \quad \forall x \in \mathcal{O}_L.$$

What would we get if we had picked another prime $\mathfrak{P}'$ of L instead?

Let τ be an automorphism of $\mathrm{Gal}(L/K)$ sending $\mathfrak{P}$ to $\mathfrak{P}'$. Then

$$\tau(\mathfrak{P}, L/K)(x) - \tau(x) \in \mathfrak{P}' \quad \forall x \in \mathcal{O}_L,$$

so

$$\tau(\mathfrak{P}, L/K)\tau^{-1}(x) - x \in \mathfrak{P}' \quad \forall x \in \mathcal{O}_L.$$

Therefore $\sigma_{\mathfrak{P}'} = \tau(\mathfrak{P}, L/K)\tau^{-1}$.

Definition 6.1. Let L/K be a finite Galois extension of number fields, and let $\mathfrak{p}$ be an unramified prime of K.

Then we define $(\mathfrak{p}, L/K)$ to be the set

$$(\mathfrak{p}, L/K) = \{(\mathfrak{P}, L/K) \mid \mathfrak{P} \text{ a prime of } L \text{ lying over } \mathfrak{p}\}.$$

This is a conjugacy class of $\mathrm{Gal}(L/K)$, since $\mathrm{Gal}(L/K)$ acts transitively on the primes of L lying over $\mathfrak{p}$.

Here is a very powerful theorem on what values $(\mathfrak{p}, L/K)$ can take that will prove useful later.

Theorem 6.2 (Chebotarev density theorem)**.** *Let C be a conjugacy class of $\mathrm{Gal}(L/K)$. Then the density of primes $\mathfrak{p}$ of K such that $(\mathfrak{p}, L/K) = C$ is $|C|/|\mathrm{Gal}(L/K)|$. In particular, there are infinitely many such primes.*

Example. Consider the case $L = \mathbb{Q}(\zeta_n), K = \mathbb{Q}$. Then $\mathrm{Gal}(L/\mathbb{Q}) \cong (\mathbb{Z}/n\mathbb{Z})^\times$, with an isomorphism given by

$$F : a \bmod n \mapsto (\zeta_n \mapsto \zeta_n^a).$$

Note this is abelian, so all conjugacy classes have size 1.

The unramified primes of $\mathbb{Q}$ are the primes coprime to n, and the Frobenius element for an unramified prime p is given by

$$(p, L/\mathbb{Q})(x) \equiv x^p \mod \mathfrak{P} \quad \forall x \in \mathcal{O}_L$$

where $\mathfrak{P}$ is a prime of L lying over p.

The element

$$F(p \bmod n) : \zeta_n \mapsto \zeta_n^p$$

satisfies the above equation, so

$$(p, L/\mathbb{Q}) = F(p).$$

The Chebotarev density theorem, in this case, tells us that for each element $\sigma \in \mathrm{Gal}(L/\mathbb{Q})$ there are infinitely many primes p such that $F(p) = \sigma$. In other words, for each $a \in (\mathbb{Z}/n\mathbb{Z})^\times$ there are infinitely many primes p that are congruent to a modulo n, which is Dirichlet's theorem on primes in arithmetic progressions.

One particularly special case is when L/K is abelian, as conjugation does not change $(\mathfrak{P}, L/K)$. So the automorphism $(\mathfrak{P}, L/K)$ is independent of the choice of $\mathfrak{P}$, and only depends on the (unramified) prime $\mathfrak{p}$ of K. Therefore, we can reinterpret $(\mathfrak{p}, L/K)$ to be an element of $\mathrm{Gal}(L/K)$, rather than a subset.

6.2 The Artin map

Definition 6.3. Define the following:

- Let I_K be the group of fractional ideals of K.
- Suppose S be a finite set of primes of K. Then define I_K^S to be the subgroup of I_K generated by the primes not in S.

Let L/K be an abelian extension. We can then extend the map

$$\mathfrak{p} \mapsto (\mathfrak{p}, L/K)$$

to a group homomorphism from I_K^S to $\mathrm{Gal}(L/K)$.

Definition 6.4. Let L/K be a finite abelian extension of number fields, and let S be the set of primes of K that ramify. The *Artin map* for L/K is the unique group homomorphism $I_K^S \to \mathrm{Gal}(L/K)$ sending each unramified prime $\mathfrak{p}$ to its Frobenius element:

$$(\cdot, L/K) : I_K^S \to \mathrm{Gal}(L/K)$$

$$(\mathfrak{a}, L/K) = \left(\prod_i \mathfrak{p}_i^{e_i}, L/K\right) = \prod_i (\mathfrak{p}_i, L/K)^{e_i}.$$

Note that the order of $(\mathfrak{p}, L/K) = (\mathfrak{P}, L/K)$ is equal to $[k_{\mathfrak{P}} : k_{\mathfrak{p}}] = f$, and $\mathrm{Nm}_{L/K}(\mathfrak{P}) = \mathfrak{p}^f$. So we have

$$(\mathrm{Nm}_{L/K}(\mathfrak{P}), L/K) = 1$$

for all unramified primes $\mathfrak{P}$ of L.

Therefore, if T is the set of all unramified primes of L, we have

$$\mathrm{Nm}_{L/K}(I_L^T) \subseteq \ker(\cdot, L/K).$$

6.3 Statements of class field theory

Class field theory is the study of abelian extensions of a field K. Of particular importance is the maximal abelian extension of K. In this section, we will state the main results of class field theory; for proofs, refer to [2].

Let $\bar{K}$ be an algebraic closure of K. Note that if $L, L' \subseteq \bar{K}$ are abelian extensions of K, then $LL' \subseteq \bar{K}$ is also an abelian extension of K. Hence, we can define

Definition 6.5. K^{ab}, the maximal abelian extension of K, is the union of all abelian extensions $L \subseteq \bar{K}$ of K.

6.3.1 Local class field theory

Let $\mathcal{L}/\mathcal{K}$ be an extension of local fields.

Recall that if $\mathcal{L}/\mathcal{K}$ is an unramified extension, then the Frobenius element $\mathrm{Fr} \in \mathrm{Gal}(k_{\mathcal{L}}/k_{\mathcal{K}})$ lifts to a unique element of $\mathrm{Gal}(\mathcal{L}/\mathcal{K})$, which we will denote by $\mathrm{Fr}_{\mathcal{L}/\mathcal{K}}$.

Theorem 6.6 (Local reciprocity law)**.** *There is a unique homomorphism (the local reciprocity map)*

$$[\cdot, \mathcal{K}] : \mathcal{K}^\times \to \mathrm{Gal}(\mathcal{K}^{ab}/\mathcal{K})$$

with the following properties:

- *If π is a uniformiser of $\mathcal{K}$ and $\mathcal{L}/\mathcal{K}$ is a finite unramified extension, then*

$$[\pi, \mathcal{L}/\mathcal{K}] = \mathrm{Fr}_{\mathcal{L}/\mathcal{K}}\,.$$

- *If $\mathcal{L}/\mathcal{K}$ is a finite abelian extension, then the local reciprocity map composed with restriction $\mathrm{Gal}(\mathcal{K}^{ab}/\mathcal{K}) \to \mathrm{Gal}(\mathcal{L}/\mathcal{K})$, which we write as $[\cdot, \mathcal{L}/\mathcal{K}]$, has kernel $\mathrm{Nm}(\mathcal{L}^\times)$.*
  Furthermore, it induces an isomorphism

$$\mathcal{K}^\times / \mathrm{Nm}(\mathcal{L}^\times) \to \mathrm{Gal}(L/K).$$

(Here Nm is the norm map $\mathrm{Nm}_{\mathcal{L}/\mathcal{K}} : \mathcal{L}^\times \to \mathcal{K}^\times$.)

Theorem 6.7 (Local existence theorem)**.** *For every open subgroup N of $\mathcal{K}^\times$ of finite index, there exists a (unique) finite abelian extension $\mathcal{L}/\mathcal{K}$ such that*

$$\mathrm{Nm}(\mathcal{L}^\times) = N.$$

Remark. If $\mathcal{K}$ is archimedean, the local reciprocity map is very simple:

- $[\cdot, \mathbb{C}] : \mathbb{C}^\times \to \mathrm{Gal}(\mathbb{C}/\mathbb{C})$ is the constant map.

- $[\cdot, \mathbb{R}] : \mathbb{R}^\times \to \mathrm{Gal}(\mathbb{C}/\mathbb{R})$ is the map

$$x \mapsto \begin{cases} id & x > 0 \\ \text{complex conjugation} & x < 0 \end{cases}.$$

There are no uniformisers or Frobenius elements, but the second part of the local reciprocity law still holds.

In the case where $\mathcal{L}/\mathcal{K}$ is unramified, the map $[\cdot, \mathcal{L}/\mathcal{K}]$ has a simple explicit description: note that

$$\mathrm{Nm}(\mathcal{O}_\mathcal{L}^\times) = \mathcal{O}_\mathcal{K}^\times,$$

so $[\cdot, \mathcal{L}/\mathcal{K}]$ is the identity on $\mathcal{O}_\mathcal{K}^\times$. Combining this with the fact $[\pi, \mathcal{L}/\mathcal{K}] = \mathrm{Fr}_{\mathcal{L}/\mathcal{K}}$ gives

$$[x, \mathcal{L}/\mathcal{K}] = \mathrm{Fr}_{\mathcal{L}/\mathcal{K}}^{v_\mathcal{K}(x)}.$$

The unramified extensions $\mathcal{L}/\mathcal{K}$ make up all the extensions with $U_\mathcal{K}^{(0)} = \mathcal{O}_\mathcal{K}^\times \subseteq \mathrm{Nm}(\mathcal{L}^\times)$. For the ramified extensions, we will instead have $U_\mathcal{K}^{(n)} \subseteq \mathrm{Nm}(\mathcal{L}^\times)$ for some $n > 0$.

6.3.2 Global class field theory

We use this local reciprocity map $[\cdot, K_\mathfrak{p}]$ to define the global reciprocity map. First, we define a map $\mathbb{I}_K \to \mathrm{Gal}(L/K)$ for each finite abelian extension L/K.

Proposition 6.8. *Let L/K be a finite abelian extension of number fields. Then there is a continuous map*

$$[\cdot, L/K] : \mathbb{I}_K \to \mathrm{Gal}(L/K)$$

given by

$$[s, L/K] = \prod_v [s_v, L_w/K_v],$$

where v ranges over places of K, and for each v, w is a place of L lying over v.

Proof. Any two places w, w' of L lying over the same place v of K will be Galois conjugates of each other. So

$$[s_v, L_w/K_v] = [s_v, L_{w'}/K_v],$$

and so $[s_v, L_w/K_v]$ is independent of the choice of w.

Next, note that $[s_\mathfrak{p}, L_\mathfrak{P}/K_\mathfrak{p}] = 1$ for all $\mathfrak{p}$ unramified such that $v_\mathfrak{p}(s_\mathfrak{p}) = 0$. This is true for all but finitely many $\mathfrak{p}$, so the product given is finite.

Next, to show this is continuous, we construct a modulus $\mathfrak{m}$ in the following way: for each place v of K, we pick an integer $\mathfrak{m}(v)$ such that

$$U_{K_v}^{(\mathfrak{m}(v))} \subseteq \ker[\cdot, L_w/K_v].$$

If $v = \mathfrak{p}$ is a ramified prime, then we must pick $\mathfrak{m}(\mathfrak{p}) > 0$. On the other hand, if $v = \mathfrak{p}$ is an unramified prime, then we will pick $\mathfrak{m}(\mathfrak{p}) = 0$, as

$$U_{K_\mathfrak{p}}^{(0)} \subseteq \ker[\cdot, L_\mathfrak{P}/K_\mathfrak{p}].$$

Hence $\mathfrak{m}(\mathfrak{p})$ is zero for all but finitely many primes, and so it really does define a modulus.

Then, for all $s \in W_\mathfrak{m}$, we will have

$$[s, L/K] = \prod_v [s_v, L_w/K_v] = \prod_v 1 = 1.$$

This shows that the kernel contains $W_\mathfrak{m}$, so it's open. Hence the map is continuous. □

These maps $[\cdot, L/K]$ are compatible with each other: if $L \subseteq L'$ are abelian Galois extensions of K, then

$$[s, L'/K]|_L = [s, L/K]$$

for all ideles $s \in \mathbb{I}_K$. Therefore, we can define

Definition 6.9. The *global reciprocity map* $[\cdot, K] : \mathbb{I}_K \to \mathrm{Gal}(K^{ab}/K)$ is the (unique) homomorphism such that

$$[s, K]|_L = [s, L/K]$$

for all finite abelian Galois extensions L/K and all $s \in \mathbb{I}_K$.

It is the unique homomorphism such that for all places v of K, abelian extensions L/K, and places w of L lying over v, the following diagram commutes:

$$\begin{array}{ccccc} K_v^\times & \xrightarrow{[\cdot, K_v]} & \mathrm{Gal}(K_v^{ab}/K_v) & \longrightarrow & \mathrm{Gal}(L_w/K_v) \\ \downarrow & & & & \downarrow \\ \mathbb{I}_K & \xrightarrow{[\cdot, K]} & \mathrm{Gal}(K^{ab}/K) & \longrightarrow & \mathrm{Gal}(L/K) \end{array}$$

It's also continuous because each of the maps $[\cdot, L/K]$ are continuous.

Let Nm be the map

$$\begin{aligned} \mathbb{I}_L &\to \mathbb{I}_K \\ (s_w)_w &\mapsto \left(\prod_{w|v} \mathrm{Nm}_{L_w/K_v}(s_w) \right)_v . \end{aligned}$$

Theorem 6.10 (Global reciprocity law)**.** *The global reciprocity map $[\cdot, K] : \mathbb{I}_K \to \mathrm{Gal}(K^{ab}/K)$ has the following properties:*

- *$[\cdot, K]$ is surjective.*
- *$K^\times$ is contained in the kernel of $[\cdot, K]$.*
- *The map*

  $$[\cdot, L/K] : \mathbb{I}_K \to \mathrm{Gal}(L/K)$$

  is surjective, and has kernel $K^\times \mathrm{Nm}(\mathbb{I}_L)$.
  So it induces an isomorphism

  $$\mathbb{I}_K / K^\times \mathrm{Nm}(\mathbb{I}_L) \to \mathrm{Gal}(L/K).$$

Theorem 6.11 (Global existence theorem)**.** *For every open subgroup $N \subset \mathbb{I}_K$ of finite index containing $K^\times$, there exists a unique finite abelian extension L/K such that*

$$K^\times \mathrm{Nm}(\mathbb{I}_L) = N.$$

6.4 Ideal-theoretic formulation of global class field theory

The ideal-theoretic formulation of global class field theory uses the ideal groups I_K, I_L and the Artin map $(\cdot, L/K)$ instead of the idele groups and the global reciprocity map $[\cdot, K]$ to state the main theorems. In this section, we will use the idele-theoretic formulations to deduce the ideal-theoretic versions.

First, we show how the global reciprocity map and the Artin map are related.

Proposition 6.12. *Let L/K be a finite abelian extension. Then there exists a modulus $\mathfrak{m}$ such that*

- *The primes dividing* $\mathfrak{m}$ *are precisely those that ramify in* L/K.
- $[s, L/K] = 1$ *for all* $s \in W_{\mathfrak{m}}$.
- $[s, L/K] = ((s), L/K)$ *for all* $s \in \mathbb{I}_{\mathfrak{m}}$.

Such a modulus $\mathfrak{m}$ *is called a* defining modulus *for* L/K.

Proof. Recall in the proof of Proposition 6.8 that we constructed a modulus $\mathfrak{m}$, divisible by precisely the ramified primes of K, such that $W_{\mathfrak{m}} \subseteq \ker[\cdot, L/K]$.

Given $s \in \mathbb{I}_{\mathfrak{m}}$, we can calculate $[s, L/K]$ in terms of the Artin map. Note that we have $s_v \in U_{K_v}^{(\mathfrak{m}(v))}$ for all v infinite and all $v = \mathfrak{p}$ ramified, so $[s_v, L_w/K_v] = 1$ for these places.

Therefore

$$\begin{aligned}
[s, L/K] &= \prod_v [s, L_w/K_v] \\
&= \prod_{\mathfrak{p} \text{ unramified}} [s_{\mathfrak{p}}, L_{\mathfrak{P}}/K_{\mathfrak{p}}] \\
&= \prod_{\mathfrak{p} \text{ unramified}} \mathrm{Fr}_{L_{\mathfrak{P}}/K_{\mathfrak{p}}}^{v_{\mathfrak{p}}(s_{\mathfrak{p}})} \\
&= \prod_{\mathfrak{p} \text{ unramified}} (\mathfrak{p}, L/K)^{v_{\mathfrak{p}}(s_{\mathfrak{p}})} \\
&= ((s), L/K)
\end{aligned}$$

□

Definition 6.13. Let $K_{\mathfrak{m},1} = K^\times \cap \mathbb{I}_{\mathfrak{m}}$. This is the set of all $\alpha \in K^\times$ such that $\alpha \in U_{K_v}^{(\mathfrak{m}(v))}$ for all v dividing $\mathfrak{m}$, i.e. the α satisfying

- $v_{\mathfrak{p}}(\alpha - 1) \geq \mathfrak{m}(\mathfrak{p})$ for all finite places $\mathfrak{p}$ dividing $\mathfrak{m}$
- $\sigma(\alpha) > 0$ for all real places $\sigma : K \to \mathbb{R}$ dividing $\mathfrak{m}$

Lemma 6.14.

$$\mathbb{I}_{\mathfrak{m}}/K_{\mathfrak{m},1} \cong \mathbb{I}_K/K^\times.$$

Proof. The kernel of the map $\mathbb{I}_{\mathfrak{m}} \to \mathbb{I}_K/K^\times$ is $K^\times \cap \mathbb{I}_{\mathfrak{m}} = K_{\mathfrak{m},1}$, so we get an injective map

$$\mathbb{I}_{\mathfrak{m}}/K_{\mathfrak{m},1} \to \mathbb{I}_K/K^\times.$$

So we just need to show that this map is surjective, i.e. for any $s \in \mathbb{I}_K$ there exists $t \in \mathbb{I}_{\mathfrak{m}}$ and $\alpha \in K^\times$ such that $s = t\alpha$.

By strong approximation theorem, there exists $\alpha \in K^\times$ such that

- $\alpha \equiv s_{\mathfrak{p}} \mod \mathfrak{p}^{\mathfrak{m}(\mathfrak{p})}$ for all $\mathfrak{p} \in S$,
- α, s_v have the same sign for all real places v dividing $\mathfrak{m}$.

This then gives $t = \alpha^{-1}s \in \mathbb{I}_{\mathfrak{m}}$, so we are done. □

Remark. This allows us to express $[s, L/K]$ in terms of the Artin map for all $s \in \mathbb{I}_K$: we write $s = \alpha t$ for some $\alpha \in K^\times$ and $t \in \mathbb{I}_{\mathfrak{m}}$, where $\mathfrak{m}$ is as in Proposition 6.12. Then $[s, L/K] = ((t), L/K)$.

Theorem 6.15 (Reciprocity law, ideal-theoretic version)**.** *Let* L/K *be a finite abelian extension. Let* S *be the set of primes of* K *that ramify, and let* T *be the set of primes of* L *lying over the primes in* K. *Then there exists a modulus* $\mathfrak{m}$ *divisible precisely by the ramified primes such that*

$$((\alpha), L/K) = 1 \quad \forall \alpha \in K_{\mathfrak{m},1},$$

i.e. $K_{\mathfrak{m},1} \subseteq \ker(\cdot, L/K)$.

Furthermore, the Artin map $(\cdot, L/K) : I_K^S \to \mathrm{Gal}(L/K)$ *is surjective, and it has kernel* $K_{\mathfrak{m},1} \operatorname{Nm}(I_L^S)$. *So it induces an isomorphism*

$$I_K^S/K_{\mathfrak{m},1} \operatorname{Nm}(I_L^T) \to \mathrm{Gal}(L/K).$$

Proof. We use the modulus $\mathfrak{m}$ from the previous proposition. Then, for all $\alpha \in K_{\mathfrak{m},1}$, we have

$$\begin{aligned}((\alpha), L/K) &= [\alpha, L/K] && \text{since } \alpha \in \mathbb{I}_{\mathfrak{m}} \\ &= 1 && \text{since } \alpha \in K^\times.\end{aligned}$$

So $(\cdot, L/K)$ is trivial on $K_{\mathfrak{m},1}$. Hence the Artin map descends to a map

$$I_K^S/K_{\mathfrak{m},1} \to \mathrm{Gal}(L/K).$$

The global reciprocity law tells us that we have an exact sequence

$$\mathbb{I}_L/L^\times \xrightarrow{\mathrm{Nm}} \mathbb{I}_K/K^\times \xrightarrow{[\cdot, L/K]} \mathrm{Gal}(L/K) \longrightarrow 0.$$

We now want to apply Lemma 6.14 on the above sequence, but we have to make sure that the norm map is still well-defined. To deal with this, we define a modulus $\mathfrak{n}$ of L by

- For $\mathfrak{P}$ a prime of L lying over $\mathfrak{p}$ a prime of K, set $\mathfrak{n}(\mathfrak{P}) = f\mathfrak{m}(\mathfrak{p})$, where $\mathrm{Nm}(\mathfrak{P}) = \mathfrak{p}^f$.
- For w a real place of L lying over v a real place of K, set $\mathfrak{n}(w) = \mathfrak{m}(v)$.

Then we have $\mathrm{Nm}(\mathbb{I}_{\mathfrak{n}}) \subseteq \mathbb{I}_{\mathfrak{m}}$ and $\mathrm{Nm}(L_{\mathfrak{n},1}) \subseteq K_{\mathfrak{m},1}$, so the map $\mathrm{Nm} : \mathbb{I}_{\mathfrak{n}}/L_{\mathfrak{n},1} \to \mathbb{I}_{\mathfrak{m}}/K_{\mathfrak{m},1}$ is well-defined. Hence, by Lemma 6.14, we get an exact sequence

$$\mathbb{I}_{\mathfrak{n}}/L_{\mathfrak{n},1} \xrightarrow{\mathrm{Nm}} \mathbb{I}_{\mathfrak{m}}/K_{\mathfrak{m},1} \xrightarrow{[\cdot, L/K]} \mathrm{Gal}(L/K) \longrightarrow 0.$$

Now we extend this to form a commutative diagram.

$$\begin{array}{ccccccc}
\mathbb{I}_{\mathfrak{n}}/L_{\mathfrak{n},1} & \xrightarrow{\mathrm{Nm}} & \mathbb{I}_{\mathfrak{m}}/K_{\mathfrak{m},1} & \xrightarrow{[\cdot, L/K]} & \mathrm{Gal}(L/K) & \longrightarrow & 0 \\
\downarrow{\scriptstyle i} & & \downarrow{\scriptstyle i} & & \| & & \\
I_L^T/L_{\mathfrak{n},1} & \xrightarrow{\mathrm{Nm}} & I_K^S/K_{\mathfrak{m},1} & \xrightarrow{(\cdot, L/K)} & \mathrm{Gal}(L/K) & \longrightarrow & 0.
\end{array}$$

This diagram commutes, because:

- The leftmost square commutes by definition of the idele norm map.
- The middle square commutes by Proposition 6.12.

We now want to show that the bottom row is exact, as this will give the result we want.

- Exactness at $\mathrm{Gal}(L/K)$ is equivalent to surjectivity of $(\cdot, L/K)$, which follows from surjectivity of $[\cdot, L/K]$.
- To show exactness at $I_K^S/K_{\mathfrak{m},1}$, note that the maps i are surjective. Therefore

$$\begin{aligned}\ker(\cdot, L/K) &= i(\ker[\cdot, L/K]) \\ &= i(\mathrm{Nm}(\mathbb{I}_{\mathfrak{n}}/L_{\mathfrak{n},1})) \\ &= \mathrm{Nm}(i(\mathbb{I}_{\mathfrak{n}}/L_{\mathfrak{n},1})) \\ &= \mathrm{Nm}(I_L^T/L_{\mathfrak{n},1}).\end{aligned}$$

So we're done. □

Theorem 6.16 (Existence theorem, ideal-theoretic version)**.** *Let $\mathfrak{m}$ be a modulus and let S be the set of primes dividing $\mathfrak{m}$. Let H be a subgroup of I_K^S containing $K_{\mathfrak{m},1}$. Then there exists a finite abelian extension L/K, unramified over all primes not dividing $\mathfrak{m}$, such that*

$$K_{\mathfrak{m},1}\,\mathrm{Nm}(I_L^T) = H,$$

where T is the set of all primes of L lying over a prime in S.

Proof. Define $N' \subseteq \mathbb{I}_\mathfrak{m}$ as the preimage of H under the ideal map $i : \mathbb{I}_\mathfrak{m} \to I_K^S$:

$$N' = i^{-1}(H) = \{s \in \mathbb{I}_\mathfrak{m} \mid (s) \in H\}.$$

Note that $i^{-1}(1) = W_\mathfrak{m} \subseteq N'$.

The preimage of $H/K_{\mathfrak{m},1}$ under $i : \mathbb{I}_\mathfrak{m}/K_{\mathfrak{m},1} \to I_K^S/K_{\mathfrak{m},1}$ is therefore

$$i^{-1}(H/K_{\mathfrak{m},1}) = N'/K_{\mathfrak{m},1}.$$

Next, define $N = K^\times N' \subseteq \mathbb{I}_K$, so that

$$N'/K_{\mathfrak{m},1} \to N/K^\times$$

is an isomorphism.

N contains $K^\times W_\mathfrak{m}$, so it's an open subgroup of $\mathbb{I}_K$ of finite index, and hence by existence theorem, there is some finite abelian field extension L/K such that $N = K^\times \operatorname{Nm}(\mathbb{I}_L)$, i.e. N is the kernel of $[\cdot, L/K]$. Since $[W_\mathfrak{m}, L/K] = 1$, we get that L/K is unramified over all primes not dividing $\mathfrak{m}$, and so $(\cdot, L/K)$ is defined on I_K^S.

But now we can convert back into a statement about ideals, obtaining

$$\begin{aligned}
\ker\big([\cdot, L/K] : \mathbb{I}_K/K^\times \to \operatorname{Gal}(L/K)\big) &= N/K^\times \\
\ker\left([\cdot, L/K] : \mathbb{I}_\mathfrak{m}/K_{\mathfrak{m},1} \to \operatorname{Gal}(L/K)\right) &= N'/K_{\mathfrak{m},1} \\
\ker\big((\cdot, L/K) : I_K^S/K_{\mathfrak{m},1} \to \operatorname{Gal}(L/K)\big) &= H/K_{\mathfrak{m},1} \\
\ker\big((\cdot, L/K) : I_K^S \to \operatorname{Gal}(L/K)\big) &= H
\end{aligned}$$

which, by the previous theorem, tells us $K_{\mathfrak{m},1} \operatorname{Nm}(I_L^T) = H$. □

6.5 Ray class fields

A particularly important case in the existence theorem is when we take $H = K_{\mathfrak{m},1}$. In the idelic formulation, this corresponds to taking $N = K^\times W_\mathfrak{m}$.

Definition 6.17. The *ray class field modulo* $\mathfrak{m}$, denoted $K_\mathfrak{m}$, is the finite abelian extension corresponding to the open subgroup $K^\times W_\mathfrak{m} \subseteq \mathbb{I}_K$.

Every finite abelian extension L has a defining modulus, hence is contained in a ray class field $K_\mathfrak{m}$ for some $\mathfrak{m}$. The smallest $\mathfrak{m}$ for which $L \subseteq K_\mathfrak{m}$ is called the *conductor* of L.

Because of this, the maximal abelian extension K^{ab} is the union of all the ray class fields.

Definition 6.18. The smallest ray class field is $K_{(1)}$, the ray class field modulo (1). This is called the *Hilbert class field*, and it is the maximal abelian extension that is unramified at all places (both finite and infinite).

The degree of the Hilbert class field is

$$\begin{aligned}
|\operatorname{Gal}(K_{(1)}/K)| &= |\mathbb{I}_K/K^\times W| \\
&= |I_K/K^\times| \\
&= |\mathcal{C}\ell(\mathcal{O}_K)| \\
&= h_K.
\end{aligned}$$

7 Main theorem of complex multiplication

First, we need a small lemma on the infinitude of primes satisfying a certain set of conditions. This follows from the Chebotarev density theorem.

Lemma 7.1. *Let $L/K/\mathbb{Q}$ be finite extensions, with L, K Galois over $\mathbb{Q}$ (so L/K is Galois too). Let $\sigma \in \operatorname{Gal}(L/K)$. Then there are infinitely many primes $\mathfrak{P}$ of L such that*

- $(\mathfrak{P}, L/K) = \sigma$
- $\mathfrak{p} = \mathfrak{P} \cap K$ *is a degree 1 prime.*

Proof. First note that σ is also an element of $\mathrm{Gal}(L/\mathbb{Q})$. Let C be the conjugacy class of σ in $\mathrm{Gal}(L/\mathbb{Q})$.

Suppose p satisfies $(p, L/\mathbb{Q}) = C$. Then there is some prime $\mathfrak{P}$ of L lying over p such that $(\mathfrak{P}, L/\mathbb{Q}) = \sigma \in C$. This $\mathfrak{P}$ satisfies

$$\sigma(x) \equiv x^p \mod \mathfrak{P} \quad \forall x \in \mathcal{O}_L,$$

so $(\mathfrak{P}, L/K) = \sigma$.

Next, let $\mathfrak{p} = \mathfrak{P} \cap K$. σ fixes K, so we have

$$x = \sigma|_K(x) \equiv x^p \mod \mathfrak{p} \quad \forall x \in \mathcal{O}_K.$$

This says that Fr_p acts trivially on $\mathcal{O}_K/\mathfrak{p}$, which tells us that $\mathfrak{p}$ is a degree 1 prime. This therefore shows that $\mathfrak{P}$ satisfies the conditions required.

By Chebotarev density theorem, there exist infinitely many primes p of $\mathbb{Q}$ such that $(p, L/\mathbb{Q}) = C$. Hence there are infinitely many $\mathfrak{P}$ satisfying the conditions. □

Now we are ready to prove the main theorem of complex multiplication, stated below.

Theorem 7.2 (Main theorem of complex multiplication)**.** *Given the following:*

- *an elliptic curve E with complex multiplication by $\mathcal{O}_K$*
- *a fractional ideal $\mathfrak{a}$ of K and a complex analytic isomorphism $f : \mathbb{C}/\mathfrak{a} \to E$*
- *an automorphism $\sigma \in Aut(\mathbb{C})$ fixing K*
- *an idele $s \in \mathbb{I}_K$ such that the global reciprocity map $[s, K]$ agrees with $\sigma|_{K^{ab}}$*

there exists a complex analytic isomorphism

$$f' : \mathbb{C}/s^{-1}\mathfrak{a} \to E^\sigma$$

making the following diagram commute:

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

Proof. First we reduce to the case where $E = E_{\bar{\mathfrak{a}}} \in \mathrm{Ell}(\mathcal{O}_K)$. This will allow us to use our results from Section 3.

Recall that $f_{\mathfrak{a}} : \mathbb{C}/\mathfrak{a} \to E_{\bar{\mathfrak{a}}}$ is an isomorphism. Suppose we know the result for $E_{\bar{\mathfrak{a}}}, f_{\mathfrak{a}}$. Then define $\phi = f \circ f_{\mathfrak{a}}^{-1}$. This gives an isomorphism of elliptic curves $E_{\bar{\mathfrak{a}}} \to E$. We then get the following diagram:

$$\begin{array}{ccc} K/\mathfrak{a} & \xrightarrow{s^{-1}} & K/s^{-1}\mathfrak{a} \\ \downarrow{\scriptstyle f_{\mathfrak{a}}} & & \downarrow{\scriptstyle (f_{\mathfrak{a}})'} \\ E_{\bar{\mathfrak{a}}}(\mathbb{C}) & \xrightarrow{\sigma} & (E_{\bar{\mathfrak{a}}})^\sigma(\mathbb{C}) \\ \downarrow{\scriptstyle \phi} & & \downarrow{\scriptstyle \phi^\sigma} \\ E(\mathbb{C}) & \xrightarrow{\sigma} & E^\sigma(\mathbb{C}) \end{array} \qquad f$$

Then we can set $f' = \phi^\sigma \circ (f^*)'$. So it suffices to prove the theorem for $E = E_{\bar{\mathfrak{a}}}, f = f_{\mathfrak{a}}$.

We will prove the existence of such an f' on $\mathfrak{c}$-torsion points, and then show that they are all the same f'. First, we need to choose a finite extension L/K that is Galois over $\mathbb{Q}$ (and hence K), and satisfies the statement of Proposition 2.11. Also pick L to be big enough to contain the ray class field $K_{(\mathfrak{c})}$.

Next, pick a prime $\mathfrak{P}$ of L satisfying the following properties:

i) $(\mathfrak{P}, L/K) = \sigma|_L$

ii) $\mathfrak{p} = \mathfrak{P} \cap K$ is a degree 1 prime.

iii) $\mathfrak{P}$ is a prime of good reduction for E.

iv) For all $\bar{\mathfrak{a}} \neq \bar{\mathfrak{a}}' \in \mathcal{Cl}(\mathcal{O}_K)$, we have $v_{\mathfrak{P}}(j(E_{\bar{\mathfrak{a}}}) - j(E_{\bar{\mathfrak{a}}'})) = 0$.

v) $\mathfrak{p}$ does not divide $\mathfrak{c}$.

Such a prime $\mathfrak{P}$ exists, because by Lemma 7.1 there are infinitely many primes satisfying (i), (ii), and there are only finitely many primes that do not satisfy (iii), (iv), (v).

We have

$$[s, K]|_{K_\mathfrak{c}} = \sigma|_{K_\mathfrak{c}} = (\mathfrak{p}, K_\mathfrak{c}/K).$$

Let π be the idele with a uniformiser in position $\mathfrak{p}$ and 1 everywhere else. Then $[\pi, K]|_{K_\mathfrak{c}} = (\mathfrak{p}, K_\mathfrak{c})$ by construction of the global reciprocity map, so we get

$$[s, K]|_{K_\mathfrak{c}} = [\pi, K]_{K_\mathfrak{c}}.$$

But the kernel of $[\cdot, K]_{K_\mathfrak{c}}$ is $K^* W_\mathfrak{c}$ by definition of ray class field. So we deduce

$$s = \pi \alpha u$$

for some $\alpha \in K^*, u \in W_\mathfrak{c}$. Taking ideals of both sides then gives $(s) = \alpha\mathfrak{p}$, so we learn that

$$C/s^{-1}\mathfrak{a} = \mathbb{C}/\alpha^{-1}\mathfrak{p}^{-1}\mathfrak{a}.$$

By assumption, $\mathfrak{p}$ does not divide $\mathfrak{c}$, so we have $\pi_\mathfrak{q} = 1$ for all $\mathfrak{q}$ dividing $\mathfrak{c}$. Hence $\pi \in \mathbb{I}_\mathfrak{c}$. Also, $u \in W_\mathfrak{c} \subseteq \mathbb{I}_\mathfrak{c}$. So

$$s\alpha^{-1} = \pi u \in \mathbb{I}_\mathfrak{c}.$$

We begin constructing f' by first taking the commutative square

$$\begin{array}{ccc} \mathbb{C}/\mathfrak{a} & \xrightarrow{\varphi_\mathfrak{p}} & \mathbb{C}/\mathfrak{p}^{-1}\mathfrak{a} \\ {\scriptstyle f_\mathfrak{a}}\downarrow\sim & & {\scriptstyle f_{\mathfrak{p}^{-1}\mathfrak{a}}}\downarrow\sim \\ E(\mathbb{C}) & \xrightarrow{\phi_\mathfrak{p}} & (\bar{\mathfrak{p}} * E)(\mathbb{C}) \end{array}$$

By Lemma 3.5, we can extend the isogeny $E \to \bar{\mathfrak{p}} * E$ by an isomorphism $\theta : \bar{\mathfrak{p}} * E \to E^\sigma$ such that the composition $\lambda = \theta \circ \phi_\mathfrak{p}$ reduces to the p-Frobenius isogeny modulo $\mathfrak{P}$.

Also, multiplication by α^{-1} gives a complex analytic isomorphism

$$\vartheta_{\alpha^{-1}} : \mathbb{C}/\mathfrak{p}^{-1}\mathfrak{a} \to \mathbb{C}/s^{-1}\mathfrak{a}.$$

So we can compose the isomorphisms above to get a complex analytic isomorphism

$$f' = \theta \circ f_{\mathfrak{p}^{-1}\mathfrak{a}} \circ (\vartheta_{\alpha^{-1}})^{-1}.$$

This gives the commutative diagram

$$\begin{array}{ccccc} \mathbb{C}/\mathfrak{a} & \xrightarrow{\varphi_\mathfrak{p}} & \mathbb{C}/\mathfrak{p}^{-1}\mathfrak{a} & \xrightarrow{\vartheta_{\alpha^{-1}}} & \mathbb{C}/s^{-1}\mathfrak{a} \\ {\scriptstyle f_\mathfrak{a}}\downarrow & & {\scriptstyle f_{\mathfrak{p}^{-1}\mathfrak{a}}}\downarrow & & {\scriptstyle f'}\downarrow \\ E(\mathbb{C}) & \xrightarrow{\phi_\mathfrak{p}} & (\bar{\mathfrak{p}} * E)(\mathbb{C}) & \xrightarrow{\theta} & E^\sigma(\mathbb{C}) \end{array}$$

We now restrict our attention to the $\mathfrak{c}$-torsion points of $\mathbb{C}/\mathfrak{a}$. Note that all the $\mathfrak{c}$-torsion points of E, E^σ are defined over L.

But

$$\begin{array}{ccccc} (K/\mathfrak{a})[\mathfrak{c}] & \xrightarrow{\varphi_\mathfrak{p}} & (K/\mathfrak{p}^{-1}\mathfrak{a})[\mathfrak{c}] & \xrightarrow{\vartheta_{\alpha^{-1}}} & (K/s^{-1}\mathfrak{a})[\mathfrak{c}] \\ \downarrow{\scriptstyle f}\sim & & & & \downarrow{\scriptstyle f'}\sim \\ E[\mathfrak{c}] & & \xrightarrow{\theta\circ\phi_\mathfrak{p}} & & E^\sigma[\mathfrak{c}] \end{array}$$

- $\vartheta_{\alpha^{-1}}$ is the map $\alpha\cdot$.
- $\pi u \in \mathbb{I}_\mathfrak{c}$, so by Proposition 5.7, $\pi u\cdot$ acts the same as $\varphi_\mathfrak{p}$ on $\mathfrak{c}$-torsion.
- For all points $T \in E[\mathfrak{c}]$, we have

$$\widetilde{\theta \circ \phi_\mathfrak{p}(T)} = \widetilde{T}^{\mathrm{Fr}_p} = \widetilde{T^\sigma}.$$

  But $\mathfrak{P}$ does not divide $\mathfrak{c}$, so the reduction modulo $\mathfrak{P}$ map is injective on $\mathfrak{c}$-torsion, and so we deduce that $\theta \circ \phi_\mathfrak{p}, \sigma$ agree on $E[\mathfrak{c}]$.

Hence in fact the following diagram commutes:

$$\begin{array}{ccccc} (K/\mathfrak{a})[\mathfrak{c}] & \xrightarrow{\pi u\cdot} & (K/\mathfrak{p}^{-1}\mathfrak{a})[\mathfrak{c}] & \xrightarrow{\alpha\cdot} & (K/s^{-1}\mathfrak{a})[\mathfrak{c}] \\ \downarrow{\scriptstyle f}\sim & & & & \downarrow{\scriptstyle f'}\sim \\ E[\mathfrak{c}] & & \xrightarrow{\sigma} & & E^\sigma[\mathfrak{c}] \end{array}$$

The top row of this diagram combines to give the map $\alpha\pi u = s$, so this shows what we wanted for $\mathfrak{c}$-torsion.

Finally, we show that f' does not depend on our choice of $\mathfrak{c}$, provided we have $Nm(\mathfrak{c}) > 4$.

Suppose $\mathfrak{c}_1$ divides $\mathfrak{c}_2$, and the corresponding complex analytic isomorphisms we get from these two ideals are f_1', f_2'. Then $f_2' \circ (f_1')^{-1}$ is an isomorphism $E^\sigma \to E^\sigma$, so it is $[\zeta]$ for some $\zeta \in \mathcal{O}_K^\times$.

Note that $E^\sigma[\mathfrak{c}_1] \subseteq E^\sigma[\mathfrak{c}_2]$. So for all $T \in E^\sigma[\mathfrak{c}_1]$, we have $(f_2')^{-1}(T) = (f_1')^{-1}(T)$, implying $T = [\zeta]T$. Hence

$$[1-\zeta](T) = 0 \text{ for all } T \in E^\sigma[\mathfrak{c}_1].$$

But, if $\zeta \neq 1$, then

$$4 < |E^\sigma[\mathfrak{c}_1]| = |\ker[1-\zeta]| = \deg[1-\zeta] = \mathrm{Nm}(1-\zeta) = |1-\zeta|^2 \leq (|1|+|\zeta|)^2 = 4,$$

which is a contradiction. So we must have $\zeta = 1$, i.e. $f_1' = f_2'$.

Therefore, the map f' we defined satisfies

$$f'(s^{-1} \cdot x) = f(x)^\sigma$$

for all $x \in K/\mathfrak{a}$.

□

8 Generating abelian extensions of K

We now reap the rewards of our work in proving the main theorem of complex multiplication. First, we use it to describe explicitly the maximal abelian extension of K.

8.1 Hilbert class field

Recall that $\mathrm{Aut}(\mathbb{C}/K)$ acts on $\mathrm{Ell}(\mathcal{O}_K)$ by Galois conjugation. It also acts on the set

$$J = \{j(E) : E \in \mathrm{Ell}(\mathcal{O}_K)\}$$

in the same way.

Recall that the ideal class group $\mathcal{Cl}(\mathcal{O}_K)$ also acts on $\mathrm{Ell}(\mathcal{O}_K)$, via $\bar{\mathfrak{b}} * E_{\bar{\mathfrak{a}}} = E_{\bar{\mathfrak{b}}^{-1}\bar{\mathfrak{a}}}$. Moreover, this action is simply transitive. So we get a simply transitive action of $\mathcal{Cl}(\mathcal{O}_K)$ on J, defined by

$$\bar{\mathfrak{b}} * j(E_{\bar{\mathfrak{a}}}) = j(E_{\bar{\mathfrak{b}}^{-1}\bar{\mathfrak{a}}}).$$

The main theorem of complex multiplication allows us to relate the action of the ideal class group and the Galois group. Specifically, it tells us that

$$E_{\bar{\mathfrak{a}}}^{\sigma} = (\bar{s}) * E_{\bar{\mathfrak{a}}},$$

where s is an idele satisfying $[s, K] = \sigma|_{K^{ab}}$. In terms of j-invariants, this states

$$j^{\sigma} = (\bar{s}) * j$$

for all $j \in J$. So the Galois action is also transitive on J.

Proposition 8.1. *Let $H = K(J)$ be the field obtained from K by adjoining all elements of J. Then*

- *H is the Hilbert extension of K.*
- *$H = K(j)$ for any $j \in J$.*

Proof. H is Galois because J is closed under Galois conjugation.

Suppose $\sigma \in \mathrm{Aut}(\mathbb{C}/K)$ fixes K^{ab}, i.e. $\sigma|_{K^{ab}} = 1$. Then $j^{\sigma} = (1) * j$ for all $j \in J$, so σ fixes H. Hence H is an abelian extension of K.

For $s \in \mathbb{I}_K$ and $j \in j$, we have $j^{[s,K]} = j$ iff $(s) * j = j$, which happens iff (s) is principal, i.e. $s \in K^{\times}W$. Therefore $[s, K]|_H = 1$ iff $s \in K^{\times}W$, and so H is the Hilbert class field of K.

Since the Galois action on J is transitive, the degree of any $j \in J$ is $|J| = h_K$. So we get

$$[K(j) : K] = h_K.$$

But, since H is the Hilbert class field, we also have $[H : K] = h_K$. So by tower law, we have

$$[H : K(j)] = 1,$$

i.e. $H = K(j)$. □

Example. Consider the imaginary quadratic extension $\mathbb{Q}(\sqrt{-5})/\mathbb{Q}$. Note that $K = \mathbb{Q}(\sqrt{-5})$ has class number 2, so the Hilbert class field of K will be a degree 2 extension.

To find the j-invariant of an elliptic curve with complex multiplication by $\mathcal{O}_K$, we first pick a lattice homothetic to a fractional ideal of $\mathcal{O}_K$. The simplest choice in this case is to take

$$\Lambda = \mathcal{O}_K = \mathbb{Z}[\sqrt{-5}] = \mathbb{Z} \oplus \mathbb{Z}\sqrt{-5} = \Lambda_{\sqrt{-5}}.$$

Then the j-invariant of $\mathbb{C}/\Lambda$ is

$$j(\sqrt{-5}) = 320(1975 + 884\sqrt{5})$$

and so the Hilbert class field is

$$K(j(E)) = \mathbb{Q}(\sqrt{-5}, 320(1975 + 884\sqrt{5})) = \mathbb{Q}(i, \sqrt{5}).$$

8.2 Weber functions

Our next step is to describe ray class fields in terms of the torsion points of E. However, what we will find is that we can only determine what happens to the torsion points up to an overall automorphism $E \to E$. Weber functions provide a way for us to 'quotient out' this ambiguity.

Definition 8.2. A *Weber function* for an elliptic curve E over L is a morphism $h : E \to \mathbb{P}^1$ defined over L such that for all $P, P' \in E$

$$h(P) = h(P') \iff \exists\, \theta : E \to E \text{ an automorphism such that } \theta(P) = P'.$$

The automorphisms of E correspond to the invertible elements of $\mathcal{O}_K$, i.e. $\mathcal{O}_K^\times$. This group of automorphisms will depend on K, giving us 3 cases.

Let $E \in \mathrm{Ell}(\mathcal{O}_K)$, and let $j = j(E)$. Recall that E has equation

$$E : \begin{cases} y^2 = x^3 - \frac{3j}{j-1728}x + \frac{2j}{j-1728} & j \neq 0, 1728 \\ y^2 = x^3 + 1 & j = 0 \\ y^2 = x^3 + x & j = 1728 \end{cases}.$$

E is defined over $K(j) = H$ the Hilbert class field of K.

- If $K \neq \mathbb{Q}(i), \mathbb{Q}(\zeta_3)$, then $\mathcal{O}_K^\times = \{1, -1\}$. Then x is a Weber function for E over H, since

$$x(P) = x(P') \iff P' = \pm P.$$

- If $K = \mathbb{Q}(\zeta_3)$, then there is only one element of $\mathrm{Ell}(\mathcal{O}_K)$, and it is

$$E : y^2 = x^3 + 1.$$

  Here we have $\mathcal{O}_K^\times = \{1, \zeta_6, \ldots, \zeta_6^5\} \cong \mathbb{Z}/6\mathbb{Z}$, and the automorphisms of E are generated by

$$[\zeta_6] : (x, y) \mapsto (\zeta_3 x, -y).$$

  Then x^3 is a Weber function:

$$x(P)^3 = x(P')^3 \iff P' = [\zeta_6^k]P \text{ for some } k.$$

- If $K = \mathbb{Q}(i)$, then there is only one element of $\mathrm{Ell}(\mathcal{O}_K)$, and it is

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

  Here we have $\mathcal{O}_K^\times = \{1, i, -1, -i\} \cong \mathbb{Z}/4\mathbb{Z}$, and the automorphisms of E are generated by

$$[i] : (x, y) \mapsto (-x, iy).$$

  Then x^2 is a Weber function:

$$x(P)^2 = x(P')^2 \iff P' = [i^k]P \text{ for some } k.$$

In summary, a Weber function for $E \in \mathrm{Ell}(\mathcal{O}_K)$ is

$$h = \begin{cases} x & K \neq \mathbb{Q}(i), \mathbb{Q}(\zeta_3) \\ x^2 & K = \mathbb{Q}(i) \\ x^3 & K = \mathbb{Q}(\zeta_3) \end{cases}.$$

We can also give an analytic formula for a Weber function, by relating E to an isomorphic complex torus $\mathbb{C}/\Lambda$.

Recall that the elliptic curve E_Λ has equation

$$E_\Lambda : y'^2 = 4x'^3 - g_2(\Lambda)x' - g_3(\Lambda).$$

So E, E_Λ are related by the change of variables

$$x' = u^2 x, y' = 2u^3 y,$$

where

$$g_2(\Lambda) = \frac{12j}{j - 1728}u^4, \quad g_3(\Lambda) = \frac{-8j}{j - 1728}u^6.$$

If we want a Weber function for E defined over H, we are free to scale by any constant in $H^\times$, so we only need to keep track of things modulo $H^\times$.

- The complex analytic isomorphism $f : \mathbb{C}/\Lambda \to E_\Lambda$ sends z to $(\wp(z), \wp'(z))$. So $x' = \wp(z)$.
- For $j \neq 0, 1728$, we have $g_3(\Lambda)/g_2(\Lambda) \in u^2 H^\times$.
- For $j \neq 0$, we have $g_2(\Lambda) \in u^4 H^\times$.
- For $j \neq 1728$, we have $g_3(\Lambda) \in u^6 H^\times$.

Therefore, in terms of points $z \in \mathbb{C}/\Lambda$, we have

$$h(z) = \begin{cases} \dfrac{g_2(\Lambda)}{g_3(\Lambda)}\wp(z) & K \neq \mathbb{Q}(i), \mathbb{Q}(\zeta_3) \\ \dfrac{1}{g_2(\Lambda)}\wp(z)^2 & K = \mathbb{Q}(i) \\ \dfrac{1}{g_3(\Lambda)}\wp(z)^3 & K = \mathbb{Q}(\zeta_3) \end{cases}.$$

This works independently of scaling Λ, so in particular we can pick Λ to be a fractional ideal $\mathfrak{a}$. Then the torsion points of $\mathbb{C}/\mathfrak{a}$ are the points of $K/\mathfrak{a}$.

8.3 Ray class fields

Next, we want to do a similar thing and find a field extension with kernel $K^\star W_\mathfrak{c}$.

Proposition 8.3. *Let $E \in \mathrm{Ell}(\mathcal{O}_K)$, and let $T \in E$ be a generator for the $\mathcal{O}_K$-module $E[\mathfrak{c}]$. Let h be a Weber function for E defined over $H = K(j(E))$. Then*

$$L = H(h(T)) = K(j(E), h(T))$$

is the ray class field modulo $\mathfrak{c}$.

Proof. Let $\sigma \in \mathrm{Aut}(\mathbb{C}/K)$, and let $s \in \mathbb{I}_K$ be such that $[s, K] = \sigma|_{K^{ab}}$.

Suppose σ fixes the ray class field $K_\mathfrak{c}$. Then σ fixes the Hilbert class field H.

We have $s \in K^\times W_\mathfrak{m}$, by the definition of $K_\mathfrak{c}$. Firstly, (s) is principal, so we have $(s) = (\alpha)$ for some $\alpha \in K^\times$.

We also have that $s^{-1}\cdot$ acts the same as $\theta_{\alpha^{-1}} : \mathbb{C}/\mathfrak{a} \to \mathbb{C}/s^{-1}\mathfrak{a}$ on $\mathfrak{c}$-torsion. Next, $T \in E[\mathfrak{c}]$, so we have

$$\begin{aligned} T^\sigma &= f'(s^{-1} \cdot f^{-1}(T)) \\ &= f' \circ \theta_{\alpha^{-1}} \circ f^{-1}(T) \end{aligned}$$

But $f' \circ \theta_{\alpha^{-1}} \circ f^{-1}$ is an isomorphism $E \to E^\sigma = E$. (Note that we cannot say that this isomorphism is the identity, so we cannot conclude $T^\sigma = T$.) So $h(T^\sigma) = h(T)$.

Since the Weber function is defined over H, and σ fixes H, we get $h(T)^\sigma = h(T)$, and so σ fixes L.

This shows:

- L is an abelian extension of K
- L is a subfield of the ray class field modulo $\mathfrak{c}$.

Next we need to show the reverse containment.

Suppose σ fixes L, and let $s \in \mathbb{I}_K$ be an idele such that $[s, K] = \sigma|_{K^{ab}}$. σ fixes H the Hilbert field, so $s \in K^\times W$. We can shift s by any element of $K^\times$, as that is in the kernel of $[\cdot, K]$, so WLOG $s \in W$.

We have $E = E^\sigma$, so we can compose $(f')^{-1} \circ f$ to get an isomorphism $\mathbb{C}/\mathfrak{a} \to \mathbb{C}/\mathfrak{a}$. This isomorphism will therefore be $[\eta]$ for some $\eta \in \mu(K)$.

We know that $h(T^\sigma) = h(T)^\sigma = h(T)$, so there is some automorphism of E sending T to T^σ. Thus, there is some $\zeta \in \mu(K)$ such that $[\zeta]T = T^\sigma$.

Let $x = f^{-1}(T)$. This generates $(\mathbb{C}/\mathfrak{a})[\mathfrak{c}]$, since T generates the $\mathfrak{c}$-torsion of E and f is an isomorphism. To find what s sends x to, we calculate

$$\begin{aligned} s \cdot x &= (f')^{-1}(T^\sigma) \\ &= (f')^{-1}[\zeta]f(x) \\ &= [\zeta](f')^{-1}f(x) \\ &= [\zeta\eta](x). \end{aligned}$$

Since x generates the $\mathfrak{c}$-torsion, this tells us that $s\cdot$ acts the same as multiplication by $\zeta\eta$ on $\mathfrak{c}$-torsion. So $s(\zeta\eta)^{-1} \in \mathbb{I}_\mathfrak{c}$. We also have $(s(\zeta\eta)^{-1}) = (\zeta\eta) = (1)$, so $s(\zeta\eta)^{-1} \in W$. Therefore $s(\zeta\eta)^{-1} \in W_\mathfrak{c}$, and so $s \in K^\times W_\mathfrak{c}$, which tells us that σ fixes $K_\mathfrak{m}$.

So we learn that L contains $K_\mathfrak{m}$, and so we are done. □

Example. Consider the case $K = \mathbb{Q}(i)$. K has class number 1, so the Hilbert class field is equal to K in this case. We take the elliptic curve $y^2 = x^3 + x$, which has complex multiplication by $\mathbb{Z}[i] = \mathcal{O}_K$.

To find the ray class field modulo 3, we need to find a torsion point that generates $E[3]$. 3 is prime in $\mathcal{O}_K$, so any 3-torsion point will work. Solving the equation $3P = O$ gives the polynomial

$$3x^4 + 6x^2 - 1 = 0,$$

which has solution

$$x = \pm\sqrt{-1 \pm \frac{2\sqrt{3}}{3}}.$$

To obtain the ray class field, we therefore need to adjoin the value of x^2 for any one of these points, giving

$$K_{(3)} = K\left(-1 + \frac{2\sqrt{3}}{3}\right) = \mathbb{Q}(i, \sqrt{3}).$$

Since the maximal abelian extension is the union of all the ray class fields, we obtain the following explicit description of the maximal abelian extension.

Corollary 8.4. *Let $E \in \mathrm{Ell}(\mathcal{O}_K)$, and let h be a Weber function for E defined over $H = K(j(E))$. Then the maximal abelian extension of K is given by adjoining the values of $j(E)$ and $h(T)$ for all $T \in E_{tors}$.*

Conclusion

In this essay, we have shown how the main theorem of complex multiplication can be used to show that the Weber function evaluated at torsion points generate the maximal abelian extension of the quadratic imaginary field K. The main theorem has other uses too, of which we will explain one in brief detail.

Given an elliptic curve defined over L with complex multiplication by $\mathcal{O}_K$, the main theorem of complex multiplication can be used to define a Hecke character associated to the elliptic curve, i.e. a continuous homomorphism

$$\psi : \mathbb{I}_L \to \mathbb{C}^\times$$

satisfying $\psi(L^\times) = 1$. This then gives rise to a Hecke L-series

$$L(s, \psi) = \prod_\mathfrak{P} (1 - \psi(\mathfrak{P}) \operatorname{Nm}(\mathfrak{P})^{-s})^{-1}$$

where

$$\psi(\mathfrak{P}) = \begin{cases} \psi((\ldots, 1, \pi, 1, \ldots)) & \mathfrak{P} \text{ unramified, } \pi \text{ a uniformiser of } L_\mathfrak{P} \\ 0 & \mathfrak{P} \text{ ramified} \end{cases}.$$

This Hecke L-series has a meromorphic continuation to $\mathbb{C}$ and satisfies a functional equation.

The L-series associated to the elliptic curve can then be shown to be related to this Hecke L-series. This then gives a proof in the special case of elliptic curves with complex multiplication of the *Hasse-Weil conjecture*, which states that the L-series associated to an elliptic curve has a meromorphic continuation to $\mathbb{C}$ and satisfies a functional equation.

References

[1] J.W.S. Cassels. "Global Fields". In: *Algebraic Number Theory*. Academic Press, 1973. Chap. II, pp. 45–84.

[2] J.S. Milne. *Class Field Theory (v4.03)*. Available at www.jmilne.org/math/. 2020.

[3] Joseph H. Silverman. "Complex Multiplication". In: *Advanced Topics in the Arithmetic of Elliptic Curves*. New York, NY: Springer New York, 1994, pp. 95–186. ISBN: 978-1-4612-0851-8. DOI: 10.1007/978-1-4612-0851-8_3. URL: https://doi.org/10.1007/978-1-4612-0851-8_3.

[4] Joseph H. Silverman. "Elliptic Curves over C". In: *The Arithmetic of Elliptic Curves*. New York, NY: Springer New York, 2009, pp. 157–183. ISBN: 978-0-387-09494-6. DOI: 10.1007/978-0-387-09494-6_6. URL: https://doi.org/10.1007/978-0-387-09494-6_6.