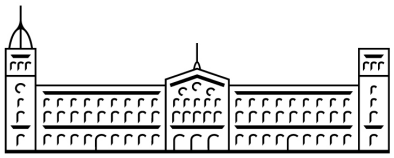

Final Master Project

MASTER IN ADVANCED MATHEMATICS

Faculty of Mathematics
Universitat de Barcelona

Explicit class field theory via elliptic curves

Author: Daniel Gil Muñoz

Director: Dr. Xavier Guitart Morales
Realized in: Departament of Mathematics and Computer Science

Barcelona, September 10, 2017

Contents

Abstract

We present and describe a proof due to Deuring of the Hilbert's 12th problem in the particular case of imaginary quadratic fields. This particular case consists in giving explicit generators of the maximal abelian extension of an imaginary quadratic field. To deal with abelian extensions of such fields, we study the classical formulation of Class Field Theory and present the main statements without proofs. The other important ingredient for the proof we will describe is the theory of elliptic curves with complex multiplication. We will combine Class Field Theory with the notions of elliptic curves to prove the desired construction.

2010 Mathematics subject classification: 11G35, 11G45, 14K22.

Keywords: Elliptic Curve, Complex Multiplication, Ray Class Field, Hilbert Class Field, Existence Theorem, Lattice, Torsion Point, Weber Function, Abelian Extension.

Introduction

In 1900, in the Paris International Congress of Mathematicians, Hilbert presented 10 unsolved mathematical problems at that moment. Shortly after, he expanded this list to 23 problems about different areas of mathematics that influenced strongly the mathematical research at the 20th century (see [1]). These problems are known as Hilbert problems.

We will focus our attention in the 12th problem of that list, which asks to extend Kronecker-Weber's theorem about abelian extensions of the field $\mathbb{Q}$ of rational numbers to any base number field.

Let us understand this statement. An extension of fields L/K is said to be abelian provided that it is Galois and the Galois group $\mathrm{Gal}(L/K)$ attached to it (i.e, the group of authomorphisms of L that fix K) is abelian. Kronecker-Weber's theorem asserts that every abelian extension of $\mathbb{Q}$ is contained in a cyclotomic extension (i.e., an extension of $\mathbb{Q}$ obtained by adjoining to $\mathbb{Q}$ a primitive root of unity).

A basic fact of Galois theory is that the compositum of any two abelian extensions of a field K is again an abelian extension of K. It follows that the maximal abelian extension of K is the compositum of all abelian extensions of K. Thus, Kronecker-Weber's theorem implies that the maximal abelian extension $\mathbb{Q}^{\mathrm{ab}}$ of $\mathbb{Q}$ is obtained by adjoining to $\mathbb{Q}$ all primitive roots of unity. Recall that for any given $N \in \mathbb{N}_{>0}$, the complex number

$$\omega = e^{\frac{2\pi i}{N}}$$

is a primitive N-th root of unity. This is a value of the exponential function (which is a trascendental function: it is defined by a series) that is an algebraic number (i.e, it is a root of some polynomial with rational coefficients). This provides an explicit construction of the field $\mathbb{Q}^{\mathrm{ab}}$ in the sense that we obtain from here a $\mathbb{Q}$-basis of $\mathbb{Q}^{\mathrm{ab}}$ and then we know the form of all elements of $\mathbb{Q}^{\mathrm{ab}}$.

Hilbert's 12th problem asks about an explicit form (in the previous sense) of the maximal abelian extension of any given number field K (i.e, a finite extension of $\mathbb{Q}$). It is often known also as *Kronecker's Jugendtraum*. The German word *Jugendtraum* means dream of youth. This problem was proposed by Kronecker in 1880, while he was elaborating the theory of complex multiplication, in a letter to Dedekind. He talked about the solution of the problem as his dream of youth (see [2], Page 79). It remains currently unsolved, but we have complete solutions when $K = \mathbb{Q}$, when K is an imaginary quadratic field (i.e, a field of the form $\mathbb{Q}(\sqrt{-n})$, $n \in \mathbb{Z}_{>0}$) and when K is a complex multiplication field (see [3]).

In this thesis, we are going to describe Deuring's proof of Hilbert's 12th problem when the base field K is imaginary quadratic. In that case, *Kronecker's Jugendtraum* can be solved by using elliptic curves or modular forms, but we will take the first approach. To

be more accurate, we will use Class Field Theory and the theory of elliptic curves with complex multiplication.

First, we will study Class Field Theory, which describes the structure of the Galois group $\mathrm{Gal}(K^{\mathrm{ab}}/K)$ for any number field K. The description of K^{ab} is not explicit in the sense that it does not provide explicit generators of the extension K^{ab}/K (in other words, we do not know a K-basis of the K-vector space induced by the previous extension). The maximal abelian extension can be described in terms of the Ray Class Fields $K_{\mathfrak{m}}$ for any modulus $\mathfrak{m}$ of K (which is a generalization of the notion of ideal in the ring of integers $\mathcal{O}_K$). When we take $\mathfrak{m} =< 1 >$, the Ray Class Field $K_{<1>}$ is called the Hilbert Class Field of K. The problem of describing the maximal abelian extensions is translated to describe the extensions $K_{\mathfrak{m}}/K$. We do not know explicit generators of $K_{\mathfrak{m}}$ for any number field K. What we will do in this thesis is to give generators of $K_{\mathfrak{m}}$ in the cases that $K = \mathbb{Q}$ and K is an imaginary quadratic field.

As we mentioned, we will present a solution to *Kronecker's Jugendtraum* by using the theory of elliptic curves. We will construct both the Hilbert Class Field and the Ray Class Field for any modulus of an imaginary quadratic field K. Let us see a brief summary of the basic notions of elliptic curves (see Chapter 4 for further details). An elliptic curve is a non-singular algebraic curve over a field F with some F-rational point, or equivalently, an algebraic curve with affine equation

$$y^2 = x^3 - g_2\, x - g_3,\ g_2, g_3 \in F,$$

such that $g_2^3 - 27\, g_3^2 \neq 0$. The discriminant of E is defined as $\triangle(E) = g_2^3 - 27\, g_3^2$ and the j-invariant of E is $j(E) = 1728\, \frac{g_2^3}{\triangle(E)}$. The set $E(F)$ of solutions (x, y) of the equation with $x, y \in F$ can be endowed with a group structure in which the zero element is the point at infinity of the curve E. This group is abelian, and in general its torsion part is non-trivial.

Let K be an imaginary quadratic field. Using the notion of j-invariant of an elliptic curve, we will introduce the j-function, which is a trascendental function. In Chapter 5, we will prove that

$$L = K(j(\tau))$$

is an abelian extension of K, where $\tau \in K$ is some complex non-real number. One can observe the analogy with the cyclotomic case: in our construction, we adjoin to K the trascendental function j evaluated at some $\tau \in \mathbb{C} - \mathbb{R}$ in such a way that $j(\tau)$ is an algebraic number. In the cyclotomic case, we adjoin to $\mathbb{Q}$ the exponential function evaluated at $\frac{2\pi i}{N} \in \mathbb{C} - \mathbb{R}$ in such a way that $e^{\frac{2\pi i}{N}}$ is an algebraic number. In fact, with an appropiate choice of τ (to be more accurate, if the lattice $< 1, \tau >$ has complex multiplication by $\mathcal{O}_K$, see Section 4 of Chapter 4), the field L is the Hilbert Class Field of K.

In Chapter 6 we will prove the mentioned Kronecker-Weber's theorem and solve completely the *Kronecker's Jugendtraum* for imaginary quadratic fields. Namely, if K is an imaginary quadratic field, we will prove that if E is any elliptic curve with complex multiplication by the ring of integers $\mathcal{O}_K$ of K and defined over the Hilbert Class Field of K, then K^{ab} is obtained by adjoining to K the j-function evaluated at some $\tau \in \mathbb{C} - \mathbb{R}$ as before and all the first coordinates of torsion points of $E(K)$.

Part I

Class field theory

Chapter 1

Preliminary: Algebraic number theory

In this chapter we recall the basic notions and results of basic algebraic number theory that we will need in the exposition. We will give the definitions and basics about number fields and their rings of integers. After that, we will review the unique-factorization property of ideals in a number ring and the splitting of prime ideals in some extension. Finally, we will introduce fractional ideals and use them in order to construct the ideal class group of the ring of integers. This will be used in the particular case of class field theory corresponding to Section 1 of Chapter 3. The main reference used in this chapter is [4].

1 Number fields and number rings

Recall that a number field is a finite extension of $\mathbb{Q}$ which is subfield of $\mathbb{C}$. We say that $n = [K : \mathbb{Q}]$ is the degree of K. An algebraic integer is any $\alpha \in \mathbb{C}$ such that there exists a monic polynomial $f \in \mathbb{Z}[X]$ such that $f(\alpha) = 0$. The ring of integers associated to K is the set of all algebraic integers of K. It is an integral domain. We have a useful result that relates a number field with its ring of integers.

Proposition 1.1. *Given $\alpha \in K$, there exists $m \in \mathbb{Z}$, $m \neq 0$ such that $m\,\alpha \in \mathcal{O}_K$.*

With this, we see that K is isomorphic to the field of fractions of $\mathcal{O}_K$.

Let K be a number field of degree n and let $\sigma_1, ..., \sigma_n$ be the $\mathbb{Q}$-embeddings of K in $\mathbb{C}$. The norm of an element $\alpha \in K$ is the number

$$N(\alpha) = \prod_{i=1}^{n} (\sigma_i(\alpha)).$$

The discriminant of the n-tuple $(\alpha_1, ..., \alpha_n) \in K^n$ is the number

$$\mathrm{disc}(\alpha_1, ..., \alpha_n) = \det([\sigma_i(\alpha_j)])^2$$

Theorem 1.2. *Let K be a number field of degree n. Then, the additive group of the ring of integers $\mathcal{O}_K$ is a free abelian group of rank n.*

An integral basis of $\mathcal{O}_K$ is any basis of the additive group of $\mathcal{O}_K$. The discriminant is an invariant for the integral basis, that is, if $\{\alpha_1, ...\alpha_n\}$ and $\{\beta_1, ..., \beta_n\}$ are two integral basis of the number ring $\mathcal{O}_K$, then $\text{disc}(\alpha_1, ..., \alpha_n) = \text{disc}(\beta_1, ..., \beta_n)$. This allows us to define the discriminant of the number ring $\mathcal{O}_K$ as

$$\text{disc}(\mathcal{O}_K) = \text{disc}(\alpha_1, ..., \alpha_n)$$

where $\{\alpha_1, ..., \alpha_n\}$ is any integral basis of $\mathcal{O}_K$.

A basic example of number field is a quadratic field, which is a number field K such that $[K : \mathbb{Q}] = 2$, or equivalently, $K = \mathbb{Q}(\sqrt{m})$, where m is a square-free integer.

If K is a quadratic field and $d_K = disc(\mathcal{O}_K)$, then we can always write:

$$\mathcal{O}_K = \mathbb{Z}\left[\frac{d_K + \sqrt{d_K}}{2}\right].$$

2 Prime factorization of ideals

A Dedekind domain is an integral domain R such that:

1. R is noetherian.
2. All non-zero prime ideal of R is maximal.
3. R is integrally closed in its field of fractions.

One can prove an important characterization: Dedekind domains are the integral domains whose ideals factorize uniquely up to order as a product of prime ideals. Here we will only state that Dedekind domains have the unique factorization property.

Lemma 1.3. *Let K be a number field and let I be an ideal of $\mathcal{O}_K$. Then, $\mathcal{O}_K/I$ is finite.*

Theorem 1.4. *Let K be a number field. Then, $\mathcal{O}_K$ is a Dedekind domain.*

Corollary 1.5. *Any proper ideal of a number ring factorizes uniquely as a product of prime ideals.*

Lemma 1.3 allows us to define the norm of an ideal I of $\mathcal{O}_K$ as $N(I) = |\mathcal{O}_K/I|$. We list some properties of such norm.

Proposition 1.6. *Let K be a number field.*

1. *If I and J are ideals of $\mathcal{O}_K$, $N(IJ) = N(I)N(J)$.*
2. *If L is an extension of K such that $[L : K] = n$ and I is an ideal of $\mathcal{O}_K$, then $N(I\,\mathcal{O}_L) = N(I)^n$.*
3. *If $\alpha \in \mathcal{O}_K$, $\alpha \neq 0$, then $N(\alpha\,\mathcal{O}_K) = |N(\alpha)|$.*

Now we consider L/K an extension of number fields. Let P be a prime ideal of $\mathcal{O}_K$ and let Q be a prime ideal of $\mathcal{O}_L$. We say that Q is over P or that P is under Q if $Q \cap \mathcal{O}_K = P$. Then, one can prove that if P is a prime ideal of $\mathcal{O}_K$, there is some prime ideal of $\mathcal{O}_L$ over P, while if Q is a prime ideal of $\mathcal{O}_L$, there is an unique prime ideal of $\mathcal{O}_K$ over Q.

Let P be a prime ideal of $\mathcal{O}_K$. Then $P\,\mathcal{O}_L$ is a proper ideal of $\mathcal{O}_L$, so it factorizes uniquely as a product of prime ideals of $\mathcal{O}_L$. This factorization is called the splitting of the prime ideal P in the number ring $\mathcal{O}_L$. Note that the prime ideals in this factorization are the prime ideals of $\mathcal{O}_L$ over P.

Let P be a prime ideal of $\mathcal{O}_K$ and let Q be a prime ideal of $\mathcal{O}_L$ over P.

1. The ramification index of Q over P, denoted by $e(Q|P)$, is the power of Q in the factorization of $P\,\mathcal{O}_L$.

2. The inertia degree of Q over P is the positive integer $f(Q|P) = [(\mathcal{O}_L/Q) : (\mathcal{O}_K/P)]$.

Definition 1.7. *Let L/K be an extension of number fields and let P be a prime ideal of $\mathcal{O}_K$.*

1. *We say that P is ramified in $\mathcal{O}_L$ if there exists a prime ideal Q of $\mathcal{O}_L$ over P such that $e(Q|P) > 1$.*

2. *We say that P splits completely in $\mathcal{O}_L$ if $e(Q|P) = f(Q|P) = 1$ for all prime ideals Q of $\mathcal{O}_L$ over P.*

Let us assume that the extension L/K is Galois. The key result is that in this case $\mathrm{Gal}(L/K)$ permutes transitively the prime ideals of $\mathcal{O}_L$ over P. As a consequence, if Q and Q' are prime ideals of $\mathcal{O}_L$ over P, then $e(Q|P) = e(Q'|P)$ and $f(Q|P) = f(Q'|P)$. Then,

$$n = e\,f\,r,$$

where r is the amount of primes in the splitting of P.

The Artin symbol

Let L/K be a Galois extension of number fields. Let P be a prime of K which is unramified in L and let Q be a prime of L over P. Then, there is an unique map $\sigma \in \mathrm{Gal}(L/K)$ such that

$$\sigma(\alpha) \equiv \alpha^{N(P)} \,(\mathrm{mod}\, Q) \text{ for all } \alpha \in \mathcal{O}_L.$$

The map σ is called the Artin symbol of L/K over Q, and it is denoted by $\left(\frac{L/K}{Q}\right)$.

Given $\sigma \in \mathrm{Gal}(L/K)$, we have that $\left(\frac{L/K}{\sigma(Q)}\right) = \sigma \circ \left(\frac{L/K}{Q}\right) \circ \sigma^{-1}$. We deduce that the conjugacy class of $\left(\frac{L/K}{Q}\right)$ does not depend on Q. The Artin symbol of L/K over P, denoted by $\left(\frac{L/K}{P}\right)$, is the conjugacy class of $\left(\frac{L/K}{Q}\right)$.

In particular, when the extension L/K is abelian, the Artin symbol $\left(\frac{L/K}{Q}\right)$ does not depend on Q, and we define the Artin symbol of L/K over P as $\left(\frac{L/K}{P}\right) = \left(\frac{L/K}{Q}\right)$.

A basic property of the Artin symbol $\left(\frac{L/K}{P}\right)$ is that the primes P for which it becomes trivial are those that split completely at L.

Proposition 1.8. *Let L/K be a Galois extension and let P be a prime of K that does not ramify in L. Then,*

$$\left(\frac{L/K}{P}\right) = 1 \Longleftrightarrow P \text{ splits completely at } L.$$

Proof. the Artin symbol $\left(\frac{L/K}{P}\right)$ is the conjugacy class of all Artin symbols $\left(\frac{L/K}{Q}\right)$ with Q prime of L over P. We want to prove that it is trivial (i.e, its unique element is the identity). Using the definitions, it is easy to prove (see [6], Corollary 5.21) that for any prime Q of L over P,

$$\left(\frac{L/K}{Q}\right) = 1 \Longleftrightarrow P \text{ splits completely at } L.$$

Then the claim follows. □

3 Fractional ideals

The introduction of fractional ideals has a double purpose: On the one hand, we will prove a unique factorization property of fractional ideals as product of prime ideals of a number ring, which will allow us to generalize the Artin symbol just introduced to any fractional ideal of K. On the other hand, we will be able to construct the ideal class group of $\mathcal{O}_K$. The theory of fractional ideals in a more general situation can be consulted in [5].

Let K be a number field. Then $\mathcal{O}_K$ acts on K with the product on K, so K has structure of $\mathcal{O}_K$-module. A fractional ideal of $\mathcal{O}_K$ is a non-zero finitely generated $\mathcal{O}_K$-submodule of K. Obviously, the fractional ideals of $\mathcal{O}_K$ that are contained in $\mathcal{O}_K$ are the ideals of $\mathcal{O}_K$. These are also called integral ideals of $\mathcal{O}_K$.

Theorem 1.9. *Let $\mathfrak{a}$ be a $\mathcal{O}_K$-submodule of K. Then, the following are equivalent:*

1. *$\mathfrak{a}$ is a fractional ideal of $\mathcal{O}_K$*
2. *$\mathfrak{a} = \alpha\, I$, where $\alpha \in K$ and I is an ideal of $\mathcal{O}_K$.*
3. *There exists $x \in \mathcal{O}_K$, $x \neq 0$ such that $x\,\mathfrak{a} \subset \mathcal{O}_K$.*

Proof. Let us see that 1 implies 2. Assume that $\mathfrak{a}$ is a fractional ideal of K. Let $\alpha_1, ..., \alpha_n \in K$ such that $\mathfrak{a} =< \alpha_1, ..., \alpha_n >_{\mathcal{O}_K}$. Let $a_1, ..., a_n, b \in \mathcal{O}_K$ such that $\alpha_i = a_i\, b^{-1}$ for all $i \in \{1, ..., n\}$. Let $\alpha = b^{-1} \in K$ and $I =< a_1, ..., a_n >_{\mathcal{O}_K}$. Since $a_1, ..., a_n \in \mathcal{O}_K$, I is an ideal of $\mathcal{O}_K$. Then,

$$\mathfrak{a} =< a_1\, b^{-1}, ..., a_n\, b^{-1} >_{\mathcal{O}_K} = \alpha \ < a_1, ..., a_n >_{\mathcal{O}_K} = \alpha\, I.$$

Conversely, let us suppose that $\mathfrak{a} = \alpha\, I$ with $\alpha \in K$ and I an ideal of $\mathcal{O}_K$. Since $\mathcal{O}_K$ is a Dedekind domain, it is noetherian, so all its ideals are finitely generated. Let $a_1, ..., a_n \in \mathcal{O}_K$ such that $I =< a_1, ..., a_n >_{\mathcal{O}_K}$. Then,

$$\mathfrak{a} = \alpha\, I = \alpha\ < a_1, ..., a_n >_{\mathcal{O}_K} =< a_1\, \alpha, ..., a_n\, \alpha >_{\mathcal{O}_K},$$

where $a_i\, \alpha \in K$ for all $i \in \{1, ..., n\}$. Then, $\mathfrak{a}$ is a fractional ideal of K.

Let us see that 2 implies 3. Let $\alpha \in K$ and I ideal of $\mathcal{O}_K$ such that $\mathfrak{a} = \alpha\, I$. If we apply Proposition 1.1 to α^{-1}, we obtain that there exists a non-zero integer m such that $m\, \alpha^{-1} \in \mathcal{O}_K$. Let $x = m\, \alpha^{-1}$. Then, $x \neq 0$, $x \in \mathcal{O}_K$ and $x\, \mathfrak{a} = m\, \alpha^{-1}\, \alpha\, I = m\, I \subset \mathcal{O}_K$.

Finally, we will prove that 3 implies 2. Let $x \in \mathcal{O}_K$, $x \neq 0$ such that $x\, \mathfrak{a} \subset \mathcal{O}_K$. This condition says in fact that $I = x\, \mathfrak{a}$ is an ideal of $\mathcal{O}_K$. In effect, if $\alpha \in I$, then there exists $y \in \mathfrak{a}$ such that $\alpha = x\, y$, and given $\beta \in \mathcal{O}_K$, we have that $\beta\, \alpha = \beta\, x\, y = x\, (\beta\, y) \in x\, \mathfrak{a} = I$ because since $\beta \in \mathcal{O}_K$, $y \in \mathfrak{a}$ and $\mathfrak{a}$ is an $\mathcal{O}_K$-submodule of K, $\beta\, y \in \mathfrak{a}$. □

Let I_K be the set of fractional ideals of $\mathcal{O}_K$. We can define an operation in I_K given by the following: If $\mathfrak{a} = \alpha\, I, \mathfrak{b} = \beta\, J$, we define

$$\mathfrak{a}\, \mathfrak{b} := \alpha\, \beta\, I\, J.$$

Proposition 1.10. *The previous product is well defined.*

Proof. First, we have to prove that it does not depend on the representatives. Let $\mathfrak{a}, \mathfrak{b}$ be fractional ideals and let $\alpha_1, \alpha_2, \beta_1, \beta_2 \in K$, and I_1, I_2, J_1, J_2 ideals of $\mathcal{O}_K$ such that $\mathfrak{a} = \alpha_1\, I_1 = \alpha_2\, I_2$ and $\mathfrak{b} = \beta_1\, J_1 = \beta_2\, J_2$. We have to prove that $\alpha_1\, \beta_1\, I_1\, J_1 = \alpha_2\, \beta_2\, I_2\, J_2$.

Since $\alpha_1\, I_1 = \alpha_2\, I_2$, we have that $I_1 = \alpha_1^{-1}\, \alpha_2\, I_2$. Similarly, $I_2 = \beta_1^{-1}\, \beta_2\, J_2$. Then,

$$\alpha_1\, \beta_1\, I_1\, J_1 = \alpha_1\, \beta_1\, \alpha_1^{-1}\, \alpha_2\, I_2\, J_1 = \beta_1\, \alpha_2\, I_2\, J_1 = \beta_1 \alpha_2 \beta_1^{-1} \beta_2\, I_2\, J_2 = \alpha_2\, \beta_2\, I_2\, J_2.$$

Finally, this product is clearly closed in I_K. □

The next goal is to prove that I_K with this operation is a group. Note that it is trivially associative and has identity element $\mathcal{O}_K$.

Proposition 1.11. *Let K be a number field and let $\mathfrak{a}$ be a non-zero fractional ideal of K. Then there exists a fractional ideal $\mathfrak{b}$ of K such that $\mathfrak{a}\, \mathfrak{b} = \mathcal{O}_K$ (that is, $\mathfrak{a}$ is invertible).*

Proof. Let us define $\mathfrak{b} = \{\alpha \in K \mid \alpha\, \mathfrak{a} \subset \mathcal{O}_K\}$. Let us see that $\mathfrak{b}$ is a fractional ideal. Let $x \in \mathfrak{a}$ such that $x \neq 0$ and $x \in \mathcal{O}_K$ (such an element x exists because of Proposition 1.1). Then, by definition of $\mathfrak{b}$, $x\, \mathfrak{b} \subset \mathcal{O}_K$. Then $\mathfrak{b}$ is a fractional ideal.

Let us see that $\mathfrak{a}\, \mathfrak{b} = \mathcal{O}_K$. By definition of $\mathfrak{b}$, it is clear that $\mathfrak{a}\, \mathfrak{b} \subset \mathcal{O}_K$. Moreover, since $\mathfrak{a}$ is an ideal of $\mathcal{O}_K$, so is $\mathfrak{a}\, \mathfrak{b}$. Let us see the other inclusion. Let $x \in \mathfrak{a}$ such that $x \neq 0$. Then, $x^{-1}\, x = 1 \in \mathcal{O}_K$, so $x^{-1} \in \mathfrak{b}$. Hence $1 = x\, x^{-1} \in \mathfrak{a}\, \mathfrak{b}$, and being $\mathfrak{a}\, \mathfrak{b}$ an ideal, we obtain that $\mathfrak{a}\, \mathfrak{b} = \mathcal{O}_K$. □

Corollary 1.12. *Let K be a number field. Then, the set I_K of the fractional ideals of K is a group under multiplication.*

Using the property of unique factorization in number rings, we are going to prove the mentioned unique factorization property in I_K.

Proposition 1.13. *Let K be a number field and let $\mathfrak{a} \in I_K$. Then, there exist unique prime ideals $P_1, ..., P_k$ in $\mathcal{O}_K$ and unique integers $r_1, ..., r_k \in \mathbb{Z}$ such that*

$$\mathfrak{a} = P_1^{r_1} ... P_k^{r_k}.$$

Proof. Let $\alpha \in K$ and I ideal of $\mathcal{O}_K$ such that $\mathfrak{a} = \alpha\, I$. Since K is isomorphic to the field of fractions of $\mathcal{O}_K$, there exist $a, b \in \mathcal{O}_K$ such that $\alpha = a\, b^{-1}$. Hence, $< b >_{\mathcal{O}_K} \mathfrak{a} = a\, I$. Now, both $< b >_{\mathcal{O}_K}$ and $a\, I$ are ideals of $\mathcal{O}_K$, so they factorize uniquely, say

$$a\, J = Q_1^{\beta_1} ... Q_r^{\beta_r},$$

$$< b >= U_1^{\gamma_1} ... U_s^{\gamma_s},$$

with Q_i, U_j prime ideals of $\mathcal{O}_K$ and $\beta_i, \gamma_j \in \mathbb{N}$. Then, from the previous equality we obtain that

$$I = Q_1^{\beta_1} ... Q_r^{\beta_r}\, U_1^{-\gamma_1} ... U_s^{-\gamma_s}.$$

If we cancel the repeated primes, we obtain the desired factorization. □

The ideal class group

Let K be a number field and let $\alpha \in K$. Then

$$< \alpha >_{\mathcal{O}_K} = \{\lambda\, \alpha \,|\, \lambda \in \mathcal{O}_K\}$$

is clearly a fractional ideal. Such an ideal is called a principal fractional ideal.

Let $< \alpha >_{\mathcal{O}_K}$ be a principal fractional ideal. We have that

$$< \alpha >_{\mathcal{O}_K} < \alpha^{-1} >_{\mathcal{O}_K} = < 1 >_{\mathcal{O}_K} = \mathcal{O}_K,$$

and hence $< \alpha >_{\mathcal{O}_K}^{-1} = < \alpha^{-1} >_{\mathcal{O}_K}$.

Given $< \alpha >_{\mathcal{O}_K}, < \beta >_{\mathcal{O}_K}$ principal fractional ideals, we have that

$$< \alpha >_{\mathcal{O}_K} < \beta^{-1} >_{\mathcal{O}_K} = < \alpha\, \beta^{-1} >_{\mathcal{O}_K}$$

is again a principal fractional ideal.

This proves that the set P_K of principal fractional ideals is a subgroup of I_K. Since I_K is abelian, P_K is a normal subgroup of I_K.

Definition 1.14. *Let K be a number field. The ideal class group of K is the quotient group*

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

We have the following useful result, whose proof can be found in [4] (Chapter 5).

Theorem 1.15. *There are finitely many ideal classes of $\mathcal{O}_K$, that is, $\mathcal{C}(\mathcal{O}_K)$ is a finite group.*

The importance of this theorem lies in the fact that it allows us to establish quantitative results related to the ideals of a ring of integers. In Chapter 5, in the case in which K is an imaginary quadratic field, we will relate also the ideal class group of $\mathcal{O}_K$ with the set of $\mathbb{C}$-isomorphism classes of elliptic curves with complex multiplication (see Chapter 4). Here the finiteness of the ideal class group will be crucial in order to prove the finiteness of such classes of elliptic curves.

Chapter 2

Orders in quadratic fields

The theory of orders in number fields is introduced in order to obtain a family of rings with similar properties as the ring of integers. This provides extra information of the arithmetic structure of the number field. The theory of orders will be very useful in part 2. For example, in Chapter 4 we will see that such orders allow us to classify the endomorphism ring of an elliptic curve. The main reference used in this chapter is [6].

The first section is about orders in general number fields. After this, we will only deal with orders in quadratic number fields. We could restrict ourselves to the quadratic case at the begining, but the notions in the first section are exactly the same in the general case.

We study the quadratic case in the second section. The study of orders in quadratic fields has a great advantadge: such orders are uniquely determined by an integer number, which is called the conductor of the order.

In the third section, we will generalize the theory of both ideals and fractional ideals of the ring of integers introduced in the previous chapter to an order. We will also focus on a special type of fractional ideals, that are proper fractional ideals. This is going to be also a fundamental ingredient in the theory of elliptic curves introduced in the second part. We will construct also the ideal class group of an order, which is the analog of the ideal class group of the ring of integers introduced in the previous chapter.

Finally, we introduce the concept of ideals prime to the conductor and we use them in order to construct another expression of the ideal class group of an order. This theory will be applied in the next chapter in order to define the ring class field.

1 Generalities

We begin by defining and studying orders in a general number field K.

Proposition 2.1. *Let K be a number field of degree n and let M be a finitely generated subgroup of K. Then:*

1. *M is a free abelian group.*
2. *M has rank n if and only if M contains a $\mathbb{Q}$-basis of K.*

Proof. 1. It is trivial.

2. Assume that M has rank n. Let $\{\alpha_1, ..., \alpha_n\}$ be a $\mathbb{Z}$-basis of M. Then, $\{\alpha_1, ..., \alpha_n\}$ is linearly independent over $\mathbb{Z}$. Let $a_1, ..., a_n \in \mathbb{Q}$ such that $a_1\,\alpha_1 + ... + a_n\,\alpha_n = 0$. We can assume that $a_i = \frac{\lambda_i}{\mu}, i \in \{1, ..., n\}$ have the same denominator, so we have that $\lambda_1\,\alpha_1 + ... + \lambda_n\,\alpha_n = 0$, with $\lambda_1, ..., \lambda_n \in \mathbb{Z}$. Then $\lambda_1 = ... = \lambda_n = 0$, and hence $a_1 = ... = a_n = 0$. This proves that $\{\alpha_1, ..., \alpha_n\}$ is linearly independent over $\mathbb{Q}$. Since K is of degree n, $< \alpha_1, ..., \alpha_n >_{\mathbb{Q}} = K$. Then $\{\alpha_1, ..., \alpha_n\}$ is a $\mathbb{Q}$-basis of K contained in M.

   Conversely, let us suppose that $\{\alpha_1, ..., \alpha_n\}$ is a $\mathbb{Q}$-basis of K contained in M. Since M is a subgroup of K, $< \alpha_1, ..., \alpha_n >_{\mathbb{Z}} \subset M$. By the hypothesis, $\{\alpha_1, ..., \alpha_n\}$ is linearly independent over $\mathbb{Q}$. Since $\mathbb{Z} \subset \mathbb{Q}$, it is linearly independent over $\mathbb{Z}$. This proves that $\text{rank}(M) \geq n$. Moreover, we can prove as in the other implication that any $\mathbb{Z}$-basis of M is a $\mathbb{Q}$-basis of K. Since the $\mathbb{Q}$-vector space K has dimension n, $\text{rank}(M) \leq n$. We deduce that $\text{rank}(M) = n$.

□

Definition 2.2. *Let K be a number field. We say that $\mathcal{O} \subset K$ is an order in K if it satisfies:*

1. *$\mathcal{O}$ is an unitary subring of K.*
2. *$\mathcal{O}$ is a finitely generated abelian group.*
3. *$\mathcal{O}$ contains a $\mathbb{Q}$-basis of K.*

Remark 2.3. *By the previous Proposition, conditions 2 and 3 together are equivalent to*

2'. $\mathcal{O}$ is a (free) finitely generated subgroup of K of rank n.

Remark 2.4. *Let $\mathcal{O}$ be an order of K. Since $\mathcal{O}$ contains a $\mathbb{Q}$-basis of K, K is isomorphic to the field of fractions of $\mathcal{O}$.*

Let K be a number field. Then, $\mathcal{O}_K$ is an order of K. Indeed, it is known that it is a unitary subring of K, and by Theorem 1.2, it is finitely generated of rank n. In fact, it is the maximal order of K.

Theorem 2.5. *Let K be a number field and let $\mathcal{O}$ be an order of K. Then, $\mathcal{O} \subset \mathcal{O}_K$*

Proof. Let $\alpha \in \mathcal{O}$. Let us define

$$\begin{array}{rccc} m_\alpha\colon & \mathcal{O} & \longrightarrow & \mathcal{O} \\ & \beta & \longmapsto & \alpha\,\beta \end{array}.$$

This map is an endomorphism. Since $\mathcal{O}$ is a free generated abelian group of rank n and $m_\alpha(\mathcal{O}) \subset \mathcal{O} = \mathbb{Z}\,\mathcal{O}$, using Proposition 2.4 of [5], there exist $a_1, ..., a_n \in \mathbb{Z}$ such that

$$m_\alpha^n + a_1\,m_\alpha^{n-1} + ... + a_{n-1}\,m_\alpha + a_n = 0.$$

Since $\mathcal{O}$ is unitary, we can evaluate in 1, and then we obtain that

$$\alpha^n + a_1\,\alpha^{n-1} + ... + a_{n-1}\,\alpha + a_n = 0.$$

That is, α is a root of a monic polynomial with integer coefficients. This proves that $\alpha \in \mathcal{O}_K$. □

2 The case of quadratic fields

Orders of quadratic fields have better properties and we can obtain stronger results about them. Moreover, we will need the imaginary ones for characterizing endomorphism rings of elliptic curves (see Chapter 4). Remember that if K is a quadratic field, then $\mathcal{O}_K =< 1, \omega_K >_{\mathbb{Z}}$, where $\omega_K = \frac{d_K + \sqrt{d_K}}{2}$ and $d_K = \text{disc}(K)$.

The key result is the following:

Theorem 2.6. *Let K be a quadratic field and let $\mathcal{O}$ be an order of K. Let $d_K = \text{disc}(K)$ and $f = [\mathcal{O}_K : \mathcal{O}]$. Then $f < \infty$ and*

$$\mathcal{O} = \mathbb{Z} + f\,\mathcal{O}_K =< 1, f\,\omega_K >_{\mathbb{Z}} .$$

Proof. Since both $\mathcal{O}$ and $\mathcal{O}_K$ are free abelian groups of rank 2, we have that $[\mathcal{O}_K : \mathcal{O}] = |\mathcal{O}_K/\mathcal{O}| < \infty$.

Let $x_1, ..., x_{f-1} \in \mathcal{O}_K$ such that $\mathcal{O}_K = \mathcal{O} \cup x_1\,\mathcal{O} \cup ... \cup x_{f-1}\,\mathcal{O}$. Then $f\,\mathcal{O}_K \subset \mathcal{O}$, and hence $\mathbb{Z} + f\,\mathcal{O}_K \subset \mathcal{O}$. On the other hand, since $\mathcal{O}_K =< 1, \omega_K >_{\mathbb{Z}}$, we have that:

$$\begin{aligned}\mathbb{Z} + f\,\mathcal{O}_K =& \{a + f\,(b + c\,\omega_K) \,|\, a, b, c \in \mathbb{Z}\} \\ &= \{(a + fb) + cf\omega_K \,|\, a, b, c \in \mathbb{Z}\} \\ &= \{a + bf\omega_K \,|\, a, b \in \mathbb{Z}\} =< 1, f\,\omega_K >_{\mathbb{Z}} .\end{aligned}$$

Hence $< 1, f\,\omega_K >_{\mathbb{Z}} \subset \mathcal{O}$. Furthermore,

$$< 1, \omega_K >_{\mathbb{Z}} / < 1, f\,\omega_K >_{\mathbb{Z}} \cong < \omega_K >_{\mathbb{Z}} / < f\,\omega_K >_{\mathbb{Z}} = \{\overline{b\,\omega_K} \,|\, b \in \{0, ..., f-1\}\}.$$

Let us see that all these elements are different. Let $b_1, b_2 \in \{0, ..., f-1\}$ such that $\overline{b_1\,\omega_K} = \overline{b_2\,\omega_K}$. Then, $(b_1 - b_2)\,\omega_K \in < f\,\omega_K >_{\mathbb{Z}}$. This means that f divides $b_1 - b_2$, but $|b_1 - b_2| < f$. We deduce that $b_1 - b_2 = 0$, that is, $b_1 = b_2$. Hence $[< 1, \omega_K >_{\mathbb{Z}} :< 1, f\,\omega_K >_{\mathbb{Z}}] = | < 1, \omega_K >_{\mathbb{Z}} / < 1, f\,\omega_K >_{\mathbb{Z}} | = f$.

Since $< 1, f\,\omega_K >_{\mathbb{Z}}$ and $\mathcal{O}$ are subgroups of index f in $\mathcal{O}_K$ and $< 1, f\,\omega_K >_{\mathbb{Z}} \subset \mathcal{O}$, necessarily $\mathcal{O} =< 1, f\,\omega_K >_{\mathbb{Z}}$. □

Definition 2.7. *Let K be a quadratic field and let $\mathcal{O}$ be an order of K. The conductor of $\mathcal{O}$ is the number $f = [\mathcal{O}_K : \mathcal{O}]$.*

Corollary 2.8. *Let K be a quadratic field. Then, every order of K is uniquely determined by its conductor.*

This result in general does not hold for number fields of degree greater than 2.

3 Ideals of orders in quadratic fields

Let K be a quadratic field and let $\mathcal{O}$ be an order of K. Recall that $\mathcal{O}$ is, by definition, a unitary subring of K, in particular we can consider its ideals. We have some similar results that we stated for the ideals of $\mathcal{O}_K$ but there is a main difference: $\mathcal{O}$ is not in general integrally closed in its field of fractions, but it is *almost* a Dedekind domain.

Lemma 2.9. *Let I be a non-zero ideal of $\mathcal{O}$. Then, there exists $m \in \mathbb{Z}$, $m \neq 0$ such that $m \in I$.*

Proof. Let $\alpha \in I$ such that $\alpha \neq 0$. Let σ be the non-trivial $\mathbb{Q}$-automorphism of K and let $\beta = \sigma(\alpha)$. We know by Theorem 2.6 that $\mathcal{O} =< 1, f\,\omega_K >_{\mathbb{Z}}$. Then, there exist $a, b \in \mathbb{Z}$ such that $\alpha = a + b\,f\,\omega_K$. Then, $\beta = \sigma(\alpha) = a + b\,f\,\sigma(\omega_K)$. Since $\omega_K \in \mathcal{O}_K$ and $\sigma \in \mathrm{Gal}(K/\mathbb{Q})$, we have that $\sigma(\omega_K) \in \mathcal{O}_K$. Then, $\beta \in \mathcal{O}$.

Let $m = N(\alpha)$. Since α is an algebraic integer, we have that $m \in \mathbb{Z}$ and $m \neq 0$ because $\alpha \neq 0$. Moreover, $m = \alpha\,\beta \in I$. □

Proposition 2.10. *Let I be an ideal of $\mathcal{O}$. Then $\mathcal{O}/I$ is finite.*

Proof. Let m be a non-zero integer such that $m \in I$. Since $\mathcal{O}$ is a free abelian group of rank 2, $|\mathcal{O}/m\,\mathcal{O}| = m^2$. On the other hand, since $m \in I$, we have that $m\,\mathcal{O} \subset I$, and then by the third isomorphism theorem,

$$|\mathcal{O}/I| \leq |\mathcal{O}/m\,\mathcal{O}| = m^2 < \infty.$$

□

Theorem 2.11. *Let K be a quadratic field and let $\mathcal{O}$ be an order of K. Then:*

1. *Every non-zero prime ideal of $\mathcal{O}$ is maximal.*
2. *$\mathcal{O}$ is noetherian.*

Proof.

1. Let P be a prime ideal of $\mathcal{O}$. Then $\mathcal{O}/P$ is an integral domain, and by the previous result it is finite. Thus $\mathcal{O}/P$ is a field, that is, P is maximal.
2. Let I be an ideal of $\mathcal{O}$. Then I can be seen as a subgroup of $\mathcal{O}$, which is free finitely generated of rank 2. Hence I is finitely generated.

   Since all ideals of $\mathcal{O}$ are finitely generated, $\mathcal{O}$ is noetherian.

□

In general, an order $\mathcal{O}$ in a quadratic field is not a Dedekind domain: If there is $\alpha \in \mathcal{O}_K$ such that $\alpha \notin \mathcal{O}$, then $\alpha \in K$ is a root of some monic polynomial with coefficients in $\mathbb{Z}$ but it does not belong to $\mathcal{O}$. That is, if $\mathcal{O} \subsetneq \mathcal{O}_K$, then $\mathcal{O}$ is not integrally closed in its field of fractions. The converse of this is clear, because $\mathcal{O}_K$ is a Dedekind domain and it is the maximal order. Hence, $\mathcal{O}$ is not a Dedekind domain if and only if the conductor f of $\mathcal{O}$ is greater than 1. As a consequence, ideals of orders do not factorize uniquely as product of prime ideals.

3.1 Fractional ideals of an order

We can generalize naturally the theory of fractional ideals of the ring $\mathcal{O}_K$ to any order $\mathcal{O}$ of a quadratic field.

Definition 2.12. *Let K be a quadratic field and let $\mathcal{O}$ be an order of K. A fractional ideal of $\mathcal{O}$ is a subset $\mathfrak{a}$ of K which is a finitely generated $\mathcal{O}$-submodule of K.*

As in the case of the ring of integers $\mathcal{O}_K$, the fractional ideals of $\mathcal{O}$ contained in $\mathcal{O}$ are the ideals of $\mathcal{O}$. Sometimes, we will refer to them as integral ideals of $\mathcal{O}$.

Theorem 2.13. *Let $\mathcal{O}$ be an order of a quadratic field K. Let $\mathfrak{a}$ be a $\mathcal{O}$-submodule of K. Then, the following are equivalent:*

1. *$\mathfrak{a}$ is a fractional ideal of $\mathcal{O}$.*
2. *$\mathfrak{a} = \alpha\, I$, where $\alpha \in K$ and I is an ideal of $\mathcal{O}$.*
3. *There exists $x \in \mathcal{O}$, $x \neq 0$ such that $x\,\mathfrak{a} \subset \mathcal{O}$.*

Proof. We will only prove that 2 implies 3, because the other implications are similar to the case of $\mathcal{O}_K$. Let $\alpha \in K$ and I ideal of $\mathcal{O}$ such that $\mathfrak{a} = \alpha\, I$. If we apply Proposition 1.1 to α^{-1}, we obtain that there exists a non-zero integer m such that $m\,\alpha^{-1} \in \mathcal{O}_K$. But we also know that $f\,\mathcal{O}_K \subset \mathcal{O}$, where f is the conductor of $\mathcal{O}$. Let $x = f\,m\,\alpha^{-1}$. Then, $x \neq 0$, $x \in \mathcal{O}$ and $x\,\mathfrak{a} = f\,m\,\alpha^{-1}\,\alpha\, I = f\,m\, I \subset \mathcal{O}$. □

Proposition 2.14. *Let $\mathcal{O}$ be an order of a quadratic field K and let $\mathfrak{a}$ be a fractional ideal of $\mathcal{O}$. Then, $\mathfrak{a}$ is a free abelian group of rank 2.*

Proof. Since $\mathfrak{a}$ is a fractional ideal, it is an $\mathcal{O}$-submodule of K, and then it is a $\mathbb{Z}$-submodule of K, that is, an abelian subgroup of the additive group of K. Moreover, by the previous result, there are $\alpha \in K$ and I ideal of $\mathcal{O}$ such that $\mathfrak{a} = \alpha\, I$. By Proposition 2.10, $|\mathcal{O}/I| < \infty$. Since $\mathrm{rank}(\mathcal{O}) = 2$, necessarily we have that $rank(I) = 2$. This leads to $\mathrm{rank}(\mathfrak{a}) = 2$. □

We can also define a product in the set of fractional ideals of an order $\mathcal{O}$ of a quadratic field K in the same way we did for the number ring $\mathcal{O}_K$: If $\mathfrak{a} = \alpha\, I$ and $\mathfrak{b} = \beta\, J$ are fractional ideals of $\mathcal{O}$, we define

$$\mathfrak{a}\,\mathfrak{b} = (\alpha\,\beta)\,(I\,J).$$

This product is well defined and the proof is the same as in the case of $\mathcal{O}_K$. Note also that $\mathcal{O}$ is the identity for this product.

However, there are fractional ideals that are not invertible. If we want to establish a group structure as in the case of the maximal order, we may restrict our set of fractional ideals.

Definition 2.15. *Let K be a quadratic field and let $\mathcal{O}$ be an order of K. We say that a fractional ideal $\mathfrak{a}$ of $\mathcal{O}$ is proper if*

$$\mathcal{O} = \{\beta \in K \mid \beta\,\mathfrak{a} \subset \mathfrak{a}\}.$$

We will prove that the set of proper fractional ideals

$$I(\mathcal{O}) = \{\mathfrak{a} \subset K \mid \mathfrak{a} \text{ is a proper fractional ideal of } \mathcal{O}\}$$

is just the set of invertible fractional ideals of $\mathcal{O}$. Then, it is a group under the natural product of fractional ideals.

Proposition 2.16. *Let K be a quadratic field. Then:*

1. *All principal fractional ideals of an order of K are proper.*
2. *All fractional ideals of $\mathcal{O}_K$ are proper.*

Proof. 1. Let $\mathcal{O}$ be an order of K and let $\mathfrak{a} =< \alpha >_{\mathcal{O}}$ be a principal ideal of $\mathcal{O}$. Given $\beta \in K$, we have that

$$\beta\, I \subset I \Longleftrightarrow \beta\,\alpha \in \mathfrak{a} \Longleftrightarrow \exists a \in \mathcal{O} \,|\, \beta\,\alpha = a\,\alpha \Longleftrightarrow \exists a \in \mathcal{O} \,|\, \beta = a \Longleftrightarrow \beta \in \mathcal{O}.$$

Hence $\mathcal{O} = \{\beta \in K \,|\, \beta\,\mathfrak{a} \subset \mathfrak{a}\}$.

2. Let $\mathfrak{a}$ be a fractional ideal of $\mathcal{O}_K$ and let $\beta \in K$ such that $\beta\,\mathfrak{a} \subset \mathfrak{a}$. We have to prove that $\beta \in \mathcal{O}_K$. Then, $\beta\,\mathfrak{a}\,\mathfrak{a}^{-1} \subset \mathfrak{a}\,\mathfrak{a}^{-1}$, that is, $\beta\,\mathcal{O}_K \subset \mathcal{O}_K$. This implies that $\beta \in \mathcal{O}_K$.

□

Lemma 2.17. *Let τ be an algebraic integer, $K = \mathbb{Q}(\tau)$ and $a\,x^2+b\,x+c = \mathrm{irr}(\tau, x, \mathbb{Q})$ the minimal irreducible polynomial of τ over $\mathbb{Q}$, where $\gcd(a, b, c) = 1$. Then, $\mathcal{O} =< 1, a\,\tau >_{\mathbb{Z}}$ is an order of K and $< 1, \tau >_{\mathbb{Z}}$ is a proper fractional ideal of $\mathcal{O}$.*

Proof. Since $a\,\tau$ is an algebraic integer, $\mathcal{O}$ is an order of K. Let $\beta \in K$. Then,

$$\beta\ < 1, \tau >_{\mathbb{Z}} \subset < 1, \tau >_{\mathbb{Z}} \Longleftrightarrow \beta, \beta\tau \in < 1, \tau >_{\mathbb{Z}}\ .$$

We have that

$$\beta \in < 1, \tau >_{\mathbb{Z}} \Longleftrightarrow \exists m, n \in \mathbb{Z} \,|\, \beta = m + n\,\tau.$$

Since $a\tau^2 + b\tau + c = 0$,

$$\beta\tau = m\tau + n\tau^2 = m\tau + \frac{n}{a}(-b\tau - c) = \frac{-c\,n}{a} + (\frac{-b\,n}{a} + b)\tau.$$

Now, using that $\gcd(a, b, c) = 1$, we obtain that

$$\beta\,\tau \in < 1, \tau >_{\mathbb{Z}} \Longleftrightarrow a | n.$$

It follows that

$$\{\beta \in K \,|\, \beta < 1, \tau >_{\mathbb{Z}} \subset < 1, \tau >_{\mathbb{Z}}\} = \{\beta \in K \,|\, \beta = m + n\tau, m, n \in \mathbb{Z}, a|n\} =< 1, a\tau >_{\mathbb{Z}} = \mathcal{O}.$$

□

Remark 2.18. *By the definition of proper ideal, this lemma gives us an useful property: If $\mathfrak{a} =< 1, \tau >_{\mathbb{Z}}$ is a proper fractional ideal of an order $\mathcal{O}$, then $\mathcal{O} =< 1, a\,\tau >_{\mathbb{Z}}$. Indeed, $\mathfrak{a}$ is a proper fractional ideal of $\mathcal{O}' =< 1, a\,\tau >_{\mathbb{Z}}$, but $\mathfrak{a}$ is proper, so*

$$\mathcal{O} = \{\beta \in K \,|\, \beta\,\mathfrak{a} \subset \mathfrak{a}\} = \mathcal{O}'.$$

Theorem 2.19. *Let $\mathcal{O}$ be an order in a quadratic field K and let $\mathfrak{a}$ be a fractional ideal of $\mathcal{O}$. Then, $\mathfrak{a}$ is proper if and only if $\mathfrak{a}$ is invertible.*

Proof. Assume that $\mathfrak{a}$ is invertible. Then, there exists some fractional ideal $\mathfrak{b}$ of $\mathcal{O}$ such that $\mathfrak{a}\,\mathfrak{b} = \mathcal{O}$. Let $\beta \in K$ such that $\beta\,\mathfrak{a} \subset \mathfrak{a}$. Then,

$$\beta\,\mathcal{O} = \beta\,(\mathfrak{a}\,\mathfrak{b}) = (\beta\,\mathfrak{a})\,\mathfrak{b} \subset \mathfrak{a}\,\mathfrak{b} = \mathcal{O}.$$

Thus $\beta \in \mathcal{O}$. This proves that

$$\mathcal{O} = \{\beta \in K \,|\, \beta\,\mathfrak{a} \subset \mathfrak{a}\}$$

and then $\mathfrak{a}$ is proper.

Now assume that $\mathfrak{a}$ is proper. First, by Proposition 2.14, we know that $\mathfrak{a}$ is a free abelian group of rank 2. Let $\alpha, \beta \in K$ such that $\mathfrak{a} =< \alpha, \beta >_{\mathbb{Z}}$. Denote $\tau = \frac{\beta}{\alpha}$. Then, $\mathfrak{a} = \alpha\ < 1, \tau >_{\mathbb{Z}}$. Let $aX^2 + bX + c$ be the minimal irreducible polynomial of τ over $\mathbb{Q}$ with $\gcd(a, b, c) = 1$ (it has integer coefficients because τ is an algebraic integer). Hence $< 1, \tau >_{\mathbb{Z}}$ is a proper fractional ideal of $\mathcal{O}$. By lemma 2.17, $\mathcal{O} =< 1, a\,\tau >_{\mathbb{Z}}$. Let $\bar{\cdot}$ be the non trivial $\mathbb{Q}$-automorphism of K, which is the complex conjugation. Similarly, since $\overline{\tau}$ is also root of $aX^2 + bX + c$, we obtain that $\overline{\mathfrak{a}} = \overline{\alpha}\ < 1, \overline{\tau} >_{\mathbb{Z}}$, and then $< 1, a\,\tau >=< 1, a\,\overline{\tau} >= \mathcal{O}$.

We claim that

$$\mathfrak{a}\,\overline{\mathfrak{a}} = \frac{N(\alpha)}{a}\,\mathcal{O}.$$

For proving this, first we note that

$$a\,\mathfrak{a}\,\overline{\mathfrak{a}} = a\,\alpha\,\overline{\alpha}\ < 1, \tau >< 1, \overline{\tau} >= N(\alpha) < a, a\,\tau, a\,\overline{\tau}, a\,\tau\,\overline{\tau} >_{\mathbb{Z}}\ .$$

But we know that the coefficients and the roots of the polynomial $aX^2 + bX + c$ of degree 2 are related by $\tau + \overline{\tau} = -\frac{b}{a}$, $\tau\,\overline{\tau} = \frac{c}{a}$. If we put this in the previous expression, we obtain that

$$a\,\mathfrak{a}\,\overline{\mathfrak{a}} = N(\alpha)\ < a, a\,\tau, -b, c >\ .$$

Now, since a, b, c are coprime, they generate $\mathbb{Z}$, so

$$a\,\mathfrak{a}\,\overline{\mathfrak{a}} = N(\alpha)\ < 1, a\,\tau >= N(\alpha)\,\mathcal{O}.$$

and hence the claim. We deduce that

$$\mathfrak{a}\,(\frac{a}{N(\alpha)}\,\overline{\mathfrak{a}}) = \mathcal{O}$$

and therefore $\mathfrak{a}$ is invertible. □

Let us consider

$$P(\mathcal{O}) = \{\mathfrak{a} \in I(\mathcal{O}) \,|\, \mathfrak{a} \text{ is principal}\}.$$

It is easy to check that $P(\mathcal{O})$ is a subgroup of $I(\mathcal{O})$ (the proof is similar to that of the case of $\mathcal{O}_K$), which is normal because $I(\mathcal{O})$ is abelian.

Definition 2.20. *Let K be a quadratic field and let $\mathcal{O}$ be an order of K. The ideal class group of $\mathcal{O}$ is the quotient group*

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

To close this section, we use Proposition 2.10 to generalize the concept of norm of an ideal to ideals of an order of a quadratic field.

Definition 2.21. *Let I be an ideal of $\mathcal{O}$. The norm of I is the integer number*

$$N(I) = |\mathcal{O}/I|.$$

Proposition 2.22. *Let $\mathcal{O}$ be an order of a quadratic field K.*

1. $N(\alpha\,\mathcal{O}) = |N(\alpha)|\ \forall \alpha \in \mathcal{O}, \alpha \neq 0$
2. $I\,\overline{I} = N(I)\,\mathcal{O}$ *for all I proper ideal of $\mathcal{O}$*
3. $N(I \cdot J) = N(I) \cdot N(J)$ *for all I, J proper ideals of $\mathcal{O}$*

Proof. 1. If f is the conductor of $\mathcal{O}$ and $\omega_K = \frac{d_K + \sqrt{d_K}}{2}$, then $\mathcal{O} =< 1, u >_{\mathbb{Z}}$ with $u = f\,\omega_K$. Let $\alpha \in \mathcal{O}$ such that $\alpha \neq 0$. First, we prove that $N(\alpha) = ad - bc$. Let $a, b \in \mathbb{Z}$ such that $\alpha = a + bu$. Then,

$$N(\alpha) = \alpha\,\overline{\alpha} = (a + bu)\,(a + b\overline{u}) = a^2 + a\,b\,(u + \overline{u}) + b^2\,u\,\overline{u}.$$

Since $\alpha\,u \in \mathcal{O}$, there exist $c, d \in \mathbb{Z}$ such that $\alpha\,u = c + du$. But we have also that $\alpha\,u = au + bu^2$, so $b\,u^2 + (a - d)\,u - c = 0$, and then $u^2 + \frac{a-d}{b}\,u - \frac{c}{b} = 0$. This proves that the minimal irreducible polynomial of u over $\mathbb{Q}$ is $f(X) = X^2 + \frac{a-d}{b}\,X - \frac{c}{b}$. Since $\deg(f) = 2$ and the roots of f are u and $\overline{u}$, we deduce that $u + \overline{u} = \frac{d-a}{b}$ and $u\,\overline{u} = -\frac{c}{b}$. Hence,

$$N(\alpha) = a^2 + a\,(d - a) - b\,c = ad - bc.$$

On the other hand, one can prove that

$$|\mathcal{O}/\alpha\,\mathcal{O}| = |ad - bc|.$$

We skip the proof because the techniques are not relevant for the contents in this document (see [6], Exercise 7.14). Then the result follows immediately.

2. Let I be a proper ideal of $\mathcal{O}$. Let us prove first that if $\alpha \in \mathcal{O}$, $\alpha \neq 0$, then $N(\alpha\,I) = N(\alpha)\,N(I)$. Since $\alpha\,I \subset \alpha\,\mathcal{O} \subset \mathcal{O}$, there is a short exact sequence

$$0 \longrightarrow \alpha\,\mathcal{O}/\alpha\,I \longrightarrow \mathcal{O}/\alpha\,I \longrightarrow \mathcal{O}/\alpha\,\mathcal{O} \longrightarrow 0.$$

Then, by the first isomorphism theorem, $|\mathcal{O}/\alpha\,I| = |\mathcal{O}/\alpha\,\mathcal{O}|\,|\alpha\,\mathcal{O}/\alpha\,I|$.

On the other hand, the map $\mathcal{O} \longrightarrow \alpha\,\mathcal{O}$ multiplication by α induces an isomorphism

$$\begin{array}{ccc} \mathcal{O}/I & \longrightarrow & \alpha\,\mathcal{O}/\alpha\,I \\ x + I & \longmapsto & \alpha\,x + \alpha\,I \end{array}.$$

Hence, $|\alpha\,\mathcal{O}/\alpha\,I| = |\mathcal{O}/I|$. Then,

$$N(\alpha\,I) = |\mathcal{O}/\alpha\,I| = |\mathcal{O}/\alpha\,\mathcal{O}|\,|\alpha\,\mathcal{O}/\alpha\,I| = |\mathcal{O}/\alpha\,\mathcal{O}|\,|\mathcal{O}/I| = N(\alpha\,\mathcal{O})\,N(I).$$

Using 1, we obtain that

$$N(\alpha\, I) = N(\alpha)\, N(I).$$

Since $\mathcal{O}/I$ is finite, I is a free abelian group of rank 2. Taking common factor, we can write $I = \alpha\ <1, \tau>_{\mathbb{Z}}$ with $\alpha \in \mathcal{O}$ and $\tau \in K$. Then, by 2.17, $\mathcal{O} =<1, a\,\tau>_{\mathbb{Z}}$, where $a\,X^2 + X + c$ is the minimal polynomial of τ. Now, $N(a\ <1, \tau>_{\mathbb{Z}}) = [<1, a\,\tau>_{\mathbb{Z}}:< a, a\,\tau>_{\mathbb{Z}}] = a$, so $N(<1, \tau>_{\mathbb{Z}}) = \frac{1}{a}$. Hence,

$$N(I) = N(\alpha\ <1, \tau>_{\mathbb{Z}}) = N(\alpha)\, N(<1, \tau>_{\mathbb{Z}}).$$

But we know from Theorem 2.19 that $I\,\overline{I} = \frac{N(\alpha)}{a}\,\mathcal{O}$, so 3 is proved.

3. Let I, J be proper ideals of $\mathcal{O}$. Using 2,

$$N(I\,J)\,\mathcal{O} = I\,J\,(\overline{I\,J}) = (I\,\overline{I})\,(J\,\overline{J}) = (N(I)\,\mathcal{O})\,(N(J)\,\mathcal{O}) = (N(I)\,N(J))\,\mathcal{O}.$$

So $N(I\,J)$ and $N(I)\,N(J)$ are equal up to an unit, and both are positive integers, so they coincide.

□

3.2 Ideals prime to the conductor

We close our study of ideals of an order in an imaginary quadratic field K with the ideals prime to the conductor of the order. This theory will give us an alternative expresion of the ideal class group $\mathcal{C}(\mathcal{O})$ in terms of ideals prime to the conductor of $\mathcal{O}$. After this, we will introduce also the notion of ideal of the maximal order prime to any integer f. When f is the conductor of some order $\mathcal{O}$, we will prove a one-to-one correspondence between both types of ideals. Finally, we will use this correspondence in order to express the ideal class group $\mathcal{C}(\mathcal{O})$ in terms of the ideals of $\mathcal{O}_K$ primes to f. This fact will be important in order to define the ring class field of an imaginary quadratic field K in the next chapter.

To introduce the concept of ideal prime to the conductor, we use the analog of the Bezout identity for integer numbers: If a is coprime to an integer number b, then $a\,\mathbb{Z} + b\,\mathbb{Z} = \mathbb{Z}$.

Definition 2.23. *Let K be a quadratic field and let $\mathcal{O}$ be an order of K with conductor f. We say that a non-zero (integral) ideal I of $\mathcal{O}$ is prime to f if $I + f\,\mathcal{O} = \mathcal{O}$.*

We begin with two elementary properties of this kind of ideals.

Lemma 2.24. *Let K be a quadratic field and let $\mathcal{O}$ be an order of K with conductor f.*

1. *An ideal I of $\mathcal{O}$ is prime to f if and only if $N(I)$ is prime to f.*
2. *If I is an ideal of $\mathcal{O}$ prime to f, then I is proper.*

Proof. 1. Let us define the map

$$\begin{array}{rccc} m_f\colon & \mathcal{O}/I & \longrightarrow & \mathcal{O}/I \\ & \alpha + I & \longmapsto & f\alpha + I \end{array}.$$

It is trivially well defined and it is a ring homomorphism. It follows from the definition of m_f that $I + f\,\mathcal{O} = \mathcal{O}$ if and only if m_f is an epimorphism. Since $\mathcal{O}/I$ is finite, m_f is an epimorphism if and only if it is an isomorphism. But the finiteness of $\mathcal{O}/I$ also implies that $\mathcal{O}/I \cong \mathbb{Z}/n_1\,\mathbb{Z} \times ... \times \mathbb{Z}/n_r\,\mathbb{Z}$, where $n_1 \,...\, n_r = N(I)$. We know that multiplication by f in $\mathbb{Z}/n_i\,\mathbb{Z}$ is an isomorphism if and only if $\gcd(f, n_i) = 1$. Hence, m_f is an isomorphism if and only if $\gcd(f, N(I)) = 1$.

2. Let I be an ideal of $\mathcal{O}$ prime to f. Let $\beta \in K$ such that $\beta\, I \subset I$. Then, $\beta \in \mathcal{O}_K$, so

$$\beta\,\mathcal{O} = \beta\,(I + f\,\mathcal{O}) = \beta\, I + \beta\, f\,\mathcal{O} \subset I + f\,\mathcal{O}_K \subset \mathcal{O}.$$

□

Let I be an ideal of $\mathcal{O}$ that is prime to f. Part 2 of the previous result says that I is a proper ideal, that is, it lies in $I(\mathcal{O})$. Moreover, using 1 and the third part of Proposition 2.22, the product of two ideals prime to f is also prime to f. Let $I(\mathcal{O}, f)$ be the subgroup of $I(\mathcal{O})$ generated by the ideals of $\mathcal{O}$ that are prime to f. As usual, we consider the subgroup $P(\mathcal{O}, f)$ of $I(\mathcal{O}, f)$ generated by principal ideals of $\mathcal{O}$ prime to f. The next result gives us the mentioned expression of $\mathcal{C}(\mathcal{O})$: it is isomorphic to the quotient of $I(\mathcal{O}, f)$ by the principal ideals prime to f.

Lemma 2.25. *Let $\mathcal{O}$ be an order of an imaginary quadratic field K. If M is a non-zero integer, any class of $\mathcal{C}(\mathcal{O})$ contains a proper ideal of $\mathcal{O}$ whose norm is comprime with M.*

The proof of this result follows from a similar result in terms of quadratic forms (see [6], Corollary 7.17).

Proposition 2.26. *The map*

$$\begin{array}{rccc} \Psi\colon & I(\mathcal{O}, f)/P(\mathcal{O}, f) & \longrightarrow & \mathcal{C}(\mathcal{O}) \\ & [I] & \longmapsto & [I] \end{array}.$$

induced by the inclusion is an isomorphism.

Proof. Let us consider

$$\begin{array}{rccc} \psi\colon & I(\mathcal{O}, f) & \longrightarrow & \mathcal{C}(\mathcal{O}) \\ & I & \longmapsto & [I] \end{array}.$$

This map is clearly a group homomorphism and it is surjective: Given $[I] \in \mathcal{C}(\mathcal{O})$, by Lemma 2.25, there exists a proper ideal J of $\mathcal{O}$ in the class of I such that $N(J)$ is prime with f. By part 1 of Lemma 2.24, this implies that J is prime to f, that is, $J \in I(\mathcal{O}, f)$. Hence $\psi(J) = [J] = [I]$.

Now, let us compute $Ker(\psi)$. Let $I \in I(\mathcal{O}, f)$ such that $[I]$ is the trivial class in $\mathcal{C}(\mathcal{O})$. This means that I is principal, so $I \in I(\mathcal{O}, f) \cap P(\mathcal{O})$. Conversely, if $I \in I(\mathcal{O}, f) \cap P(\mathcal{O})$, trivially $I \in Ker(\psi)$. This proves that $Ker(\psi) = I(\mathcal{O}, f) \cap P(\mathcal{O})$.

We claim that $I(\mathcal{O}, f) \cap P(\mathcal{O}) = P(\mathcal{O}, f)$. This implies by first isomorphism theorem that Ψ is an isomorphism.

Note that any ideal of $P(\mathcal{O}, f)$ is in particular an ideal of $\mathcal{O}$ prime to f and also a principal ideal of $\mathcal{O}$. Thus, $P(\mathcal{O}, f) \subset I(\mathcal{O}, f) \cap P(\mathcal{O})$.

Conversely, let $\mathfrak{a} \in I(\mathcal{O}, f) \cap P(\mathcal{O})$. Since $\mathfrak{a} \in I(\mathcal{O}, f)$ there exist I, J ideals of $\mathcal{O}$ prime to f such that $\mathfrak{a} = I\,J^{-1}$. On the other hand, since $\mathfrak{a} \in P(\mathcal{O})$, there exists $\alpha \in K$ such that $\mathfrak{a} = \alpha\,\mathcal{O}$. Let $m = N(J)$. By Proposition 2.22,

$$m\,\mathcal{O} = N(J)\,\mathcal{O} = J\,\overline{J}.$$

Thus, $m\,J^{-1} = \overline{J}$. Then, $m\,\alpha\,\mathcal{O} = I\,m\,J^{-1} = I\,\overline{J} \subset \mathcal{O}$. It follows that $m\,\alpha\,\mathcal{O}$ belongs to $P(\mathcal{O}, f)$. Now,

$$\alpha\,\mathcal{O} = (\alpha\,\mathcal{O})\,(m\,\mathcal{O})\,(m\,\mathcal{O})^{-1} = (m\,\alpha\,\mathcal{O})\,(m\,\mathcal{O})^{-1} \in P(\mathcal{O}, f).$$

□

Now, we introduce the concept of ideals of the maximal order prime to an integer m. The definition is similar to the definition prime to the conductor.

Definition 2.27. *Let I be an ideal of $\mathcal{O}_K$. We say that I is prime to an integer m if $I + m\,\mathcal{O}_K = \mathcal{O}_K$.*

The procedure in this part will be analog to the one that we have just done. First, let us choose an integer number m which is the conductor of some order $\mathcal{O}$ of K. Let f be the conductor of $\mathcal{O}$. We consider the subgroup $I_K(m)$ of $I(\mathcal{O})$ generated by the ideals prime to m and establish an isomorphism between $\mathcal{C}(\mathcal{O})$ and the quotient of $I_K(m)$ by some subgroup $P_{K,\mathbb{Z}}(m)$ of principal ideals. The main difference each principal ideals of $P_{K,\mathbb{Z}(m)}$ has not arbitrary generator: it is going to be congruent with a number coprime to f modulo $f\,\mathcal{O}_K$.

As in the case of the ideals prime to the conductor of the corresponding order, we have the result:

Proposition 2.28. *Let I be an ideal of $\mathcal{O}_K$ and let m be an integer. Then, I is prime to m if and only if* $\gcd(N(I), m) = 1$.

The proof is similar to the proof of 1 of Lemma 2.24, because there we did not use that f is the conductor of the order.

As in the case of ideals prime to the conductor, we deduce that the product of ideals prime to m is again prime to m. Let us denote by $I_K(m)$ the subgroup of I_K generated by the ideals of $\mathcal{O}_K$ prime to m.

When m is the conductor of some order $\mathcal{O}$ in K, ideals of $\mathcal{O}_K$ prime to m are related in a one-to-one correspondence with the ideals of $\mathcal{O}$ prime to m. This correspondence is given by the contraction and the extension of ideals in the ring extension $\mathcal{O} \subset \mathcal{O}_K$.

Proposition 2.29. *Let $\mathcal{O}$ be an order of a quadratic field K.*

1. *If $I \in I_K(f)$, then $I \cap \mathcal{O} \in I(\mathcal{O}, f)$ and $N(I \cap \mathcal{O}) = N(I)$.*
2. *If $I \in I(\mathcal{O}, f)$, then $I\,\mathcal{O}_K \in I_K(f)$ and $N(I\,\mathcal{O}_K) = N(I)$.*
3. *The maps*

$$\begin{array}{rccc} \phi\colon & I_K(f) & \longrightarrow & I(\mathcal{O}, f) \\ & I & \longmapsto & I \cap \mathcal{O} \end{array},$$

$$\begin{array}{rccc} \psi\colon & I(\mathcal{O},f) & \longrightarrow & I_K(f) \\ & I & \longmapsto & I\,\mathcal{O}_K \end{array}$$

are group isomorphisms and inverses to each other.

Proof. 1. Let $I \in I_K(f)$. Let us define

$$\begin{array}{rccc} \varphi\colon & \mathcal{O} & \longrightarrow & \mathcal{O}_K/I \\ & \alpha & \longmapsto & \alpha + I \end{array}.$$

This map is an homomorphism with kernel $\mathcal{O} \cap I$, so using the first isomorphism theorem, $\mathcal{O}/I \cap \mathcal{O}$ is isomorphic to a subgroup of $\mathcal{O}_K/I$. Hence, $N(I \cap \mathcal{O})$ divides $N(I)$ in $\mathbb{Z}$. Since $\gcd(N(I), f) = 1$, we deduce that $\gcd(N(I \cap \mathcal{O}), f) = 1$. Hence $I \cap \mathcal{O} \in I(\mathcal{O}, f)$.

Let us prove that in fact $N(I \cap \mathcal{O}) = N(I)$. Since $f\,\mathcal{O}_K \subset \mathcal{O}$, we have that

$$\mathcal{O}_K/I = (I + f\,\mathcal{O}_K)/I$$

But $(I + f\,\mathcal{O}_K)/I$ can be embedded in $(I + \mathcal{O})/I \cong \mathcal{O}/I \cap \mathcal{O}$. This implies that $N(I)$ divides $N(I \cap \mathcal{O})$. Since both of them are positive integers, $N(I) = N(I \cap \mathcal{O})$.

2./3. Let $I \in I(\mathcal{O}, f)$. Then,

$$I\,\mathcal{O}_K + f\,\mathcal{O}_K = (I + f\,\mathcal{O})\,\mathcal{O}_K = \mathcal{O}\,\mathcal{O}_K = \mathcal{O}_K.$$

Thus, $I\,\mathcal{O}_K \in I_K(f)$. This proves the first part of 2.

Now, let us prove that ϕ and ψ are bijective and inverses to each other. Let $I \in I(\mathcal{O}, f)$. We have to prove that $(I\,\mathcal{O}_K) \cap \mathcal{O} = I$. Indeed, $I \subset (I\,\mathcal{O}_K) \cap \mathcal{O}$ is trivial and conversely,

$$\begin{aligned}(I\,\mathcal{O}_K) \cap \mathcal{O} = ((I\,\mathcal{O}_K) \cap \mathcal{O})\,\mathcal{O} = ((I\,\mathcal{O}_K) \cap \mathcal{O})\,(I + f\,\mathcal{O}) \subset \\ I + f((I\,\mathcal{O}_K) \cap \mathcal{O}) \subset I + I\,f\,\mathcal{O}_K \subset I + I\,\mathcal{O} = I.\end{aligned}$$

On the other hand, let $I \in I_K(f)$. We have to prove that $I = (I \cap \mathcal{O})\,\mathcal{O}_K$. The inclusion $(I \cap \mathcal{O})\,\mathcal{O}_K \subset I$ is trivial. Conversely, since $I \cap \mathcal{O} \in I(f, \mathcal{O})$ by 1,

$$I = I\,\mathcal{O} = I\,(I \cap \mathcal{O} + f\,\mathcal{O}) \subset (I \cap \mathcal{O})\,\mathcal{O}_K + f\,I$$

Now, $f\,I \subset f\,\mathcal{O}_K \subset \mathcal{O}$ and $f\,I \subset I$. Hence $f\,I \subset I \cap \mathcal{O}$, so

$$I \subset (I \cap \mathcal{O})\,\mathcal{O}_K + I \cap \mathcal{O} \subset (I \cap \mathcal{O})\,\mathcal{O}_K.$$

Next, let us prove that $N(I\,\mathcal{O}_K) = N(I)$ for all $I \in I(\mathcal{O}, f)$. Indeed, if $I \in I(\mathcal{O}, f)$, then $I\,\mathcal{O}_K \in I_K(f)$. Using 1, $(I\,\mathcal{O}_K) \cap \mathcal{O} \in I(\mathcal{O}, f)$ and $N((I\mathcal{O}_K) \cap \mathcal{O}) = N(I\,\mathcal{O}_K)$. But we have that $(I\,\mathcal{O}_K) \cap \mathcal{O} = I$ by 2. Hence the required equality follows.

Finally, we prove that ϕ and ψ are group homomorphisms. This is trivial for ψ. Since ϕ and ψ are inverses one to the other, we can prove it easily for ϕ:

$$\phi(I\,J) = \phi(\psi(\phi(I))\,\psi(\phi(J))) = \phi(\psi(\phi(I)\,\phi(J))) = \phi(I)\,\phi(J).$$

That completes the proof.

□

The next step is to identify the subgroup $P_{K,\mathbb{Z}}(f)$ of $I_K(f)$ that we mentioned before. Instead of choosing the subgroup generated by all principal ideals of $\mathcal{O}_K$ prime to f, we choose those of the form $\alpha\,\mathcal{O}_K$ with $\alpha \equiv a \,(\mathrm{mod}\, f\,\mathcal{O}_K)$ for some $a \in \mathbb{Z}$ prime to f. All this ideals are prime to f. Indeed, if $\alpha \equiv a \,(\mathrm{mod}\, f\,\mathcal{O}_K)$ with a as before, then $\alpha - a = f\,x$ with $x \in \mathcal{O}_K$. On the other hand, Bezout identity gives us that $r\,a + s\,f = 1$ with $r, s \in \mathbb{Z}$. Then $1 = (\alpha - f\,x)\,r + f\,s = \alpha\,r + f\,(s - r\,x) \in \alpha\,\mathcal{O}_K + f\,\mathcal{O}_K$, so $\mathcal{O}_K = \alpha\,\mathcal{O}_K + f\,\mathcal{O}_K$. The group generated of all principal ideals of this form is denoted by $P_{K,\mathbb{Z}}(f)$.

At this point, we have all the ingredients to prove that $\mathcal{C}(\mathcal{O})$ is the quotient of $I_K(f)$ by $P_{K,\mathbb{Z}}(f)$. We need the following lemma:

Lemma 2.30. *Let K be an imaginary quadratic field and let $\alpha, \beta \in \mathcal{O}_K$ such that $\alpha \equiv \beta \,(\mathrm{mod}\, m\,\mathcal{O}_K)$ for some $m \in \mathbb{Z}$. Then $N(\alpha) \equiv N(\beta) \,(\mathrm{mod}\, m)$.*

Proof. Since K is an imaginary quadratic field, $N(\alpha) = \alpha\,\overline{\alpha}$ and $N(\beta) = \beta\,\overline{\beta}$. Then,

$$N(\alpha) - N(\beta) = \alpha\,\overline{\alpha} - \beta\,\overline{\beta} = \alpha\,\overline{\alpha} - \alpha\,\overline{\beta} + \alpha\,\overline{\beta} - \beta\,\overline{\beta} = \alpha\,(\overline{\alpha - \beta}) + \overline{\beta}\,(\alpha - \beta).$$

Now, since $\alpha \equiv \beta \,(\mathrm{mod}\, m\,\mathcal{O}_K)$, there exists $x \in \mathcal{O}_K$ such that $\alpha - \beta = m\,x$. Then,

$$N(\alpha) - N(\beta) = \alpha\overline{m\,x} + \overline{\beta}\,m\,x = m(\alpha\,\overline{x} + \overline{\beta}\,x),$$

where we have used that m is its own conjugate (because it is an integer number).

It remains to prove that $\alpha\,\overline{x} + \overline{\beta}\,x \in \mathbb{Z}$. Since α, β and $\overline{x}$ lie in $\mathcal{O}_K$, $\alpha\,\overline{x} + \overline{\beta}\,x \in \mathcal{O}_K$ (note that $\overline{x} \in K$ because it is the conjugate of x and K is normal).

We claim that $\alpha\,\overline{x} + \overline{\beta}\,x \in \mathcal{O}_K$ is fixed by the complex conjugation. This will be enough for proving the result, because since K is imaginary quadratic, $\mathcal{O}_K \cap \mathbb{R} = \mathbb{Z}$. Indeed, from the trivial identity $m\,\overline{x}\,x = m\,x\,\overline{x}$ follows that $(\overline{\alpha - \beta})\,x = (\alpha - \beta)\,\overline{x}$ (we use again that m is its own conjugate). From here, we deduce that $\overline{\alpha}\,x - \overline{\beta}\,x = \alpha\,\overline{x} - \beta\,\overline{x}$. This is equivalent to

$$\overline{\alpha}\,x + \beta\,\overline{x} = \alpha\,\overline{x} + \overline{\beta}\,x,$$

which completes the proof. □

Proposition 2.31. *Let $\mathcal{O}$ be an order of an imaginary quadratic field K with conductor f. Then, the map*

$$\begin{array}{rccc} \Phi\colon & I_K(f)/P_{K,\mathbb{Z}}(f) & \longrightarrow & \mathcal{C}(\mathcal{O}) \\ & [I] & \longmapsto & [I] \end{array}.$$

induced by the inclusion is an isomorphism.

Proof. We proved in the previous proposition that

$$\begin{array}{rccc} \psi\colon & I(\mathcal{O}, f) & \longrightarrow & I_K(f) \\ & I & \longmapsto & I\,\mathcal{O}_K \end{array}$$

is a group isomorphism. If we prove that $\psi(P(\mathcal{O}, f)) = P_{K,\mathbb{Z}}(f)$, then we compose the inverse of the induced isomorphism $I(\mathcal{O}, f)/P(\mathcal{O}, f) \longrightarrow I_K(f)/P_{K,\mathbb{Z}}(f)$ with the map Ψ of Proposition 2.26 and we are done.

We know that $P(\mathcal{O}, f)$ is generated by the ideals $\alpha\,\mathcal{O}$ with $\alpha \in \mathcal{O}$ and $N(\alpha)$ coprime with f, and $\psi(\alpha\,\mathcal{O}) = \alpha\,\mathcal{O}_K$. Then, we have to prove that for $\alpha \in \mathcal{O}$, $\gcd(N(\alpha), f) = 1$ is equivalent to $\alpha \equiv a (\mathrm{mod}\, f\,\mathcal{O}_K)$ with $a \in \mathbb{Z}$ prime to f.

Assume that $\alpha \equiv a \,(\mathrm{mod}\, f\,\mathcal{O}_K)$ with $a \in \mathbb{Z}$ prime to f. By the previous lemma, $N(\alpha) \equiv a^2 \,(\mathrm{mod}\, f)$. Hence $\gcd(N(\alpha), f) = \gcd(a^2, f) = 1$. Conversely, assume that $\gcd(N(\alpha), f) = 1$. Now, $\mathcal{O} =< 1, f\,\omega_K >_{\mathbb{Z}}$. Then there exist $a, b \in \mathbb{Z}$ such that $\alpha = a + b\,f\,\omega_K$, and hence $\alpha \equiv a \,(\mathrm{mod}\, f\,\mathcal{O}_K)$. Since $\gcd(N(\alpha), f) = 1$ and $N(\alpha) \equiv a^2 \,(\mathrm{mod}\, f)$, we obtain that $\gcd(a, f) = 1$.

After this, we obtain that $\psi(P(\mathcal{O}, f))$ is generated by the ideals $\alpha\,\mathcal{O}_K$, where $\alpha \equiv a \,(\mathrm{mod}\, f\,\mathcal{O}_K)$ for some $a \in \mathbb{Z}$ prime with f. That is, $\psi(P(\mathcal{O}, f)) = P_{K,\mathbb{Z}}(f)$. □

Remember that an order in general is not a Dedekind domain and does not satisfy the unique factorization property of ideals. We can use the relation given by the previous result to prove that the ideals prime to the conductor of an order factorize uniquely as a product of ideals of the order again prime to the conductor (see [6], Exercise 7.26).

Chapter 3

Class field theory

In this chapter we present the classical formulation of Class Field Theory. As we mentioned before, the theorems of Class Field Theory provide the structure of abelian extensions of a number field K by using the arithmetic of K. This formulation describes the Galois groups of abelian extensions of K in terms of generalized ideal class groups. The main reference used in this chapter is [6].

In the first section, we begin with a particular case of abelian extension, which is the Hilbert Class Field. Concretely, the Hilbert Class Field of K is the maximal unramified abelian extension of K. We are going to construct also the Artin map of the Hilbert Class Field and state the Artin Reciprocity Theorem for the Hilbert Class Field. This has a natural generalization via the modulus of a number field, that are formal products of primes of the number fields.

In the second section we state the main results such as the general Artin Reciprocity Theorem and the Existence Theorem. The last one allows us to obtain certain abelian extensions of number fields, called class fields, in terms of modulus. The Hilbert Class Field is nothing but a particular case of class field. Using this theory we will also introduce the Ray Class Field of a number field K for a modulus of K.

After this, we will introduce the Dirichlet density and state the Chebotarev density Theorem. This is an useful tool to prove the existence of primes with certain properties. On that line, we apply this result to prove a Class-Field-Theory version of Dirichlet Theorem in arithmetic progressions and to characterize a Galois extension of a number field K in terms of the splitting primes of K.

Finally, we relate the theory of orders introduced in the previous chapter with the class field theory in order to define the Ring Class Fields of an imaginary quadratic field K, that depend on an order of K.

Both Hilbert Class Fields and Ray Class Fields are not given in an explicit form by this theory. In Part 2 of this thesis we will give explicit constructions when K is an imaginary quadratic field, which is fundamental to solve *Kronecker's Jugendtraum* in the imaginary-quadratic case.

1 The Hilbert Class Field

Recall that a field extension L/K is said to be abelian provided that it is Galois and $\mathrm{Gal}(L/K)$ is abelian.

In this section we are going to introduce the Hilbert Class Field and study its main properties. It represents a good particular case of the general situation in class field theory. We will define the Hilbert Class Field of a number field K as the maximal unramified abelian extension of K. But here ramification does not take into account only the prime ideals of the ring of integers of K. These are called finite primes, but we consider also infinite primes.

Definition 3.1. *Let K be a number field. A real infinite prime is an embedding $\sigma : K \longrightarrow \mathbb{R}$ and an imaginary infinite prime is a pair of conjugate embeddings $\sigma, \overline{\sigma} : K \longrightarrow \mathbb{C}$.*

Once we have defined the concept of infinite prime, it would be logic to define a ramified extension as an extension L/K where some prime of K ramifies in L. In Chapter 1 we established the meaning of a finite prime of K ramifying in L. Now, we proceed to define the ramification for infinite primes.

Definition 3.2. *Let L/K be an extension of number fields. We say that an infinite prime σ of K ramifies in L if it is real and has some extension to L which is complex.*

Remark 3.3. *An infinite prime σ of K does not ramify in L if it is imaginary or all its extensions to L are real.*

With these new concepts, we can introduce ramified extensions.

Definition 3.4. *Let L/K be an extension of number fields. We say that L/K is ramified if some prime (finite or infinite) of K ramifies in L. Otherwise, we say that L/K is unramified.*

Unramified primes of an extension L/K of number fields have better properties that the ramified ones. For this reason, it is easier to deal with unramified extensions.

Theorem 3.5. *Let K be a number field. Then, there is an unique finite Galois extension L of K such that:*

1. *L/K is abelian and unramified.*
2. *Any abelian unramified extension of K is contained in L.*

This field L is called the Hilbert Class Field of K.

This result will follow from the results we will present in the next secion. The main aim of this section is to obtain information about the Hilbert Class Field using the ideal class group of the base number field K. This is a good example of the idea of class field theory: to say something about an abelian extension just using the arithmetic of the base field.

We can generalize the Artin symbol introduced in Chapter 1 for abelian unramified extensions. Let L/K be an abelian unramified extension of number fields. Let $\mathfrak{a}$ be a fractional ideal of K. Then, $\mathfrak{a}$ has an unique factorization

$$\mathfrak{a} = P_1^{r_1} ... P_k^{r_k},$$

where $P_1, .., P_k$ are prime ideals of $\mathcal{O}_K$ and $r_1, ..., r_k \in \mathbb{Z}$. Thus, we can define the Artin symbol of $\mathfrak{a}$ as

$$\left(\frac{L/K}{\mathfrak{a}}\right) = \prod_{i=1}^{k} \left(\frac{L/K}{P_i}\right)^{r_i},$$

where the product is that of the Galois group $\mathrm{Gal}(L/K)$.

Thus, we have a map

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

which is called the Artin map of the extension L/K.

Remark 3.6. *We need the extension L/K to be unramified because the Artin symbol of L/K over a prime P is only defined when P is unramified in L. In the next section we remove this condition and consider the Artin map defined over the unramified ideals of $\mathcal{O}_K$.*

When we take L as the Hilbert Class Field of K, we obtain a very nice result for the Artin map of this extension.

Theorem 3.7 (**Artin Reciprocity Theorem for the Hilbert Class Field**). *Let K be a number field and let L be its Hilbert Class Field. Then, $\left(\frac{L/K}{\cdot}\right) : I_K \longrightarrow \mathrm{Gal}(L/K)$ is a group epimorphism with $Ker(\left(\frac{L/K}{\cdot}\right)) = P_K$. Thus, it induces an isomorphism*

$$\begin{array}{rccc} \Phi\colon & \mathcal{C}(\mathcal{O}_K) & \longrightarrow & \mathrm{Gal}(L/K) \\ & [I] & \longmapsto & \left(\frac{L/K}{I}\right) \end{array}.$$

This statement will be proved also in the next section. It allows us to establish a one-to-one correspondence between the unramified abelian extensions of K and the subgroups of $\mathcal{C}(\mathcal{O}_K)$.

Corollary 3.8. *Let K be a number field and let L be the Hilbert Class Field of K. Then, there is a one-to-one correspondence between the sets*

$$\mathcal{L} = \{M \subset L \,|\, M \text{ abelian unramified extension of } K\},$$
$$\mathcal{S} = \{H \subset \mathcal{C}(\mathcal{O}_K) \,|\, H \text{ is subgroup of } \mathcal{C}(\mathcal{O}_K)\}.$$

Proof. It is a direct consequence of the fundamental theorem of Galois theory. □

This illustrates the kind of results we obtain in class field theory: we classify some class of extensions of K in terms of intrinsic information of K, which is the ideal class group.

We have another useful consequence.

Corollary 3.9. *Let K be a number field and let L be the Hilbert Class Field of K. Let P be a prime ideal of $\mathcal{O}_K$. Then, P splits completely in L if and only if P is a principal ideal.*

Proof. We know by Proposition 1.8 that P splits completely in L if and only if $\left(\frac{L/K}{P}\right) = 1$. But $\left(\frac{L/K}{P}\right) = \Phi([P])$ and by Theorem 3.7, Φ is an isomorphism. Hence P splits completely in L if and only if $[P]$ is the trivial class, which is equivalent to saying that P is a principal ideal. □

2 The main statements

In this section we are going to present (without proof) the general statements of class field theory that we will need.

We are going to define generalized ideal class groups for a number field K, which will be quotients of modules described in terms of the primes of K. The main idea is that these ideal class groups are the Galois groups of all abelian extensions of K and this connection is provided by the Artin maps of the abelian extensions.

A basic object in the classical formulation of class field theory is that of modulus in a number field.

Definition 3.10. *Let K be a number field. A modulus in K is said to be a formal product*

$$\mathfrak{m} = \prod_P P^{n_P}$$

taken in the set of primes (finite or infinite) of K such that the powers n_P are integers that satisfy:

1. *$n_P \geq 0$ for all P and $n_P = 0$ for almost every P.*
2. *If P is a complex infinite prime, then $n_P = 0$.*
3. *If P is a real infinite prime, then $n_P \leq 1$.*

A modulus $\mathfrak{m}$ can be written in the form $\mathfrak{m} = \mathfrak{m}_0\,\mathfrak{m}_\infty$, where $\mathfrak{m}_0$ is the formal product of all finite primes and $\mathfrak{m}_\infty$ is the formal product of all infinite primes.

Given a prime P with $n_P > 0$ we will say that P divides $\mathfrak{m}$. Let $\mathfrak{m} = \prod_P P^{n_{P,\mathfrak{m}}}$ and $\mathfrak{n} = \prod_P P^{n_{P,\mathfrak{n}}}$ be two modulus of K. We say that $\mathfrak{m}$ divides $\mathfrak{n}$, denoted by $\mathfrak{m}|\mathfrak{n}$, if for all prime P that divides $\mathfrak{m}$, we have that P divides $\mathfrak{n}$ and $n_{P,\mathfrak{m}} \leq n_{P,\mathfrak{n}}$. It is clear after the defitions that

$$\mathfrak{m}|\mathfrak{n} \Longrightarrow \mathfrak{m}_0|\mathfrak{n}_0 \text{ and } \mathfrak{m}_\infty|\mathfrak{n}_\infty.$$

Note that given any modulus $\mathfrak{m}$ of K, the modulus $\mathfrak{m}_0$ can be naturally identified with an (integral) ideal of $\mathcal{O}_K$, because the primes that divide $\mathfrak{m}$ are all finite (that is, prime ideals of $\mathcal{O}_K$) and there are finitely many.

Note that if K is an imaginary quadratic field, then it has one infinite prime: the pair form by the identity and the complex conjugation. Thus, a modulus of K has no infinite part because the only infinite prime is complex and it has power 0.

Let $\mathfrak{m}$ be a modulus and let $I_K(\mathfrak{m})$ be the group of all fractional ideals of $\mathcal{O}_K$ which are relatively prime to the finite primes dividing $\mathfrak{m}$. Let $P_{K,1}(\mathfrak{m})$ be the subgroup of $I_K(\mathfrak{m})$ generated by the principal ideals $\alpha\,\mathcal{O}_K$ that satisfy:

1. For any prime ideal P such that $n_P > 0$, we have that $\alpha \equiv 1 \pmod{P^{n_P}}$.
2. Given a real infinite prime σ with $n_\sigma > 0$, it holds that $\sigma(\alpha) > 0$.

Definition 3.11. *A congruence subgroup for a modulus $\mathfrak{m}$ is a subgroup H of $I_K(\mathfrak{m})$ such that $P_{K,1}(\mathfrak{m}) \subset H$.*

Let H be a congruence subgroup for $\mathfrak{m}$. Since the group $I_K(\mathfrak{m})$ is abelian, H is a normal subgroup and the quotient $I_K(\mathfrak{m})/H$ makes sense. Moreover, one can prove that the index $[I_K(\mathfrak{m}) : P_{K,1}(\mathfrak{m})]$ is finite. Hence $I_K(\mathfrak{m})/H$ is a finite group.

Definition 3.12. *A generalized ideal class group for a modulus* $\mathfrak{m}$ *is any group of the form* $I_K(\mathfrak{m})/H$*, where* H *is a congruence subgroup of* $\mathfrak{m}$*.*

Now, we proceed to define the Artin map of any abelian extension L/K. Let $\mathfrak{m}$ be a modulus of K divisible by all primes of K that ramify in L. Actually we will define a map for each modulus $\mathfrak{m}$ of this type. The procedure is completely analog to what we do to define the Artin map of an abelian unramified extension. Let $\mathfrak{a} \in I_K(\mathfrak{m})$. Then $\mathfrak{a}$ factorizes uniquely as a product of prime ideals

$$\mathfrak{a} = P_1^{\alpha_1} ... P_k^{\alpha_k},$$

where $\alpha_1, ..., \alpha_k \in \mathbb{Z}$. Then, it is natural to define the Artin symbol of L/K over $\mathfrak{a}$ as

$$\left(\frac{L/K}{\mathfrak{a}}\right) = \prod_{i=1}^{k} \left(\frac{L/K}{P_i}\right)^{\alpha_i}.$$

We may make sure that this defition is correct. By defition of $I_K(\mathfrak{m})$, $\mathfrak{a}$ is prime with $\mathfrak{m}$. Then, none of the primes $P_1, ..., P_K$ divide $\mathfrak{m}$, that is, $n_{P_i} = 0$ for all $i \in \{1, ..., k\}$. Since $\mathfrak{m}$ is divisible by all primes of K that ramify in L, we deduce that $P_1, ..., P_K$ are unramified in L. Therefore, the Artin symbols $\left(\frac{L/K}{P_i}\right)$ are defined.

When $\mathfrak{m} =< 1 >$, then $I_K(< 1 >) = I_K$, so this definition of the Artin symbol coincides with the one we gave in the previous section.

Definition 3.13. *Let* L/K *be an abelian extension of number fields and let* $\mathfrak{m}$ *be a modulus of* K *divisible by all primes of* K *that ramify in* L*. The Artin map of* L/K *for* $\mathfrak{m}$ *is the map*

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

which sends each $\mathfrak{a} \in I(\mathfrak{m})$ *to the Artin symbol* $\left(\frac{L/K}{\mathfrak{a}}\right)$*.*

If L/K is an abelian unramified extension of number fields, the Artin map of L/K for the modulus $\mathfrak{m} =< 1 >$ sends every $\mathfrak{a} \in I_K$ to the Artin symbol $\left(\frac{L/K}{\mathfrak{a}}\right)$, so this definition coincides with the definition of Artin map given in the previous section.

When we only deal with a single abelian extension L/K, it is usual to denote the Artin map for L/K over $\mathfrak{m}$ as $\Phi_{\mathfrak{m}}$ instead of $\Phi_{L/K,\mathfrak{m}}$.

Let L/K be an abelian extension of number fields. Let $\mathfrak{m}$, $\mathfrak{n}$ be modulus of K such that $\mathfrak{m}|\mathfrak{n}$ and $\mathfrak{m}$ is divisible by all primes of K that ramify in L (then so is $\mathfrak{n}$). Then any fractional ideal coprime with $\mathfrak{n}$ is also coprime with $\mathfrak{m}$, that is, $I_K(\mathfrak{n}) \subset I_K(\mathfrak{m})$. Since the Artin map of L/K for a given modulus depends only on the Artin symbols of L/K over the finite primes of K, we deduce that $\Phi_{\mathfrak{m}}|_{I_K(\mathfrak{n})} = \Phi_{\mathfrak{n}}$.

Now, we state the general Artin Reciprocity Theorem for any abelian extension L/K of number fields.

Theorem 3.14 (**Artin Reciprocity Theorem**). *Let L/K be an abelian extension of number fields and let $\mathfrak{m}$ be a modulus of K divisible by all the primes of K that ramify in L. Then:*

1. *$\Phi_{\mathfrak{m}}$ is surjective, and as a consequence, we have a group isomorphism*

$$\begin{array}{ccc} I_K(\mathfrak{m})/\operatorname{Ker}(\Phi_{\mathfrak{m}}) & \longrightarrow & \operatorname{Gal}(L/K) \\ [\mathfrak{a}] & \longmapsto & \left(\frac{L/K}{\mathfrak{a}}\right) \end{array}$$

2. *If the powers of the finite primes dividing $\mathfrak{m}$ are large enough, then $\operatorname{Ker}(\Phi_{\mathfrak{m}})$ is a congruence subgroup for $\mathfrak{m}$, so $\operatorname{Gal}(L/K)$ is a generalized ideal class group of $\mathfrak{m}$.*

As in the case of the Hilbert Class Field, this result allows us to characterize the splitting primes of K in a given abelian extension.

Corollary 3.15. *Let L/K be an abelian extension of number fields. Let P be a prime of K which is unramified in L. Then,*

$$\left(\frac{L/K}{P}\right) = 1 \Longleftrightarrow P \text{ is principal.}$$

The proof is completely analogous to the proof of Corollary 3.9.

Fixed an abelian extension L/K of number fields, there is not an unique modulus $\mathfrak{m}$ divisible by all primes of K that ramify in L such that $\operatorname{Ker}(\Phi_{\mathfrak{m}})$ is congruence subgroup for $\mathfrak{m}$. In fact, the following result gives us that there are infinitely many.

Proposition 3.16. *Let L/K be an abelian extension and let $\mathfrak{m}$ be a modulus of K divisible by all primes of K that ramify in L such that $\operatorname{Ker}(\Phi_{\mathfrak{m}})$ is a congruence subgroup for $\mathfrak{m}$. Let $\mathfrak{n}$ be another modulus of K for which $\mathfrak{m}|\mathfrak{n}$. Then, $\operatorname{Ker}(\Phi_{\mathfrak{n}})$ is a congruence subgroup for $\mathfrak{n}$.*

Proof. Let us prove that $P_{K,1}(\mathfrak{n}) \subset \operatorname{Ker}(\Phi_{\mathfrak{n}})$. Let $\mathfrak{a} \in P_{K,1}(\mathfrak{n})$. First of all, recall that since $\mathfrak{m}|\mathfrak{n}$, $I_K(\mathfrak{n}) \subset I_K(\mathfrak{m})$. By the definition of $P_{K,1}(\mathfrak{m})$, we have that $\mathfrak{a} =< \alpha >$, with $\alpha \equiv 1 \pmod{\mathfrak{n}_0}$ and $\sigma(\alpha) > 0$ for all σ dividing $\mathfrak{n}_\infty$. Since $\mathfrak{m}|\mathfrak{n}$, we have that $\mathfrak{m}_0|\mathfrak{n}_0$ and $\mathfrak{m}_\infty|\mathfrak{n}_\infty$. The first of these facts imply that $\alpha - 1 \in \mathfrak{n}_0 \subset \mathfrak{m}_0$, so we deduce that $\alpha \equiv 1 \pmod{\mathfrak{m}_0}$. From the second one we trivially obtain that $\sigma(\alpha) > 0$ for all σ dividing $\mathfrak{m}_0$. This proves that $\mathfrak{a} \in P_{K,1}(\mathfrak{m})$. Since $\operatorname{Ker}(\Phi_{\mathfrak{m}})$ is a congruence subgroup for $\mathfrak{m}$, $\mathfrak{a} \in \operatorname{Ker}(\Phi_{\mathfrak{m}})$. Hence, using that the Artin symbol for $\mathfrak{n}$ is the restriction of the Artin symbol for $\mathfrak{m}$ to $I_K(\mathfrak{n})$, we obtain that

$$\Phi_{\mathfrak{n}}(\mathfrak{a}) = \Phi_{\mathfrak{m}}(\mathfrak{a}) = 1.$$

This says that $\mathfrak{a} \in \operatorname{Ker}(\Phi_{\mathfrak{n}})$, which completes the proof. □

After this result, it is clear that if there is a modulus $\mathfrak{m}$ divisible by all primes of K that ramify in L for which $\operatorname{Ker}(\Phi_{\mathfrak{m}})$ is a congruence subgroup for $\mathfrak{m}$, then there are infinitely many, because there are infinitely many modulus $\mathfrak{n}$ such that $\mathfrak{m}|\mathfrak{n}$. The following theorem asserts that indeed there is such a modulus and it is a minimal modulus for this property.

Theorem 3.17. *Let L/K be an abelian extension. Then, there exists a modulus $\mathfrak{f}$ of K such that:*

1. *If P is a prime of K, then P ramifies in L if and only if P divides $\mathfrak{f}$.*
2. *If $\mathfrak{m}$ is a modulus divisible by all primes of K which ramify in L, $\mathrm{Ker}(\Phi_{\mathfrak{m}})$ is a congruence subgroup for $\mathfrak{m}$ if and only if $\mathfrak{f}$ divides $\mathfrak{m}$.*

Remark 3.18. *Fixed the abelian extension L/K, $\mathfrak{f}$ is unique. Indeed, let $\mathfrak{f}'$ is another modulus of K satisfying 1 and 2. Since $\mathfrak{f}$ (resp. $\mathfrak{f}'$) is a conductor and it is divisible by itself, $\mathrm{Ker}(\Phi_{\mathfrak{f}})$ (resp. $\mathrm{Ker}(\Phi_{\mathfrak{f}'})$) is a congruence subgroup for $\mathfrak{f}$ (resp. $\mathfrak{f}'$). Now, we use that $\mathfrak{f}$ is a conductor with $\mathfrak{m} = \mathfrak{f}'$. By 2, $\mathfrak{f}$ divides $\mathfrak{f}'$. Similarly, using that $\mathfrak{f}'$ is a conductor with $\mathfrak{m} = \mathfrak{f}$, we obtain that $\mathfrak{f}'$ divides $\mathfrak{f}$. Hence, $\mathfrak{f} = \mathfrak{f}'$.*

Definition 3.19. *The modulus $\mathfrak{f} = \mathfrak{f}(L/K)$ is called the conductor of the abelian extension L/K.*

The key result of class field theory that we will need is the following.

Theorem 3.20. ***(Existence Theorem)*** *Let $\mathfrak{m}$ be a modulus of K and let H be a congruence subgroup for $\mathfrak{m}$. Then, there is an unique abelian extension L of K such that $\mathfrak{m}$ is divisible by all primes of K that ramify in L and $H = \mathrm{Ker}(\Phi_{\mathfrak{m}})$, where $\Phi_{\mathfrak{m}}$ is the Artin map of the extension L/K.*

Remark 3.21. *Under the conditions of the Existence Theorem, we have that the Artin map $\Phi_{\mathfrak{m}}$ induces an isomorphism $I_K(\mathfrak{m})/H \cong \mathrm{Gal}(L/K)$. Indeed, by Existence Theorem, we have that $H = \mathrm{Ker}(\Phi_{\mathfrak{m}})$. On the other hand, $\mathfrak{m}$ is divisible by all primes of K that ramify in L, so the claim follows from Artin Reciprocity Theorem.*

We can appreciate here again the idea of class field theory: This result allows us to define abelian extensions of a number field and describe their Galois groups just by using generalized ideal class groups of a modulus of the number field.

Proposition 3.22. *Let K be a number field and let L, M be abelian extensions of K. Then $L \subset M$ if and only if there is a modulus $\mathfrak{m}$ of K divisible by all primes of K that ramify in either L or M such that*

$$P_{K,1}(\mathfrak{m}) \subset \mathrm{Ker}(\Phi_{M/K,\mathfrak{m}}) \subset \mathrm{Ker}(\Phi_{L/K,\mathfrak{m}}).$$

Proof. Let us assume that $L \subset M$. By the comment after Proposition 3.16 applied separately to L/K and M/K:

- There is a modulus $\mathfrak{m}_1$ of K divisible by all primes of K that ramify in L such that $\mathrm{Ker}(\Phi_{\mathfrak{m}_1})$ is a congruence subgroup for $\mathfrak{m}_1$.
- There is a modulus $\mathfrak{m}_2$ of K divisible by all primes of K that ramify in M such that $\mathrm{Ker}(\Phi_{\mathfrak{m}_2})$ is a congruence subgroup for $\mathfrak{m}_2$.

Let $\mathfrak{m} = \mathfrak{m}_1\,\mathfrak{m}_2$. It is clearly a modulus of K. Since $\mathfrak{m}_1|\mathfrak{m}$, an argument as in the proof of Proposition shows that $P_{K,1}(\mathfrak{m}) \subset P_{K,1}(\mathfrak{m}_1)$. Moreover, we have also that $\Phi_{L/K,\mathfrak{m}_1} = \Phi_{L/K,\mathfrak{m}}|_{I_K(\mathfrak{m}_1)}$, so $\mathrm{Ker}(\Phi_{L/K,\mathfrak{m}_1}) \subset \mathrm{Ker}(\Phi_{L/K,\mathfrak{m}})$. Thus, we have the chain of inclussions

$$P_{K,1}(\mathfrak{m}) \subset P_{K,1}(\mathfrak{m}_1) \subset \mathrm{Ker}(\Phi_{L/K,\mathfrak{m}_1}) \subset \mathrm{Ker}(\Phi_{L/K,\mathfrak{m}}),$$

which proves that $\mathrm{Ker}(\Phi_{L/K,\mathfrak{m}})$ is a congruence subgroup for $\mathfrak{m}$. A similar argument shows that it is also a congruence subgroup for $\mathrm{Ker}(\Phi_{M/K,\mathfrak{m}})$.

Let $r : \mathrm{Gal}(M/K) \longrightarrow \mathrm{Gal}(L/K)$ be the restriction homormorphism. A straightforward calculation shows that $r \circ \Phi_{M/K,\mathfrak{m}} = \Phi_{L/K,\mathfrak{m}}$ (see [6], Exercise 5.16). Then, $\mathrm{Ker}(\Phi_{M/K,\mathfrak{m}}) \subset \mathrm{Ker}(\Phi_{L/K,\mathfrak{m}})$.

Conversely, let us assume that

$$P_{K,1}(\mathfrak{m}) \subset Ker(\Phi_{M/K,\mathfrak{m}}) \subset \mathrm{Ker}(\Phi_{L/K,\mathfrak{m}}).$$

Let $H = \Phi_{M/K,\mathfrak{m}}(\mathrm{Ker}(\Phi_{L/K,\mathfrak{m}}))$, which is a subgroup of $\mathrm{Gal}(M/K)$. By the fundamental theorem of Galois theory, H correspond to an intermediate field $\widetilde{L} = M^H$ of the extension M/K. Now, if we apply the first part of the proof to $\widetilde{L} \subset M$, we obtain that $\mathrm{Ker}(\Phi_{M/K,\mathfrak{m}}) \subset \mathrm{Ker}(\Phi_{\widetilde{L}/K,\mathfrak{m}})$, so $\mathrm{Ker}(\Phi_{\widetilde{L}/K,\mathfrak{m}}) = \mathrm{Ker}(\Phi_{L/K,\mathfrak{m}})$.

Thus, both L and $\widetilde{L}$ are abelian extensions of K such that $\mathrm{Ker}(\Phi_{\widetilde{L}/K,\mathfrak{m}}) = \mathrm{Ker}(\Phi_{L/K,\mathfrak{m}})$ and $\mathfrak{m}$ is divisible by all primes of K that ramify in L. By the Artin Reciprocity Theorem 3.14, $\mathrm{Gal}(L/K) \cong I_K(\mathfrak{m})/\,\mathrm{Ker}(\Phi_{L/K,\mathfrak{m}})$. Hence, by the uniqueness in the Existence Theorem, $L = \widetilde{L} \subset M$. □

Definition 3.23. *Let $\mathfrak{m}$ be a modulus of K and let H be a congruence subgroup for $\mathfrak{m}$. The field L of the Existence Theorem is called the class field of H.*

Now, we are ready to prove the existence and uniqueness of the Hilbert Class Field and the Artin Reciprocity Theorem for the Hilbert Class Field.

Proof. (of theorems 3.5 and 3.7)

Let us consider the modulus $\mathfrak{m} =< 1 >$ of the number field K. Then $I_K(\mathfrak{m}) = I_K$, and the subgroup P_K of the principal ideals of I_K is a congruence subgroup of I_K. Now, we apply the Existence Theorem to P_K and $\mathfrak{m}$. Then, there exists an unique abelian extension L of K such that $\mathfrak{m}$ is divisible by all primes of K that ramify in L and $P_K = \mathrm{Ker}(\Phi_{L/K,\mathfrak{m}})$.

Since $\mathfrak{m} =< 1 >$, no prime of K divide $\mathfrak{m}$, so no prime of K ramify in L. In other words, L/K is an unramified extension.

Let M be another unramified extension of K. By the first part of Theorem 3.17, a prime of K ramifies in M if and only if it divides the conductor $\mathfrak{f}(M/K)$ of the extension, and M is unramified, so $\mathfrak{f}(M/K) = 1$. Furthermore, $\mathfrak{m} =< 1 >$ is a modulus divisible by all primes of K that ramify in L, so by the second part of Theorem 3.17, we deduce that $\mathrm{Ker}(\Phi_{M/K,\mathfrak{m}})$ is a congruence subgroup for $\mathfrak{m}$. Then, $P_K \subset \mathrm{Ker}(\Phi_{M/K,\mathfrak{m}})$. Now, $P_K = \mathrm{Ker}(\Phi_{L/K,\mathfrak{m}})$, so by Corollary 3.22, we obtain that $M \subset L$. This completes the proof of 3.5.

Let us prove 3.7. This is a trivial checking: By the Existence Theorem, $\left(\frac{L/K}{\cdot}\right)$ is a group epimorphism with $\mathrm{Ker}(\left(\frac{L/K}{\cdot}\right)) = P_K$. By the remark after the Existence Theorem, since $\mathcal{C}(\mathcal{O}_K) = I_K/P_K$, the map $\Phi : \mathcal{C}(\mathcal{O}_K) \longrightarrow \mathrm{Gal}(L/K)$ is an isomorphism □

After this, it is clear that Theorem 3.14 is a generalization of Theorem 3.7.

Actually, there is a class of abelian extensions of a number field that generalize the Hilbert Class Field. Let K be a number field and let $\mathfrak{m}$ be a modulus of K. It is automatic that $P_{K,1}(\mathfrak{m})$ is a congruence subgroup for $\mathfrak{m}$. By the Existence Theorem applied to $P_{K,1}(\mathfrak{m})$ and $\mathfrak{m}$, there is an unique abelian extension $K_\mathfrak{m}$ of K such that $\mathfrak{m}$ is divisible by all primes of K that ramify in L and

$$P_{K,1}(\mathfrak{m}) = \mathrm{Ker}(\Phi_{K_\mathfrak{m}/K,\mathfrak{m}}).$$

Definition 3.24. *Given a number field K and a modulus $\mathfrak{m}$ of K, the field $K_\mathfrak{m}$ is called the Ray Class Field of K for $\mathfrak{m}$.*

Note that the Ray Class Field of K for $\mathfrak{m} =< 1 >$ is just the Hilbert Class Field of K.

The Ray Class Field is essentially the maximal abelian extension K with a given conductor. We could erase the word *essentially* if the conductor of $K_\mathfrak{m}$ were $\mathfrak{m}$, but this is not true in general. What is true is that the conductor of $K_\mathfrak{m}$ divides $\mathfrak{m}$ (this follows from the definitions of Ray Class Field and conductor). More generally:

Proposition 3.25. *Let K be a number field and let $\mathfrak{m}$ be a modulus of K. Then, any abelian extension L of K such that $\mathfrak{f}(L/K)$ divides $\mathfrak{m}$ is contained in $K_\mathfrak{m}$.*

Proof. The idea of the proof is to apply Proposition 3.22 in order to prove that $L \subset K_\mathfrak{m}$. Thus, we may check that $\mathfrak{m}$ is divisible by all primes of K that ramify in either L or $K_\mathfrak{m}$. It is clear for $K_\mathfrak{m}$ because of the definition of Ray Class Field. Let us prove it for K. By definition of conductor, $\mathfrak{f}(L/K)$ is divisible by all primes of K that ramify in L, and by the hypothesis, $\mathfrak{f}(L/K)$ divides $\mathfrak{m}$. Hence, $\mathfrak{m}$ is divisible by all primes of K that ramify in L, as claimed. Then, Proposition 3.22 gives us the desired inclussion. □

3 The Chebotarev Density Theorem

Let K be a number field. In this section we are going to introduce the notion of density of a subset of finite primes of K, which is a function that assings non negative numbers to certain subsets of primes of K. For such a subset S, one can think in the natural density

$$\delta(S) = \lim_{N\to\infty} \frac{\#\{P \,|\, N(P) \leq N,\, P \in S\}}{\#\{P \,|\, N(P) \leq N,\, P \text{ prime}\}}.$$

This function indeed satisfies what we want. However, the limit may not exist, and in that case the density of S is not defined. We will introduce the Dirichlet density for subsets of finite primes of K. Again this density may not exist, but it is stronger than the natural density in the sense that if the natural density of a set S exists, then also does the Dirichlet density of S and there are subsets S for which the Dirichlet density of S exists and the natural density of S does not.

After this, we will state the Chebotarev Density Theorem, which is the main result of this section. Given some extension L of a number field K, the Chebotarev Density Theorem gives us the Dirichlet density of the set of primes P of K that ramify in L for which the Artin symbol of L/K over P is the conjugacy class of a given element of

$\mathrm{Gal}(L/K)$. This theorem we will useful because a set with positive Dirichlet density is infinite.

We will use the Chebotarev Density Theorem to prove a result a Class-Field-Theory version of a theorem of Dirichlet: there are infinitely many primes in an arithmetic progession in which the initial term and the difference are coprime. We will define degree 1 primes and prove that a number field has infinitely many of them. What the theorem we want to prove says is that there are infinitely many degree 1 primes in each class of a generalized ideal class group $I_K(\mathfrak{m})/P_{K,1}(\mathfrak{m})$.

Finally, we will see another application of Chebotarev Density Theorem that characterizes the Galois extensions of a number field K in terms of the primes of K that split completely in the extension.

Definition 3.26. *Let K be a number field and let us denote*

$$\mathcal{P}_K = \{P \subset K \,|\, P \text{ is a finite prime of } K\}.$$

The Dirichlet density of a subset $S \subset \mathcal{P}_K$ is the number

$$\delta(S) = \lim_{s \to 1^+} \frac{\sum_{P \in S} N(P)^{-s}}{-\log(s-1)},$$

whenever this limit exists.

We begin by studying several basic properties of the Dirichlet density that are listed in [6] (Page 169).

Proposition 3.27. *1. $\delta(\mathcal{P}_K) = 1$.*

2. If $S \cap T = \emptyset$ and $\delta(S), \delta(T)$ exist, then $\delta(S \cup T) = \delta(S) + \delta(T)$.

3. If $S \subset \mathcal{P}_K$ is finite, then $\delta(S) = 0$.

4. Given $S\mathcal{P}_K$, $\delta(S) = \delta(S \cap \mathcal{P}_{K,1})$

The second statement of last proposition says also that if $\delta(S) > 0$, then S is infinite. This suggests the following strategy: If we want to prove that there exists a finite prime of K satisfying certain properties, we could show that the set of finite primes of that type has positive Dirichlet density, and then there are infinitely many. We will use this strategy in order to prove the Dirichlet Theorem for degree 1 primes, that we proceed to define.

Let us define

$$\mathcal{P}_{K,1} = \{P \in \mathcal{P}_K \,|\, N(P) \text{ is prime}\}.$$

The elements of $\mathcal{P}_{K,1}$ are called degree 1 primes in K. The reason is that if $P \in \mathcal{P}_{K,1}$ and $p \in \mathbb{Z}$ is the prime number of $\mathbb{Q}$ under P, then p has inertia degree 1 in K.

We can proof easily that there are infinitely many degree 1 primes in K. Indeed, since $\delta(\mathcal{P}_K) = 1$, using Property 4 of Proposition 3.27,

$$0 < \delta(\mathcal{P}_K) = \delta(\mathcal{P}_K \cap \mathcal{P}_{K,1}) = \delta(\mathcal{P}_{K,1}),$$

which proves that $\mathcal{P}_{K,1}$ is infinite.

We have a stronger result, the Dirichlet Theorem for degree 1 primes: There are infinitely many degree 1 primes in every ideal class of $I_K(\mathfrak{m})/P_{K,1}(\mathfrak{m})$, where $\mathfrak{m}$ is a modulus in K. For proving this, we need the Chebotarev density Theorem.

Let L/K be a Galois extension. Given a finite prime P in K which is unramified in L and a prime Q in L over P, recall that $\left(\frac{L/K}{P}\right)$ is the conjugacy class of $\left(\frac{L/K}{Q}\right)$.

Theorem 3.28 (Chebotarev density Theorem)**.** *Let L/K be a Galois extension and let $\sigma \in \mathrm{Gal}(L/K)$. Let us denote by $[\sigma]$ the conjugacy class of σ. Set*

$$S = \{P \in \mathcal{P}_K \mid P \text{ is unramified in } L,\ \left(\frac{L/K}{P}\right) = [\sigma]\}.$$

Then, the Dirichlet density of S is

$$\delta(S) = \frac{|[\sigma]|}{[L:K]}.$$

This gives us the following:

Corollary 3.29. *Let L be an abelian extension of K and let $\mathfrak{m}$ be a modulus divisible by all the primes of K that ramify in L. Given $\sigma \in \mathrm{Gal}(L/K)$,*

$$\delta(\{P \in \mathcal{P}_K \mid P \text{ does not divide } \mathfrak{m},\ \left(\frac{L/K}{P}\right) = \sigma\}) = \frac{1}{[L:K]}.$$

Proof. It is enough to note that a prime which does not divide $\mathfrak{m}$ is unramified in L since $\mathfrak{m}$ is divisible by all primes that ramify in L, and apply the previous theorem. □

We are ready to prove the result we wanted.

Theorem 3.30. *[Dirichlet Theorem for degree 1 primes] Let K be a number field and let $\mathfrak{m}$ be an integral ideal of $\mathcal{O}_K$. Given $\overline{\mathfrak{a}} \in I_K(\mathfrak{m})/P_{K,1}(\mathfrak{m})$,*

$$\#\{P \in \mathcal{P}_K \mid \overline{P} = \overline{\mathfrak{a}},\ P \in \mathcal{P}_{K,1}\} = \infty.$$

Proof. The Existence Theorem with the congruence subgroup $P_{K,1}(\mathfrak{m})$ for $\mathfrak{m}$ gives us that there is an unique abelian extension L of K such that $\mathrm{Ker}(\Phi_{L/K,\mathfrak{m}})$ is a congruence subgroup for $\mathfrak{m}$.

By the previous corollary with $\sigma = \left(\frac{L/K}{\mathfrak{a}}\right)$, the set

$$S = \{P \in \mathcal{P}_K \mid P \text{ does not divide } \mathfrak{m},\ \left(\frac{L/K}{P}\right) = \sigma\}$$

has Dirichlet density $\delta(S) > 0$.

Let $P \in S$. Then, $\left(\frac{L/K}{P}\right) = \left(\frac{L/K}{\mathfrak{a}}\right)$. Since $\mathcal{C}(\mathcal{O}_K) \cong \mathrm{Gal}(L/K)$ and the isomorphism is induced by the Artin map, this equality implies that $\overline{P} = \overline{\mathfrak{a}}$. Hence, it is enough to find infinite degree 1 primes in S.

Let $T = S - \mathcal{P}_{K,1}$. We have that

$$\delta(T) = \lim_{s\to 1^+} \frac{\sum_{P\in T} N(P)^{-s}}{-\log(s-1)} \leq \lim_{s\to 1^+} \frac{\sum_p \frac{1}{(p^2)^s}}{-\log(s-1)} = 0$$

because the series $\sum_p \frac{1}{(p^2)^s}$ is convergent.

Since $\delta(S) > 0$ and $\delta(T) = 0$, necessarily $\delta(S-T) > 0$. But $S - T$ is just the complementary of T in S, which is the set of degree 1 primes in S. Then, such a set is infinite, which concludes the proof. □

Now, we study another application of the Chebotarev Density Theorem. Let K be a number field and let L be a Galois extension of K. Let us denote

$$S_{L/K} = \{P \in \mathcal{P}_K \mid P \text{ splits completely in } L\}.$$

The aim is to prove that L is determined by $S_{L/K}$ up to a finite number of primes. In other words, we want to prove that if M is another Galois extension of K, then the primes of $S_{L/K}$ are the primes of $S_{M/K}$ up to a finite number if and only if $L = M$.

Fix a Galois extension L/K. We can prove without difficulty that the set $S_{L/K}$ is infinite. Indeed, given a modulus $\mathfrak{m}$ of K divisible by all primes of K that ramify in L,

$$\#\{P \in \mathcal{P}_K \mid P \text{ does not divide } \mathfrak{m}, \left(\frac{L/K}{P}\right) = 1\} = \infty.$$

But by Proposition 1.8, given $P \in \mathcal{P}_K$,

$$\left(\frac{L/K}{P}\right) = 1 \iff P \text{ splits completely at } L.$$

In particular, if $\left(\frac{L/K}{P}\right) = 1$ then P does not ramify in L, so it does not divide $\mathfrak{m}$. Then,

$$\#\{P \in \mathcal{P}_K \mid P \text{ splits completely at } L\} = \infty,$$

as claimed.

In order to state the mentioned result, we introduce the following notation: For any subsets S, T, we say that $S \dot{\subset} T$ if there is some finite subset Σ such that $S \subset T \cap \Sigma$. We say that $S \doteq T$ if $S \dot{\subset} T$ and $T \dot{\subset} S$.

Theorem 3.31. *Let L, M be Galois extensions of K. Then:*

1. *$L \subset M$ if and only if $S_{M/K} \dot{\subset} S_{L/K}$.*
2. *$L = M$ if and only if $S_{M/K} \doteq S_{L/K}$.*

We need the Chebotarev Density Theorem in order to prove this result. The proof of 1 is in [6] (Theorem 8.19), and the proof of 2 follows immediately from 1. This result is very strong: the second part says that if two Galois extensions of K have the same splitting primes up to a finite number, then they coincide. This will be so useful in part 2, where we want to prove an explicit form of class fields of imaginary quadratic fields.

4 Ring class fields

In this section we are going to apply the theory of orders in order to construct a special type of abelian extensions of a imaginary quadratic field, which are the ring class fields.

Let K be an imaginary quadratic field and let $\mathcal{O}$ be the order of K of conductor f. We know by Proposition 2.31 that $\mathcal{C}(\mathcal{O}) \cong I_K(f)/P_{K,\mathbb{Z}}(f)$. Let $\mathfrak{m} = f\,\mathcal{O}_K$. It is a modulus of K because it has a factorization as a product of prime ideals of $\mathcal{O}_K$, and $\mathfrak{m}_0 = \mathfrak{m}$, $\mathfrak{m}_\infty = 1$.

We claim that

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

Let I be a generator of $P_{K,1}(\mathfrak{m})$. That is, $I = \alpha\,\mathcal{O}_K$ with $\alpha \in \mathcal{O}_K$, $\alpha \equiv 1\,(mod\, f\,\mathcal{O}_K)$. Since $a = 1$ is trivially prime to f, we conclude that $I \in P_{K,\mathbb{Z}}(f)$. This proves the first inclusion. The second one follows by definition, and the last equality follows from the fact that the ideals prime to f are just the ideals prime to $f\,\mathcal{O}_K$.

Hence, $P_{K,\mathbb{Z}}(f)$ is a congruence subgroup for $\mathfrak{m}$, and we deduce that $\mathcal{C}(\mathcal{O})$ is a generalized ideal class group of K for $\mathfrak{m} = f\,\mathcal{O}_K$. By the Existence Theorem applied to $P_{K,\mathbb{Z}}$ and $\mathfrak{m}$, there is an unique abelian extension L of K such that $\mathrm{Ker}(\Phi_{L/K,\mathfrak{m}}) = P_{K,\mathbb{Z}}(f)$ and $\mathrm{Gal}(L/K) \cong \mathcal{C}(\mathcal{O})$. Recall that L is called the class field of $P_{K,\mathbb{Z}}(f)$

Definition 3.32. *Let K be an imaginary quadratic field and $\mathcal{O}$ the order of conductor f of K. The ring class field of $\mathcal{O}$ is the class field L of $P_{K,\mathbb{Z}}(f)$.*

The Ring Class Fields are not important in our main purpose, which is to solve the *Kronecker's Jugendtraum* when K is an imaginary quadratic field. However, they allow us to give a complete information in the explicit construction that we will do in Chapter 5.

Part II

Construction of class fields via elliptic curves

Chapter 4

Elliptic curves

In this chapter we study the main notions and properties of elliptic curves. The theory of elliptic curves is interesting by itself and appears in many problems related with arithmetic geometry, but we will need it to obtain class fields of an imaginary quadratic field K and to give an explicit construction of such class fields.

The explicit construction is obtained by adjoining to K a trascendental function j evaluated at some purely imaginary complex number. This function j is going to be defined in terms of the j-invariant of an elliptic curve with complex multiplication, and the number in which we evaluate j is given by the $\mathbb{C}$-isomorphism class of the elliptic curve.

First, we will introduce the definition and basic notions of elliptic curves defined over general fields and the j-invariant of an elliptic curve. In our explicit construction we will only deal with elliptic curves defined over $\mathbb{C}$, so in this chapter we pay special attention to that case. Such elliptic curves have a very nice relation with lattices in $\mathbb{C}$: we can parametrize the elliptic curve by a complex torus. This also allows us to characterize the homothety classes of lattices and the $\mathbb{C}$-isomorphism classes of elliptic curves in terms of the j-invariant.

We are specially interested in elliptic curves defined over $\mathbb{C}$ with complex multiplication. This has a natural definition for lattices by means of their endomorphism rings, and we will relate it to endomorphism rings of elliptic curves. This will allow us to define complex multiplication for elliptic curves. Elliptic curves with complex multiplications are related to orders in quadratic fields and their proper fractional ideals. Concretely, the endomorphism ring of such an elliptic curve is an order in an imaginary quadratic field. We will exploit this fact in Chapter 5.

The next section is about torsion points of elliptic curves. For defining such torsion points we use the group structure of the $\mathbb{C}$-rational points of an elliptic curve. We will need the torsion points in order to construct the maximal abelian extension in Chapter 6. In that section we will also introduce the Tate module and the Weil pairing.

To close the chapter, we will study elliptic curves over finite fields. Althought we will work on fields of characteristic zero, we will need elliptic curves over finite fields because sometimes we reduce the equations of elliptic curves to a residue field.

1 Elliptic curves over a field

The main purpose in this section is to introduce the basic definitions and properties of elliptic curves. We will assume in the sequel that K is a field with $\mathrm{char}(K) \neq 2, 3$. This is no problem for us, because we will usually work in charasteristic zero.

Definition 4.1. *An elliptic curve E over K is an algebraic curve given by the affine equation*

$$y^2 = 4\,x^3 - g_2\,x - g_3,$$

where $g_2, g_3 \in K$ and $g_2^3 - 27\,g_3^2 \neq 0$. This equation is called the Weierstrass equation of E.

In this definition, we used affine coordinates. The Weierstrass equation of an eliptic curve E in projective coordinates $(X : Y : Z)$ is

$$E:\ Z\,Y^2 - 4\,X^3 - g_2\,X\,Z^2 - g_3\,Z^3 = 0.$$

A point that satisfies the equation of E is said to be a K-rational point provided that it has coordinates on K. Note that the infinity point $\infty = (0 : 1 : 0)$ satisfies this equation, so it is a K-rational point of the curve. We can also define an elliptic curve in an intrinsic way: it is a non-singular algebraic curve with genus 1 with a K-rational point.

Remark 4.2. *Looking at this intrinsic definition, an elliptic curve has general equation*

$$E\ :\ Y^2\,Z + a_1\,XYZ + a_3\,YZ^2 = X^3 + a_2\,X^2Z + a_4\,XZ^2 + a_6\,Z^3,$$

where $a_i \in K$. If K has not charasteristic 2 or 3, we can apply transformations to the affine version of the previous equation in order to obtain the Weierstrass equation presented in Definition 4.1.

Definition 4.3. *Let E be an elliptic curve over a field K with equation as in the previous definition.*

1. *The set*
$$E(K) = \{(x, y) \in K \times K \,|\, y^2 = 4\,x^3 - g_2\,x - g_3\} \cup \{\infty\}$$
is called the set of K-rational points of the elliptic curve E.

2. *The discriminant of E is defined as*
$$\Delta(E) = g_2^3 - 27\,g_3^2.$$

3. *The j-invariant of E is defined as*
$$j(E) = 1728\,\frac{g_2^3}{\Delta(E)}.$$

Next, we are going to define a group structure in the set $E(K)$.

Definition 4.4. *Let E be an elliptic curve over a field K. Let $P_1, P_2 \in E(K)$.*

1. *If $P_1 = \infty$, we define $P_1 + P_2 := P_2$, and similarly for $P_2 = \infty$.*
2. *Otherwise, put $P_1 = (x_1, y_1), P_2 = (x_2, y_2)$.*

   2.1. *If $x_1 \neq x_2$, we define $P_1 + P_2 := (x_3, y_3)$, where*

$$x_3 = -x_1 - x_2 - \frac{1}{4}\left(\frac{y_1 - y_2}{x_1 - x_2}\right)^2,$$

$$y_3 = -y_1 - (x_3 - x_1)\left(\frac{y_1 - y_2}{x_1 - x_2}\right)^2.$$

   2.2. *If $x_1 = x_2$, the Weierstrass equations imply that $y_1 = \pm y_2$. If $y_1 = -y_2$, we define $P_1 + P_2 := \infty$. Otherwise, we define $P_1 + P_2 \equiv 2\,P_1 := (x_3, y_3)$, where*

$$x_3 = -2\,x_1 - \frac{1}{16}\left(\frac{12x_1^2 - g_2}{y_1}\right)^2,$$

$$y_3 = -y_1 - (x_3 - x_1)\left(\frac{12\,x_1 - g_2}{2\,y_1}\right).$$

It can be proved that this gives us a well-defined binary operation in $E(K)$ and endow it with an abelian group structure with identity ∞. This algebraic definition of the sum of points of an elliptic curve looks strange, but it has a very nice geometric interpretation.

We define now the meaning of two elliptic curves over K being K-isomorphic. This is necessary because two isomorphic elliptic curves have similar properties.

Definition 4.5. *Let E, E' be elliptic curves defined over the same field K with Weierstrass equations*

$$E \,:\, y^2 = x^3 - g_2\,x - g_3,$$
$$E' \,:\, y^2 = x^3 - g_2'\,x - g_3'.$$

We say that E and E' are isomorphic if there exists $c \in K$, $c \neq 0$ such that

$$g_2' = c^4\,g_2,$$

$$g_3' = c^6\,g_3.$$

Note that if E and E' are isomorphic elliptic curves, then the map

$$\begin{array}{ccc} E(K) & \longrightarrow & E'(K) \\ (x, y) & \longmapsto & (c^2\,x, c^3\,y) \end{array}$$

is a group isomorphism.

The following result gives us that isomorphic elliptic curves have the same j-invariant.

Proposition 4.6. *Let E and E' be isomorphic elliptic curves over K. Then, $j(E) = j(E')$.*

Proof. We consider the Weierstrass equations of E and E' as before. Then,

$$j(E') = 1728\,\frac{(g_2')^3}{(g_2')^3 - 27\,(g_3')^2} = 1728\,\frac{c^{12}\,g_2^3}{c^{12}\,g_2^3 - 27\,c^{12}\,g_3^2} = 1728\,\frac{g_2^3}{g_2^3 - 27\,g_3^2} = j(E).$$

□

If K is algebraically closed, the converse is true (see [9], Chapter III, Proposition 1.4.*b*). In particular, the j-invariant of an elliptic curve defined over $\mathbb{C}$ characterizes completely its $\mathbb{C}$-isomorphism class. This allows us to classify $\mathbb{C}$-isomorphism classes of elliptic curves by using the arithmetic of such elliptic curves. In the next chapter we will use this fact to prove that the j-invariant of a complex elliptic curve is an algebraic number.

We will need also the following result, which says that all the elements of the algebraic clossure of a field are the j-invariant of some elliptic curve.

Proposition 4.7. *Given $j_0 \in \overline{K}$, there is an elliptic curve E defined over $K(j_0)$ such that $j(E) = j_0$.*

The proof can be found in [9] (Chapter III, Proposition 1.4.*c*).

2 Lattices and elliptic curves

In this section we study elliptic curves defined over $\mathbb{C}$. We introduce lattices and study their main properties. As we mentioned at the begining of the chapter, lattices can be used to obtain elliptic curves defined over $\mathbb{C}$. We will see also a result that allows us to characterize homothety classes of lattices in terms of $\mathbb{C}$-isomorphisms classes of elliptic curves. We will omit the proofs and only give the main notions (see [8] for a detailed lecture).

Lattices

Definition 4.8. *A lattice in $\mathbb{C}$ is a $\mathbb{Z}$-submodule of $\mathbb{C}$ of the form*

$$\Lambda =< w_1, w_2 >_{\mathbb{Z}},$$

where $w_1, w_2 \in \mathbb{C}$ are $\mathbb{R}$-linearly independent as vectors in the complex plane.

Observe that a lattice can be represented in the complex plane as a grid whose lines are determined by the direction and the module of the vectors w_1, w_2.

We have two basic objects related to a lattice.

Definition 4.9. *Let Λ be a lattice in $\mathbb{C}$.*

1. *The fundamental parallelotope associated to Λ is the set*

$$\prod\nolimits_{\Lambda} = \{a\,w_1 + b\,w_2 \,|\, a, b \in \mathbb{R}, 0 \leq a, b \leq 1\}.$$

2. *The torus associated to Λ is*

$$T_\Lambda = \mathbb{C}/\Lambda.$$

Doubly periodic functions

Definition 4.10. *Let Λ be a lattice in $\mathbb{C}$. A meromorphic function $f : \mathbb{C} \longrightarrow \mathbb{C} \cup \infty$ is said to be elliptic or doubly periodic with respect to Λ if $f(z+l) = f(z)$ for all $z \in \mathbb{C}$ and $l \in \Lambda$.*

The meaning of the name doubly periodic is very natural: the function has the same values in two points when they differ by any of the generators of the lattice. Then, a doubly-periodic function factors through the complex torus of the lattice.

The set ξ_Λ of all elliptic functions with respect to Λ is a field with the pointwise sum and product. Since any complex constant function is trivially elliptic, ξ_Λ is an extension of $\mathbb{C}$.

Our meromorphic functions are holomorphic in all the domain of definition up to poles. This directly gives us the following.

Proposition 4.11. *Let $f \in \xi_\Lambda$. If f has no poles in $\prod_\Lambda$, then it is constant.*

The Weierstrass $\wp$-function

Definition 4.12. *Let Λ be a lattice in $\mathbb{C}$. The Weierstrass $\wp$-function associated to Λ is*

$$\wp(z, \Lambda) = \frac{1}{z^2} + \sum_{w \in \Lambda - \{0\}} \left(\frac{1}{(z-w)^2} - \frac{1}{w^2} \right), \; z \in \mathbb{C} - \Lambda$$

The Weierstrass $\wp$-function will allow us to establish some important notions and results about elliptic curves related especially with lattices. It is well defined because the series that appears in its definition converges absolutely and uniformly over compact subsets of $\mathbb{C} - \Lambda$. The idea for proving this is to prove first that the series

$$G_k(\Lambda) = \sum_{w \in \Lambda - \{0\}} \frac{1}{w^k}$$

converges absolutely (see [8], Page 23).

We commented that ξ_Λ is an extension of $\mathbb{C}$. In fact, it can be obtained by adjoining to $\mathbb{C}$ the Weierstrass $\wp$-function and its derivative, that is, $\xi_\Lambda = \mathbb{C}(\wp(z, \Lambda), \wp'(z, \Lambda))$. A proof of this result can be found in [8]. What we actually prove is that the field of even elliptic functions equals to $\mathbb{C}(\wp(z, \Lambda))$ (see [8], Chapter I, Proposition 9) by giving an explicit expression of each even elliptic function in terms of $\wp(z, \Lambda)$, and from here we obtain easily the desired result (see [8], Chapter I, Proposition 8).

Let us fix a lattice Λ in $\mathbb{C}$. The Weierstrass $\wp$-function $\wp'(z, \Lambda)^2$ is an even elliptic function. Using the explicit expression in terms of $\wp(z, \Lambda)$ (see [8], Page 22), we obtain that

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

where

$$g_2(\Lambda) = 60\,G_4(\Lambda),$$
$$g_3(\Lambda) = 140\,G_6(\Lambda).$$

It is also true that $g_2(\Lambda)^3 - 27\,g_3(\Lambda)^2 \neq 0$, because the polynomial $f(x) = 4\,x^3 - g_2(\Lambda)\,x - g_3(\Lambda)$ has distinct roots (see [8]). Thus, this is just the equation of an elliptic curve.

Definition 4.13. *The elliptic curve associated to a lattice Λ in $\mathbb{C}$ is the curve given by the affine equation*

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

Complex elliptic curves

We can define the discriminant and the j-invariant of a lattice Λ by using the elliptic curve over $\mathbb{C}$ that induces Λ.

Definition 4.14. *Let Λ be a lattice in $\mathbb{C}$ and let E_Λ be the elliptic curve associated to Λ.*

1. *The discriminant of Λ is defined as*

$$\Delta(\Lambda) = \Delta(E_\Lambda).$$

2. *The j-invariant of E_Λ is defined as*

$$j(\Lambda) = j(E_\Lambda).$$

The relation between complex elliptic curves and lattices is given by the following result.

Theorem 4.15. *Let Λ be a lattice in $\mathbb{C}$ and let E_Λ be the elliptic curve associated to Λ. Then, the map*

$$\begin{array}{rccc} \xi\colon & \mathbb{C}/\Lambda & \longrightarrow & E_\Lambda(\mathbb{C}) \\ & z+\Lambda & \longmapsto & (\wp(z), \wp'(z)) \\ & \Lambda & \longmapsto & \infty \end{array}$$

is an analitic isomorphism and a group isomorphism if we consider the additive structures in both sets.

With the notation of the previous theorem, we say that ξ is an analytic parametrization of E_Λ. Since this map is a group isomorphism when we consider in $E_\Lambda(\mathbb{C})$ the defined group structure, we can find easily the sum of two points $P_1 = (x_1, y_1)$, $P_2 = (x_2, y_2)$ of an elliptic curve associated to a lattice by identifying the corresponding $z_1, z_2 \in \prod$ such that $x_i = \wp(z_i)$, $i \in \{1, 2\}$ and adding them in $\mathbb{C}/\Lambda$. That is,

$$(x_1, y_1) + (x_2, y_2) = (\wp(z_1), \wp'(z_1)) + (\wp(z_2), \wp'(z_2)) = (\wp(z_1 + z_2), \wp'(z_1 + z_2)).$$

Homothety of lattices

Definition 4.16. *We say that two lattices Λ, Λ' in $\mathbb{C}$ are homothetic, denoted by $\Lambda \sim \Lambda'$ if there exists $\alpha \in \mathbb{C} - \{0\}$ such that $\Lambda' = \alpha\, \Lambda$.*

The j-invariant of a lattice characterizes the homothety class of the lattice. This is closely connected with the analogous property for elliptic curves.

Proposition 4.17. *Let Λ, Λ' be lattices in $\mathbb{C}$. The following are equivalent:*

1. *E_Λ and $E_{\Lambda'}$ are isomorphic over $\mathbb{C}$.*

2. Λ *and* Λ' *are homothetic.*

3. $j(\Lambda) = j(\Lambda')$.

By definition, elliptic curves associated to lattices are defined over $\mathbb{C}$, but in fact there are no other elliptic curves over $\mathbb{C}$.

Theorem 4.18 (Uniformization Theorem)**.** *Let* $g_2, g_3 \in \mathbb{C}$ *such that* $g_2^3 - 27\, g_3^2 \neq 0$. *Then, there is an unique lattice* Λ *in* $\mathbb{C}$ *up to homothety such that* $g_2 = g_2(\Lambda)$ *and* $g_3 = g_3(\Lambda)$.

A proof of this result is in [9] (Chapter VI, Theorem 5.1).
An immediate consequence of the Uniformization Theorem is the following.

Corollary 4.19. *Let* E *be an elliptic curve defined over* $\mathbb{C}$. *Then, there is an unique lattice* Λ *in* $\mathbb{C}$ *up to homothety and an analitic isomorphism* $\xi : T_\Lambda \longrightarrow \mathbb{C}$ *such that* $\xi(z) = (\wp(z), \wp'(z))$. *Thus,* $E \cong E_\Lambda$.

3 Maps between elliptic curves

When we introduce an object with some structure, it is natural to ask for the morphisms between this kind of objects. In that section we are going to define the morphisms in the category of elliptic curves, and we will focus on a special kind of these morphisms, the isogenies.

3.1 Morphisms of elliptic curves

Let E be an elliptic curve defined over K. Then, the set

$$I(E) = \{f \in K[x, y] \,|\, f(P) = 0 \text{ for all } P \in E\}$$

is a prime ideal of $K[x, y]$ (see [9], Chapter I, Section 1). The field of the restrictions of rational functions to the curve E is the field

$$K(E) := \mathrm{Frac}(K[x, y]/I(E)).$$

Let us consider the field $\overline{K}(E)$, where $\overline{K}$ denotes the algebraic closure of K. An element $f \in \overline{K}(E)$ is a class

$$[f(x, y)] = \{f(x, y) + g(x, y) \,|\, g \in K[x, y], g(P) = 0 \text{ for all } P \in E\},$$

so it can be seen as a function $f : E \longrightarrow \overline{K}$.

We will first define rational maps between elliptic curves and from this we will introduce morphisms between elliptic curves. This can be done in general for algebraic varieties (see [9], Chapter I, Section 3). Let E_1, E_2 be elliptic curves defined over the same field K. Let us consider E_1 and E_2 as projective curves. A rational map from E_1 to E_2 is a map of the form

$$\phi = [f_0, f_1, f_2] : E_1 \longrightarrow E_2,$$

where $f_i \in \overline{K}(E_1)$ and for each $P \in E_1$, f_0, f_1, f_2 are defined at P and

$$\phi(P) = [f_0(P), f_1(P), f_2(P)] \in E_2.$$

If $\phi : E_1 \longrightarrow E_2$ is a rational map and $\sigma \in \mathrm{Gal}(\overline{K}/K)$, then

$$\phi^\sigma = [f_0^\sigma, f_1^\sigma, f_2^\sigma] : E_1 \longrightarrow E_2$$

is also a rational map. By using the definition of homomorphism, it holds that

$$(\phi(P))^\sigma = \phi^\sigma(P^\sigma) \text{ for all } P \in E_1.$$

We say that a rational map $\phi : E_1 \longrightarrow E_2$ is defined over K if there exists a non-zero number $\lambda \in \overline{K}$ such that $\lambda f_0, \lambda f_1, \lambda f_2 \in K(E_1)$. This is equivalent to the condition $\phi^\sigma = \phi$ for all $\sigma \in \mathrm{Gal}(\overline{K}/K)$.

Definition 4.20. *Let $\phi : E_1 \longrightarrow E_2$ be a rational map. We say that ϕ is defined at a point $P \in E_1$ if there exists $g \in \overline{K}(E_1)$ such that $g f_i$ is defined at P for every $i \in \{0, 1, 2\}$ and there is some f_{i_0} for which $g f_{i_0}(P) \neq 0$.*

Now, we can establish the definition of morphism of elliptic curves.

Definition 4.21. *A morphism of elliptic curves is a rational map $\phi : E_1 \longrightarrow E_2$ which is defined at every point of E_1.*

When we take affine coordinates, a morphism of elliptic curves $\phi : E_1 \longrightarrow E_2$ is of the form

$$\phi(x, y) = (R(x, y), S(x, y))$$

where $R(x, y), S(x, y) \in K(E_1)$. Moreover, given $\sigma \in \mathrm{Gal}(\overline{K}/K)$, we have that

$$\phi^\sigma(x, y) = (R^\sigma(x, y), S^\sigma(x, y)).$$

Theorem 4.22. *Let $\phi : E_1 \longrightarrow E_2$ be a morphism of elliptic curves. Then, ϕ is constant or surjective.*

This result is in [9] (Chapter II, Theorem 2.3).

Let $\phi : E_1 \longrightarrow E_2$ be a morphism of elliptic curves over K. Then ϕ induces a monomorphism of fields

$$\begin{array}{rccc} \phi^*: & \overline{K}(E_2) & \longrightarrow & \overline{K}(E_1) \\ & f & \longmapsto & f \circ \phi \end{array}.$$

Definition 4.23. *Let $\phi : E_1 \longrightarrow E_2$ be a morphism of elliptic curves over K.*

1. *We say that ϕ is finite (resp. separable) if so is the field extension $\overline{K}(E_1)/\overline{K}(E_2)$.*
2. *The degree of ϕ is*
$$\deg(\phi) := [\overline{K}(E_1) : \overline{K}(E_2)].$$

Let us study two representatives examples of morphisms of elliptic curves: the first one is the called multiplication-by-m morphism, where the elliptic curves are defined over a field of charasteristic 0, and the other one is the Frobenius morphism, where the elliptic curves are defined over a finite field.

Multiplication-by-m morphism

Let $K = \mathbb{C}$ and let E be an elliptic curve defined over $\mathbb{C}$ with equation

$$E \,:\, y^2 = 4\,x^3 - g_2\,x - g_3.$$

Let us define the map

$$\begin{array}{rccc} [2]\colon & E(K) & \longrightarrow & E(K) \\ & (x,y) & \longmapsto & 2\,(x,y) \\ & \infty & \longmapsto & \infty \end{array}.$$

By the duplication formula in definition 4.4, this map is a morphism of elliptic curves $[2] : E \longrightarrow E$ from E to itself.

Let $m \in \mathbb{N}$. By induction and the formula of the sum of two points in definition 4.4, we can show that the map

$$\begin{array}{rccc} [m]\colon & E(K) & \longrightarrow & E(K) \\ & (x,y) & \longmapsto & m\,(x,y) \\ & \infty & \longmapsto & \infty \end{array}$$

defines a morphism of elliptic curves $[m] : E \longrightarrow E$.

Frobenius morphism

We proceed to introduce the Frobenius map. Let us consider a finite field K of charasteristic $p > 0$. Take an elliptic curve E over K with equation

$$E \,:\, y^2 = x^3 + a\,x + b.$$

Let $q = p^r$ be any power of p. Let us define an algebraic curve $E^{(q)}$ over K given by the equation

$$E^{(q)} \,:\, x^3 + a^q\,x + b^q.$$

Since $\mathrm{char}(K) = p$, $\Delta(E^{(p)}) = \Delta(E)^p \neq 0$, so $E^{(q)}$ is an elliptic curve defined over K.

The q-th power Frobenius map of E is

$$\begin{array}{rccc} \mathrm{Frob}_q\colon & E(K) & \longrightarrow & E^{(p)}(K) \\ & (x,y) & \longmapsto & (x^q, y^q) \\ & \infty & \longmapsto & \infty \end{array}.$$

First of all, let us see that it is well defined. Given $(x,y) \in E(\mathbb{F}_q)$, since $char(\mathbb{F}_q) = p$, we have that:

$$(y^q)^2 - ((x^q)^3 + a^q\,x^q + b^q) = (y^2 - (x^3 + a\,x + b))^q = 0.$$

Thus, $(x^q, y^q) \in E^{(q)}(K)$. Moreover, $R(x,y) = x^p$ and $S(x,y) = y^p$ are rational functions over K.

Hence, the previous map defines a morphism $\mathrm{Frob}_q : E \longrightarrow E^{(q)}$ of elliptic curves.

3.2 Isogenies

Definition 4.24. *Let E_1, E_2 be elliptic curves over K. An isogeny from E_1 to E_2 is a morphism of elliptic curves $\phi : E_1 \longrightarrow E_2$ such that $\phi(\infty) = \infty$. If $\phi(E_1) \neq \{\infty\}$, we say that E_1 and E_2 are isogenous.*

It is automatic that the multiplication-by-m and Frobenius morphisms are isogenies.

We restrict our morphisms of elliptic curves to isogenies because they behave well with the group structure of the sets of K-rational points of the elliptic curves.

Theorem 4.25. *If $\phi : E_1 \longrightarrow E_2$ is an isogeny, then*

$$\phi(P + Q) = \phi(P) + \phi(Q) \text{ for all } P, Q \in E_1.$$

In other words, the corresponding map $\phi : E_1(K) \longrightarrow E_2(K)$ is a group homomorphism.

We have also an easier expression of the degree of a separable isogeny.

Theorem 4.26. *Let $\phi : E_1 \longrightarrow E_2$ be a non-constant isogeny. If ϕ is separable, then* $\deg(\phi) = |\operatorname{Ker}(\phi)|$.

A morphism of elliptic curves defined over a finite field factors through a reduction of the elliptic curve that depends on its degree.

Proposition 4.27. *Let $\Phi : E_1 \longrightarrow E_2$ be a morphism of elliptic curves over a finite field of charasteristic $p > 0$. Then, there is a power q of p for which there is a unique separable morphism of elliptic curves $\lambda : E_1^{(q)} \longrightarrow E_2$ such that $\Phi = \lambda \circ \operatorname{Frob}_q$.*

The proof can be found in [9] (Chapter II, Corollary 2.12). We can use this result to determine the order of the kernel of an isogeny when the isogeny is not separable.

Definition 4.28. *Let $\phi : E_1 \longrightarrow E_2$ be an isogeny between elliptic curves over a finite field. Let $\lambda : E_1^{(q)} \longrightarrow E_2$ be the separable morphism of elliptic curves and q the power of p such that $\phi = \lambda \circ \operatorname{Frob}_q$.*

1. *The separable degree of ϕ is defined as* $\deg_s(\phi) = \deg(\lambda)$.

2. *The inseparable degree of ϕ is* $\deg_i(\phi) = q$.

After this, one can prove that for every isogeny $\phi : E_1 \longrightarrow E_2$ in charasteristic 0, $\deg(\phi) = \deg_s(\phi)\ \deg_i(\phi)$ (see [7], Page 32).

Theorem 4.29. *Let K be a field of charasteristic $p > 0$ and let q be any power of p. Then,* Frob_q *is purely inseparable of degree q.*

The proof of this result can be found in [9] (Chapter II, Proposition 2.11).

Dual isogenies

To close this section, we introduce the notion of dual isogeny. The proofs of the corresponding results can be found in [9] (Chapter III, Section 6).

Theorem 4.30. *Let $\phi : E_1 \longrightarrow E_2$ be a non-constant isogeny of degree m. Then, there exists an unique isogeny $\hat{\phi} : E_2 \longrightarrow E_1$ such that*

$$\hat{\phi} \circ \phi = [m].$$

Definition 4.31. *If $\phi : E_1 \longrightarrow E_2$ is a non-constant isogeny of degree m, the dual isogeny of ϕ is defined as the isogeny $\hat{\phi} : E_2 \longrightarrow E_1$ of the previous result.*

Proposition 4.32 (Properties of the dual isogeny)**.** *Let $\phi : E_1 \longrightarrow E_2$ be a non-constant isogeny of degree m. Then:*

1. *$\hat{\phi} \circ \phi = [m]$ on E_1 and $\phi \circ \hat{\phi} = [m]$ on E_2.*
2. *$\deg(\phi) = \deg(\hat{\phi})$.*
3. *$\hat{\hat{\phi}} = \phi$.*

4 Elliptic curves with complex multiplication

Complex multiplication of elliptic curves is a fundamental ingredient in the explicit construction of abelian extensions of imaginary quadratic fields. In this section we are going to study the definition of complex multiplication for elliptic curves over $\mathbb{C}$, which involves the concept of endomorphism ring of an elliptic curve. We will also see a connection with the theory of orders in quadratic fields in which we see proper fractional ideals as lattices. This new point of view allows us to define the j-function that appears in our explicit construction.

We know that $\mathbb{C}$-isomorphisms classes of elliptic curves correspond to homothetic classes of lattices, so we begin with complex multiplication of lattices.

Definition 4.33. *Let $\Lambda \subset \mathbb{C}$ be a lattice. The endomorphism ring of Λ is the set*

$$\mathrm{End}(\Lambda) = \{\alpha \in \mathbb{C} \,|\, \alpha\,\Lambda \subset \Lambda\}.$$

By definition of lattice, $\mathbb{Z} \subset \mathrm{End}(\Lambda)$.

Definition 4.34. *We say that a lattice $\Lambda \subset \mathbb{C}$ has complex multiplication if $\mathbb{Z} \subsetneq \mathrm{End}(\Lambda)$.*

We are going to translate this concepts to elliptic curves defined over $\mathbb{C}$ by means of analytic parametrizations introduced in this chapter.

Definition 4.35. *Let E be an elliptic curve defined over a field K. The endomorphism ring of E is*

$$\mathrm{End}_K(E) = \{\phi : E \longrightarrow E \,|\, \phi \text{ is an isogeny}\}.$$

It has ring structure with the sum and the composition of isogenies (which means composition of the corresponding maps from $E(K)$ to itself). This definition is general, but in this section we particularize to elliptic curves defined over $\mathbb{C}$. For such an elliptic curve, there is a lattice Λ such that $E = E_\Lambda$, so one can think that the rings of endomorphisms of E and Λ may be related. What we are going to prove is that they are isomorphic.

Theorem 4.36. *Let E_1, E_2 be elliptic curves defined over $\mathbb{C}$ and let Λ_1, Λ_2 be lattices such that $E_i = E_{\Lambda_i}$, $i \in \{1,2\}$. Let $\xi_i : \mathbb{C}/\Lambda_i \longrightarrow E_i$, $i \in \{1,2\}$, be analytic parametrizations.*

1. *There is a bijection*

$$\begin{array}{ccc} \{\alpha \in \mathbb{C} \,|\, \alpha\,\Lambda_1 \subset \Lambda_2\} & \longrightarrow & \{\phi : \mathbb{C}/\Lambda_1 \longrightarrow \mathbb{C}/\Lambda_2 \textit{ holomorphic}, \phi(0) = 0\} \\ \alpha & \longmapsto & \phi_\alpha(z + \Lambda_1) = \alpha\, z + \Lambda_2 \end{array}.$$

2. *The following map is bijective:*

$$\begin{array}{ccc} \mathrm{Hom}(E_1, E_2) & \longrightarrow & \{\phi : \mathbb{C}/\Lambda_1 \longrightarrow \mathbb{C}/\Lambda_2 \textit{ holomorphic}, \phi(0) = 0\} \\ \lambda & \longmapsto & \xi_2^{-1} \circ \lambda \circ \xi_1 \end{array}.$$

Proof.

1. Let $\alpha, \beta \in \mathbb{C}$ with $\alpha\,\Lambda_1 \subset \Lambda_2$ and $\beta\,\Lambda_1 \subset \Lambda_2$ such that $\phi_\alpha = \phi_\beta$. Then, $\alpha\, z \equiv \beta\, z \,(\mathrm{mod}\, \Lambda_2)$ for all $z \in \mathbb{C}$. This implies that $(\alpha - \beta)\, z \in \Lambda_2$ for all $z \in \mathbb{C}$. Then, the function $z \mapsto (\alpha - \beta)\, z$ is continuous in $\mathbb{C}$ and has image contained in Λ_2, which is discrete. We deduce that $(\alpha - \beta)\, z = 0$ for all $z \in \mathbb{C}$, so $\alpha = \beta$. Then, the map is injective.

Let $\phi : \mathbb{C}/\Lambda_1 \longrightarrow \mathbb{C}/\Lambda_2$ be holomorphic such that $\phi(0) = 0$. Since $\mathbb{C}$ is simply connected, we can lift ϕ to an holomorphic map $f : \mathbb{C} \longrightarrow \mathbb{C}$ such that the following diagram commutes.

$$\begin{array}{ccc} \mathbb{C} & \xrightarrow{f} & \mathbb{C} \\ \downarrow & & \downarrow \\ \mathbb{C}/\Lambda_1 & \xrightarrow{\phi} & \mathbb{C}/\Lambda_2 \end{array}$$

The vertical maps are the corresponding projections. This means that

$$\phi(z + \Lambda_1) = f(z) + \Lambda_2,\ z \in \mathbb{C}.$$

Let $z \in \mathbb{C}$, $w \in \Lambda_1$. Then

$$f(z + w) + \Lambda_2 = \phi(z + w + \Lambda_1) = \phi(z + \Lambda_1) = f(z) + \Lambda_2\, z \in \mathbb{C}.$$

We deduce that $f(z + w) - f(z) \in \Lambda_2$ for all $z \in \mathbb{C}$ and $w \in \Lambda_1$. Hence, for fixed $w \in \Lambda_1$, the continuous function $z \mapsto f(z + w) - f(z)$ has image contained in Λ_2. Since Λ_2 is discrete, we conclude that $f(z + w) = f(z)$ for all $z \in \mathbb{C}$. Taking derivatives, $f'(z + w) = f'(z)$ for all $z \in \mathbb{C}$. Then, $f' \in \xi_{\Lambda_1}$. But f' is entire, so it is constant.

Since f' is constant, there are $\alpha, \gamma \in \mathbb{C}$ such that $f(z) = \alpha\, z + \gamma$. But $0 = f(0) = \gamma$, so $f(z) = \alpha\, z$. This gives us that

$$\phi(z + \Lambda_1) = \alpha\, z + \Lambda_2$$

for all $z \in \mathbb{C}$. Since $f(\Lambda_1) \subset \Lambda_2$, we conclude that $\alpha\,\Lambda_1 \subset \Lambda_2$. This proves the surjectivity.

2. Let us see that the map is well defined. Let $\lambda \in \mathrm{Hom}(E_1, E_2)$. Then, the coordinates of $\lambda(x, y)$ are given by rational functions on x and y. Since ξ_1 and ξ_2 are analytic and both the Weierstrass $\wp$-function and its derivative are holomorphic, $\xi_2^{-1} \circ \lambda \circ \xi_1$ is holomorphic. Moreover, $\xi_2^{-1} \circ \lambda \circ \xi_1(0) = 0$.

The map is clearly injective. Let us check the surjectivity. Let $\phi : \mathbb{C}/\Lambda_1 \longrightarrow \mathbb{C}/\Lambda_2$ such that $\phi(0) = 0$. By part a, there exists $\alpha \in \mathbb{C}$ with $\alpha\,\Lambda_1 \subset \Lambda_2$ such that $\phi = \phi_\alpha$.

Let $\lambda = \xi_2 \circ \phi_\alpha \circ \xi_1^{-1} : E_1 \longrightarrow E_2$. Let $(x, y) \in E_1$. Then, there is an unique class $z + \Lambda_1 \in \mathbb{C}/\Lambda_1$ such that $(x, y) = \xi_1(z + \Lambda_1) = (\wp(z, \Lambda_1), \wp'(z, \Lambda_1))$. We have that

$$\lambda(x, y) = \lambda(\wp(z, \Lambda_1), \wp'(z, \Lambda_1)) = \xi_2 \circ \phi_\alpha(z) = \xi_2(\alpha\, z) = (\wp(\alpha\, z, \Lambda_1), \wp'(\alpha\, z, \Lambda_1)).$$

Let $w \in \Lambda_1$. Since $\alpha\,\Lambda_1 \subset \Lambda_2$, we have that $\alpha\, w \in \Lambda_2$. Using that $\wp$ and $\wp'$ are doubly periodic,

$$\wp(z + w, \Lambda_2) = \wp(\alpha\, z + \alpha\, w, \Lambda_2) = \wp(\alpha\, z, \Lambda_2),$$
$$\wp'(\alpha\,(z + w), \Lambda_2) = \wp'(\alpha\, z + \alpha\, w, \Lambda_2) = \wp'(\alpha\, z, \Lambda_2).$$

Then, $\wp(\alpha\, z, \Lambda_2)$, $\wp'(\alpha\, z, \Lambda_2) \in \xi_{\Lambda_1} = \mathbb{C}(\wp(z, \Lambda_1), \wp'(z, \Lambda_1)) = \mathbb{C}(x, y)$. Hence the coordinates of $\lambda(x, y)$ are rational functions on x and y. This means that $\lambda \in \mathrm{Hom}(E_1, E_2)$. □

Corollary 4.37. *With the conditions of the previous theorem, there is a bijection*

$$\begin{array}{ccc} \{\alpha \in \mathbb{C} \,|\, \alpha\,\Lambda_1 \subset \Lambda_2\} & \longrightarrow & \mathrm{Hom}(E_1, E_2) \\ \alpha & \longmapsto & \xi_2 \circ \phi_\alpha \circ \xi_1^{-1} \end{array}.$$

Corollary 4.38. *Let E be an elliptic curve defined over $\mathbb{C}$ and let Λ be a lattice such that $E = E_\Lambda$. Then, there is a bijection*

$$\begin{array}{ccc} \mathrm{End}(\Lambda) & \longrightarrow & \mathrm{End}(E) \\ \alpha & \longmapsto & \xi \circ \phi_\alpha \circ \xi^{-1} \end{array}.$$

This gives rise naturally to the following definition.

Definition 4.39. *Let E be an elliptic curve defined over $\mathbb{C}$ and let Λ be a lattice such that $E = E_\Lambda$. We say that E has complex multiplication if so has Λ.*

The meaning of complex multiplication looks strange for elliptic curves, but it is natural for lattices: a lattice has complex multiplication if it has some dilation by a complex non-integer number which is inside the lattice itself.

Remark 4.40. *At this point, we can identify explicitely the elements of* $\mathrm{End}(E_\Lambda)$ *that correspond to integer numbers in* $\mathrm{End}(\Lambda)$. *Let $m \in \mathbb{Z}$. Then, the corresponding endomorphism is given by*

$$\xi \circ \phi_m \circ \xi^{-1}(\wp(z, \Lambda), \wp'(z, \Lambda)) = \xi \circ \phi_m(z + \Lambda) = \xi(mz + \Lambda) = (\wp(mz + \Lambda), \wp'(mz + \Lambda)) = [m](\wp(z, \Lambda), \wp'(z, \Lambda)).$$

Hence, $\xi \circ \phi \circ \xi^{-1} = [m]$. Then, E has complex multiplication if it has some endomorphism different from multiplication-by-m morphisms.

As we mentioned before, elliptic curves with complex multiplication have a surprising connection with orders in imaginary quadratic fields. These orders appear in the classification of the ring of endomorphisms of elliptic curves with complex multiplication, given by the following result.

Theorem 4.41. *Let Λ be a lattice in $\mathbb{C}$. Then, End(Λ) is $\mathbb{Z}$ or an order $\mathcal{O}$ in an imaginary quadratic field. In the last case, Λ is homothetic to a proper ideal of $\mathcal{O}$.*

Proof. If $\mathrm{End}(\Lambda) = \mathbb{Z}$, there is nothing to prove. Let us assume that $\mathbb{Z} \subsetneqq \mathrm{End}(\Lambda)$ (that is, Λ has complex multiplication). By the definition of endomorphism ring, $\mathrm{End}(\Lambda)$ is invariant by homothety, so we can assume that $\Lambda =< 1, \tau >$, $\tau \in \mathbb{C} - \mathbb{R}$.

Given $\alpha \in \mathrm{End}(\Lambda)$, $\alpha\Lambda =< \alpha, \alpha\,\tau >\subset \Lambda$. This says that $\alpha \in \Lambda$. Hence $\mathrm{End}(\Lambda) \subset \Lambda$.

Let $\alpha \in \mathrm{End}(\Lambda) - \mathbb{Z}$. Then $\alpha \in \Lambda$, so there exist $a, b \in \mathbb{Z}$ with $b \neq 0$ such that $\alpha = a + b\,\tau$. On the other hand, by the definition of α, we have that $\alpha\,\tau \in \Lambda$, so there exist $c, d \in \mathbb{Z}$ such that $\alpha\,\tau = c + d\,\tau$. Multiplying the previous equality by τ, we obtain:

$$c + d\,\tau = a\,\tau + b\,\tau^2 \Longrightarrow b\,\tau^2 + (a - d)\,\tau - c = 0.$$

Let $f(X) = \beta\,X^2 + (a - d)\,X - c \in \mathbb{Q}[x]$. Since $b \neq 0$, we have that $deg(f) = 2$. Moreover, the previous equality says that τ is a root of f. Since $\tau \notin \mathbb{Q}$, f is irreducible over $\mathbb{Q}$. Hence f is the minimal polynomial of τ, which implies that $[\mathbb{Q}(\tau) : \mathbb{Q}] = 2$. We have also that $\tau \in \mathbb{C} - \mathbb{R}$, so $K = \mathbb{Q}(\tau)$ is an imaginary quadratic field. Note that the equality $\alpha = a + b\,\tau$ implies that $K = \mathbb{Q}(\alpha)$.

Now, we have $\mathrm{End}(\Lambda) \subset \Lambda \subset K$, and both $\mathrm{End}(\Lambda)$ and K are subrings of $\mathbb{C}$. Then, $\mathrm{End}(\Lambda)$ is an unitary subring of K. Furthermore, the previous chain of inclusions also implies that $\mathrm{End}(\Lambda)$ is a subgroup of Λ, so it is finitely generated as $\mathbb{Z}$-module. Finally, it follows from the definition that $\{1, \tau\}$ is a $\mathbb{Q}$-basis of K, and it is contained in $\mathrm{End}(\Lambda)$. We conclude that $\mathcal{O} = \mathrm{End}(\Lambda)$ is an order of K.

It remains to prove that Λ is homothetic to a proper ideal of $\mathcal{O}$. First, we observe that $\mathrm{End}(\Lambda)$ has finite index as subgroup of Λ because it is an order in K, so it has rank 2 as $\mathbb{Z}$-module, and Λ has also rank 2. Then, since $\tau \in \Lambda$ and $\mathrm{End}(\Lambda)$ is a subgroup of Λ, there exists $\gamma \in \mathbb{Z}$ such that $\gamma\tau \in \mathrm{End}(\Lambda)$. Since $\Lambda =< 1, \tau >_{\mathbb{Z}}$, this implies that $\gamma\,\Lambda \subset \mathrm{End}(\Lambda)$. Given $\beta \in K$, we have that $\beta(\gamma\Lambda) \subset \gamma\Lambda$ if and only if $\beta\Lambda \subset \Lambda$, which is equivalent to $\beta \in \mathrm{End}(\Lambda)$. In other words,

$$\{\beta \in K \mid \beta\gamma\Lambda \subset \gamma\Lambda\} = \mathrm{End}(\Lambda) = \mathcal{O}.$$

This proves that $\gamma\,\Lambda$ is a proper ideal of $\mathrm{End}(\Lambda)$, and it is clearly homothetic to Λ. □

In the sequel, K will always denote an imaginary quadratic field.

We can precise a bit more this connection. The following theorem characterizes whether a complex non-integer number lies in the endomorphism ring of a lattice in terms of the Weierstrass $\wp$-function of the lattice and an order in a imaginary quadratic field. Thus, it characterizes the complex multiplication property of the elliptic curve.

Theorem 4.42. *Let Λ be a lattice and let $\alpha \in \mathbb{C} - \mathbb{Z}$. The following statements are equivalent:*

1. *There is a rational function $R(x) \in \mathbb{C}(x)$ such that $\mathfrak{P}(\alpha\,z) = R(\mathfrak{P}(z))$*

2. $\alpha\,\Lambda \subset \Lambda$.

3. *There is an order $\mathcal{O}$ in a imaginary quadratic field K such that $\alpha \in \mathcal{O}$ and Λ is homothetic to a proper fractional ideal of $\mathcal{O}$.*

The proof of this result can be found in [6] (Theorem 10.14).

Let K be an imaginary quadratic field and let $\mathcal{O}$ be an order of K. Once we have established the connection between complex multiplication and orders in imaginary quadratic fields, we can relate it to fractional ideals of $\mathcal{O}$ (or homothety classes of such ideals, to be more accurate). Namely, let $\mathfrak{a}$ be a fractional ideal of $\mathcal{O}$. By Proposition 2.14, $\mathfrak{a}$ is a free $\mathbb{Z}$-module of rank 2. But $\mathcal{O}$ contains a $\mathbb{Q}$-basis of K, so the two generators of $\mathfrak{a}$ are $\mathbb{R}$-linearly independent. This says that $\mathfrak{a}$ itself is a lattice. It is not true that different lattices correspond to different fractional ideals of $\mathcal{O}$. Instead of this, we have the following.

Proposition 4.43. *Let $\mathfrak{a}$, $\mathfrak{b}$ be fractional ideals of $\mathcal{O}$. Then,*

$$\overline{\mathfrak{a}} = \overline{\mathfrak{b}} \Longleftrightarrow \mathfrak{a} \sim \mathfrak{b},$$

where $\sim$ denotes the homothety relation of lattices (see Definition 4.16).

Proof. We have that $\mathfrak{a}$ and $\mathfrak{b}$ are homothetic if and only if there exists a non-zero $\alpha \in \mathbb{C}$ such that $\mathfrak{a} = \alpha\,\mathfrak{b} =< \alpha > \mathfrak{b}$. Since $\overline{< \alpha >} = 1$ for all $\alpha \in \mathbb{C} - \{0\}$, this is equivalent to $\overline{\mathfrak{a}} = \overline{\mathfrak{b}}$. □

We can define the j-invariant of a non-real complex number in the following way.

Definition 4.44. *Let $\tau \in \mathbb{C} - \mathbb{R}$. The j-invariant of τ is*

$$j(\tau) = j(< 1, \tau >_{\mathbb{Z}}).$$

We have a function $j : \mathbb{C} - \mathbb{R} \longrightarrow \mathbb{C}$ which is trascendent (it is given by some arithmetic operations with series).

Let $\alpha, \beta \in \mathbb{C}$ such that $\mathfrak{a} =< \alpha, \beta >_{\mathbb{Z}}$. Since α and β are $\mathbb{R}$-linearly independent, at least one of them is not real. Hence

$$\mathfrak{a} = \alpha\ < 1, \tau >_{\mathbb{Z}},\ \alpha \in \mathbb{C}, \tau \in \mathbb{C} - \mathbb{R}.$$

Thus, $\mathfrak{a}$ and $< 1, \tau >_{\mathbb{Z}}$ are homothetic. By Proposition 4.17, $j(\tau) = j(\mathfrak{a})$.

Let us denote $\mathcal{R} = \{\Lambda \subset \mathbb{C} \,|\, \Lambda \text{ lattice, } \mathrm{End}(\Lambda) \cong \mathcal{O}\}$. By the previous proposition, there is a well defined and bijective map

$$\begin{array}{ccc} \mathcal{C}(\mathcal{O}) & \longrightarrow & \mathcal{R}/\sim \\ \overline{\mathfrak{a}} & \longmapsto & [\mathfrak{a}] \end{array},$$

where $[\Lambda]$ denotes the homothety class of the lattice Λ.

Proposition 4.45. *Let $\mathcal{O}$ be an order of K. A lattice Λ in $\mathbb{C}$ is homothetic to a proper fractional ideal of $\mathcal{O}$ if and only if* $\mathrm{End}(\Lambda) = \mathcal{O}$.

Proof. The implication to the left side follows immediately from Theorem 4.41. Conversely, let $\mathfrak{a}$ be a proper fractional ideal of $\mathcal{O}$ such that $\Lambda \sim \mathfrak{a}$. Then, there exists $\beta \in \mathbb{C}$ such that $\Lambda = \beta\,\mathfrak{a}$. Now, by the definition of proper fractional ideal:

$$\mathrm{End}(\Lambda) = \{\alpha \in \mathbb{C} \,|\, \alpha\,\Lambda \subset \Lambda\} = \{\alpha \in \mathbb{C} \,|\, \alpha\,\beta\,\mathfrak{a} \subset \beta\,\mathfrak{a}\} = \{\alpha \in \mathbb{C} \,|\, \alpha\,\mathfrak{a} \subset \mathfrak{a}\} = \mathcal{O}.$$

□

Let $E = E_\Lambda$ be an elliptic curve defined over $\mathbb{C}$ and let $\xi : \mathbb{C}/\Lambda \longrightarrow E$ be an analytic parametrization. To close the section, we see an application of Theorem 4.42 in order to compute the explicit expression of the image of a point $P \in E$ by the endomorphism $\xi^{-1} \circ \phi_\alpha \circ \xi$ induced by an element $\alpha \in \mathrm{End}(\Lambda)$ (see Corollary 4.38).

Corollary 4.46. *Let $E = E_\Lambda$ be an elliptic curve over $\mathbb{C}$ with complex multiplication and let $\alpha \in \mathrm{End}(\Lambda)$, $\alpha \notin \mathbb{Z}$. Let $\xi : \mathbb{C}/\Lambda \longrightarrow E$ be an analytic parametrization. There is a rational function $R(x) \in \mathbb{C}(x)$ such that*

$$\xi \circ \phi_\alpha \circ \xi^{-1}(x, y) = (R(x), \frac{1}{\alpha}\, R'(x)\, y),\ (x, y) \in E(\mathbb{C}).$$

Proof. Since $\alpha\,\Lambda \subset \Lambda$ and $\alpha \notin \mathbb{Z}$, by the previous theorem, there exists $R(x) \in \mathbb{C}(x)$ such that $\wp(\alpha\, z) = R(\wp(z))$ for all $z \in \mathbb{C}$. If we derivate at both sides of the equality with respect to z,

$$\wp'(\alpha\, z) = \frac{1}{\alpha}\, R'(\wp(z))\, \wp'(z).$$

Let $(x, y) \in E(\mathbb{C})$. By Theorem 4.15, there exists $z \in \mathbb{C}$ such that $(x, y) = (\wp(z), \wp'(z))$. Then,

$$\xi \circ \phi_\alpha \circ \xi^{-1}(x, y) = (\wp(\alpha\, z), \wp'(\alpha\, z)) = (R(\wp(z)), \frac{1}{\alpha}\, R'(\wp(z))\, \wp'(z)) = (R(x), \frac{1}{\alpha}\, R'(x)\, y).$$

□

5 Torsion points of elliptic curves

Let E be an elliptic curve defined over a field F. We know that we can endow its set of points $E(F)$ with a group structure. The points of finite order of this kind of groups are a very useful tool in algebraic number theory. We will also construct the Tate module and the Weil pairing. If $F = K$ is an imaginary quadratic field, this will play an important role in order to make the explicit construction of the ray class field of K.

Definition 4.47. *Let E be an elliptic curve and let $m \in \mathbb{Z}_{\geq 0}$. The m-torsion subgroup of E is the set*

$$E[m] = \{P \in E(\overline{F}) \,|\, [m]P = \infty\}$$

of the points of E that have order dividing m.

After this definition, it is automatic that $E[m] = \mathrm{Ker}([m])$.

Definition 4.48. *The torsion subgroup of an elliptic curve E is the set*

$$E_{tors} = \bigcup_{m=1}^{\infty} E[m].$$

It is interesting to mention that $E[m] \cong (\mathbb{Z}/m\mathbb{Z}) \times (\mathbb{Z}/m\mathbb{Z})$ whenever m is coprime to $char(K)$. The proof of this fact can be found in [9] (Chapter III, Corollary 6.4).

The Tate module and the Weil pairing

Let E be an elliptic curve defined over a field F. Let l be a prime number and $m \geq 2$ prime to $\mathrm{char}(F)$ if $\mathrm{char}(F) \neq 0$. Let us consider the group

$$E[l^m] = \{P \in E(\overline{F}) \,|\, l^m\, P = \infty\} \cong \mathbb{Z}/(l^m\mathbb{Z}) \times \mathbb{Z}/(l^m\mathbb{Z}).$$

Note that the collection of the groups $E[l^m]$ together with the morphisms multiplication by l

$$\begin{array}{ccc} E[l^m] & \longrightarrow & E[l^{m-1}] \\ P & \longmapsto & l\,P \end{array}$$

form a inverse system.

Definition 4.49. *The l-adic Tate module associated to E is the inverse limit*

$$T_l(E) := \lim_{\longleftarrow} E[l^m].$$

If $\mathbb{Z}_l$ is the ring of l-adic numbers, then $\mathbb{Z}_l = \lim_{\longleftarrow} \mathbb{Z}/(l^m\mathbb{Z})$. Moreover, $E[l^m] \cong \mathbb{Z}/(l^m\mathbb{Z}) \times \mathbb{Z}/(l^m\mathbb{Z})$. Then,

$$T_l(E) \cong \mathbb{Z}_l \times \mathbb{Z}_l.$$

The idea to define the Weil pairing is to construct a collection of pairings $e_{E,m} : E[m] \times E[m] \longrightarrow \mu_m$, where m is a non-negative integer μ_m is the group of m-th roots of unity. Taking inverse limits, we obtain a pairing $e_E : T_l(E) \times T_l(E) \longrightarrow T_l(\mu)$ called the Weil pairing. Here the latter module is the inverse limit

$$T_l(\mu) = \lim_{\longleftarrow} \mu_{l^m}$$

with respect to the multiplication by l morphisms. We will only state the existence result of the Weil pairing, but this strategy can be consulted in [10].

Proposition 4.50. *There exists a pairing*

$$e_E : T_l(E) \times T_l(E) \longrightarrow T_l(\mu)$$

which is:

1. *Bilinear, i.e,*

$$e_E(P_1 + P_2, Q) = e_E(P_1, Q)\, e_E(P_2, Q) \text{ for all } P_1, P_2, Q \in T_l(E),$$
$$e_E(P, Q_1 + Q_2) = e_E(P, Q_1)\, e_E(P, Q_2) \text{ for all } P, Q_1, Q_2 \in T_l(E).$$

2. *Alternating, i.e, $e_E(P, P) = 1$ for all $P \in T_l(E)$.*

3. *Non-degenerate, that is,*

$$e_E(P, Q) = 1 \text{ for all } P \in E[m] \Longrightarrow Q = \infty.$$

4. *Galois invariant, that is,*

$$e_E(P, Q)^\sigma = e_E(P^\sigma, Q^\sigma) \text{ for all } \sigma \in \mathrm{Gal}(\overline{K}/K).$$

We will need another property of the Weil pairing: if $\phi : E_1 \longrightarrow E_2$ is an isogeny and $\hat{\phi}$ is its dual, then ϕ and $\hat{\phi}$ are adjoint for the Weil pairing, that is,

$$e_{E_2}(\phi(x), y) = e_{E_1}(x, \hat{\phi}(y)).$$

6 Elliptic curves over finite fields

In this section we are going to present the main notions and results about elliptic curves over finite fields. First, we will revise a few notions about such elliptic curves and after that we will study the reduction of elliptic curves, which will be fairly used in the second part of the thesis. The idea is to reduce the coefficients of an equation to some residue field of the number ring by a prime ideal in such a way we obtain an elliptic curve.

Recall that if K is a finite field with q elements, then $q = p^r$, where p is prime and $r \in \mathbb{N}$. We denote $K = \mathbb{F}_q$.

Let E be an elliptic curve over a finite field $\mathbb{F}_q$. It is immediate that $E(\mathbb{F}_q)$ is finite.

As we classified the endomorphism ring of lattices (or equivalently, of elliptic curves defined over $\mathbb{C}$), we can also classify the endomorphism ring of elliptic curves defined over finite fields. To understand this classification, we introduce quaternion algebras.

Definition 4.51. *A quaternion algebra is an algebra over $\mathbb{Q}$ with a basis $\{1, \alpha, \beta, \alpha\,\beta\}$ such that $\alpha^2, \beta^2 \in \mathbb{Q}^-$ and $\alpha\,\beta = -\beta\,\alpha$.*

The concept of order in a quaternion algebra is a natural generalization of the case of number fields.

Definition 4.52. *An order in a quaternion algebra $\mathcal{H}$ is a subring $\mathcal{O}$ of $\mathcal{H}$ such that $\mathcal{O} \oplus \mathbb{Q} = \mathcal{H}$.*

Now, the following theorem gives us the possibilities for the ring of endomorphisms of an elliptic curve defined over a finite field.

Theorem 4.53. *Let E be an elliptic curve defined over $\mathbb{F}_q$. Then, $\mathrm{End}_{\mathbb{F}_q}(E)$ is either an order in an imaginary quadratic field or an order in a quaternion algebra.*

The proof is in [9] (Chapter V, Theorem 3.1).

Reduction of elliptic curves

Let K be a number field and let E be an elliptic curve defined by the Weierstrass equation

$$y^2 = 4x^3 - g_2\,x - g_3,\ g_2, g_3 \in K.$$

Let us fix a prime ideal P of $\mathcal{O}_K$. Assume that P is not over g_2 and g_3. Since K is the field of fractions of $\mathcal{O}_K$, $g_i = \frac{\alpha_i}{\beta_i}$, with $\alpha_i, \beta_i \in \mathcal{O}_K$, $\beta_i \notin P$. Hence, we can define

$$[g_i] := [\alpha_i]\,[\beta_i]^{-1},$$

where $[\cdot]$ is the class in $\mathcal{O}_K$ modulo P. Thus, we can define an algebraic curve $\widetilde{E}$ of equation

$$y^2 = 4x^3 - [g_2]x - [g_3].$$

The discriminant of this curve is

$$\Delta = [g_2]^3 - 27[g_3]^2.$$

If $\Delta \neq 0$, then $\widetilde{E}$ is an elliptic curve over $\mathcal{O}_K/P$, and we say that E has good reduction at P. Otherwise, we say that E has bad reduction at P.

Proposition 4.54. *Let E be an elliptic curve defined over K, P a prime of K such that E has good reduction at P and let $\widetilde{E}$ be its reduction. Let $m \in \mathbb{Z}$ be a positive integer coprime with $char(k)$, where $k = \mathcal{O}_K/P$ is the residue field. Then, the restriction of the projection map to $E[m]$,*

$$E[m] \longrightarrow \widetilde{E}(k),$$

is injective.

As we mentioned at the beginning of this chapter, reduction of elliptic curves is a very important tool for us because we will need to reduce equations of elliptic curves to a residue field. But we will also deal with isogenies, so we may define the reduction of an isogeny.

Definition 4.55. *Let $\phi : E_1 \longrightarrow E_2$ be an isogeny between elliptic curves defined over a finite field F. Let $R(x,y), S(x,y) \in K(E_1)$ such that $\phi(x,y) = (R(x,y), S(x,y))$. Let P be a prime of F such that both E_1 and E_2 have good reduction at P. We define the reduction of ϕ as the isogeny*

$$\begin{array}{rccc} \widetilde{\phi}: & \widetilde{E_1} & \longrightarrow & \widetilde{E_2} \\ & (x,y) & \longmapsto & (\widetilde{R}(x,y), \widetilde{S}(x,y)) \end{array}$$

The reduction of an isogeny is indeed an isogeny because the reduction of the infinity point of an elliptic curve is the infinity point of the reduction of the elliptic curve. Hence, the reduction map

$$\begin{array}{ccc} \mathrm{Hom}(E_1, E_2) & \longrightarrow & \mathrm{Hom}(\widetilde{E_1}, \widetilde{E_2}) \\ \phi & \longmapsto & \widetilde{\phi} \end{array}$$

is well defined. Using the results studied in this section, we can prove that this map is injective.

Proposition 4.56. *Let L be a number field and let Q be a prime ideal in L. Let E_1, E_2 be elliptic curves defined over L with good reduction at Q. Then, the map*

$$\begin{array}{ccc} \mathrm{Hom}(E_1, E_2) & \longrightarrow & \mathrm{Hom}(\widetilde{E_1}, \widetilde{E_2}) \\ \phi & \longmapsto & \widetilde{\phi} \end{array}$$

is injective and $\deg(\phi) = \deg(\widetilde{\phi})$.

Proof. Let $\phi \in \mathrm{Hom}(E_1, E_2)$ such that $\widetilde{\phi}$ is the zero isogeny. If p is the prime number under Q, then $\mathrm{char}(\mathcal{O}_L/Q) = p$. Given a positive integer m coprime with p, by Proposition 4.54, we have that the reduction map

$$E_2[m] \longrightarrow \widetilde{E_2}$$

is injective. Let $P \in E_1[m]$. Then,

$$\widetilde{\phi(P)} = \widetilde{\phi}(\widetilde{P}) = \widetilde{\infty},$$

so $\phi(P)$ lies in the kernel of the previous reduction map, and then $\phi(P) = \infty$. This proves that $E_1[m] \subset \mathrm{Ker}(\phi)$ for all m positive integer coprime with p. Now, the set of

such m is infinite, so $\mathrm{Ker}(\phi)$ is infinite. But the kernel of a non-zero isogeny is finite (see [9], Chapter III, Corollary 4.9). We conclude that ϕ is the zero isogeny, which proves that the reduction map is injective.

It remains to prove that $\deg(\phi) = \deg(\widetilde{\phi})$. Let l be a prime number such that $l \neq p$. Let $x, y \in T_l(E_1)$. Then, using the properties of the dual isogeny and the Weil pairing,

$$e_{E_1}(x,y)^{\deg(\phi)} = e_{E_1}(\deg(\phi)\, x, y) = e_{E_1}(\hat{\phi} \circ \phi(x), y) = e_{E_2}(\phi(x), \phi(y)).$$

Using the same argument,

$$e_{\widetilde{E_1}}(\widetilde{x}, \widetilde{y})^{\deg(\widetilde{\phi})} = e_{\widetilde{E_2}}(\widetilde{\phi}(\widetilde{x}), \widetilde{\phi}(\widetilde{y})).$$

Let $n \in \mathbb{N}$. Since the reduction $E[l^n] \longrightarrow \widetilde{E}$ is injective and its image is $\widetilde{E}[l^n]$, we have that $E[l^n] \cong \widetilde{E}[l^n]$. Since n is arbitrary, $T_l(E) \cong T_l(\widetilde{E})$. Then, by the construction of the Weil pairing,

$$\widetilde{e_E(x,y)} = e_{\widetilde{E}}(\widetilde{x}, \widetilde{y}) \text{ for all } x, y \in T_l(E).$$

Now, for all $x, y \in T_l(E_1)$,

$$e_{\widetilde{E_1}}(\widetilde{x}, \widetilde{y})^{\deg(\phi)} = \widetilde{e_{E_1}(x,y)}^{\deg(\phi)} = e_{E_2}(\widetilde{\phi(x), \phi(y)}) = e_{\widetilde{E_2}}(\widetilde{\phi}(\widetilde{x}), \widetilde{\phi}(\widetilde{y}) = e_{\widetilde{E_1}}(\widetilde{x}, \widetilde{y})^{\deg(\widetilde{\phi})}.$$

By the linearity of the Weil pairing, this implies that

$$e_{\widetilde{E_1}}((\deg(\phi) - \deg(\widetilde{\phi}))\, x, y) = 0$$

and by the non-degeneracy of the Weil paring, $(\deg(\phi) - \deg(\widetilde{\phi}))\, x = 0$ for all $x \in T_l(E_1)$, that is, $\deg(\phi) = \deg(\widetilde{\phi})$. □

Chapter 5

Class fields of imaginary quadratic fields

The theorems of class field theory provide us information about class fields in a strictly theoretical sense, but the proofs are quite technical and the isomorphisms are highly non-canonical. It is very hard to give an explicit description of class fields of general number fields.

Once we have introduced the theory of elliptic curves, we can precise what we mentioned at the Introduction. If the number field we take is imaginary quadratic, then we can use the theory of elliptic curves with complex multiplication to obtain abelian extensions of an imaginary quadratic field K, and this is the main object of this chapter. For each order $\mathcal{O}$ of K, we will obtain an abelian extension of K. We will provide an explicit construction when the order we take is the ring of integers and we will present without proof a generalization for the situation in which we take any given order.

Recall that the m-th cyclotomic field is

$$L = \mathbb{Q}(e^{\frac{2\pi i}{m}}).$$

This means that the abelian extension L of $\mathbb{Q}$ is obtained by adjoining to $\mathbb{Q}$ the exponential function, which is a trascendental function, evaluated at some complex non-real value. The result we are going to obtain has the same flavor. Concretely, we will see that if K is an imaginary quadratic field, for each order $\mathcal{O}$ in K we can construct an abelian extension of K by adjoining to K the j-function introduced in Definition 4.44 evaluated at some complex non-real number, i.e,

$$L = K(j(\tau)),\ \tau \in \mathbb{C} - \mathbb{R},$$

in such a way that the homothety class of the lattice $\Lambda =< 1, \tau >_{\mathbb{Z}}$ corresponds to any elliptic curve E with complex multiplication by $\mathcal{O}$.

We will see that if we choose $\mathcal{O} = \mathcal{O}_K$, then L is the Hilbert Class Field of K. It is true also that for the order $\mathcal{O}$ of conductor f, L is the Ring class field of conductor f of K.

1 The space of differential forms

We begin by defining and stating the main properties of the space of differential forms of an elliptic curve.

Certainly, the following definitions work with general algebraic curves, but we will restrict to the situation of elliptic curves because we only deal with such curves.

Definition 5.1. *Let E be an elliptic curve defined over a field F. The space of differential forms on E, denoted by Ω_E, is the $\overline{F}(E)$-vector space generated by the symbols of the form dx, $x \in \overline{F}(E)$, with the relations:*

1. $d(x+y) = dx + dy$, $x, y \in \overline{F}(E)$.
2. $d(x\,y) = x\,dy + dx\,y$, $x, y \in \overline{F}(E)$
3. $da = 0$, $a \in \overline{F}$

The space Ω_E has dimension 1 over $\overline{F}(E)$. The proof of this result can be seen in [9] (Chapter IV, Section 4).

Let $\phi : E_1 \longrightarrow E_2$ be a non-constant morphism of elliptic curves. Then the map

$$\phi^* : \overline{F}(E_2) \longrightarrow \overline{F}(E_1)$$

induces another map

$$\begin{array}{rccc} \phi^* : & \Omega_{E_2} & \longrightarrow & \Omega_{E_1} \\ & \sum_{i=1}^n f_i\, dg_i & \longmapsto & \sum_{i=1}^n \phi^*(f_i)\, d(g_i \circ \phi) \end{array} .$$

In other words, we extend ϕ^* to Ω_{E_2} by defining $\phi^*(df) = d(f \circ \phi)$ for $df \in \Omega_{E_2}$ and in such a way that the diagram

$$\begin{array}{ccc} \overline{F}(E_2) \times \Omega_{E_2} & \longrightarrow & \Omega_{E_2} \\ \downarrow & & \downarrow \\ \overline{F}(E_1) \times \Omega_{E_1} & \longrightarrow & \Omega_{E_1} \end{array}$$

is commutative, where the vertical maps are given by $(f, dg) \mapsto (\phi^*(df), \phi^*(dg))$ and the top and bottom maps are given by $(f, dg) \mapsto (f\,dg)$. This map is called the pull-back of ϕ.

Proposition 5.2. *Let $\phi : E_1 \longrightarrow E_2$ be a non constant morphism of elliptic curves. Then, ϕ is separable if and only if the pull back $\phi^* : \Omega_{E_2} \longrightarrow \Omega_{E_1}$ is injective.*

The proof is in [9], Chapter II, Section 4.

Note that, in particular, when E_1 and E_2 are defined over $\mathbb{C}$, ϕ^* is injective.

Let E be an elliptic curve over a field F. Let $Q \in E(F)$. Then, the map

$$\begin{array}{rccc} \tau_Q : & E & \longrightarrow & E \\ & P & \longmapsto & P + Q \end{array}$$

is an isomorphism of algebraic curves (it is not an isogeny unless $Q = \infty$). Its pull-back is

$$\begin{array}{rccc} \tau_Q^* : & \Omega_E & \longrightarrow & \Omega_E \\ & df & \longmapsto & d(f \circ \tau_Q). \end{array}$$

Definition 5.3. *We say that a differential $\omega \in \Omega_E$ is invariant if $\tau_Q^*(\omega) = \omega$ for all $Q \in E(F)$.*

Let $\omega = \frac{dx}{2y} \in \Omega_E$ (here x and y denote the first and second coordinate functions from E to $\overline{F}$, respectively). Then $\tau_Q^*(\omega) = \omega$ for every $Q \in E$ (see [9], Chapter III, Proposition 5.1). The differential ω is an invariant differential of E. This differential is usually called the invariant differential of E. The reason is that the invariant differentials from a K-vector space of dimension 1 (see [7], Page 32).

Remark 5.4. *For the general form of the equation of an elliptic curve, the invariant differential is*

$$\omega = \frac{2x}{2y + a_1\, x + a_3}.$$

We use these notions to introduce an important tool: the normalized identification of the endomorphism rings of elliptic curves with complex multiplication. The idea is the following: If E_Λ is an elliptic curve defined over $\mathbb{C}$ with complex multiplication by $\mathcal{O}$, by Theorem 4.41, $\mathrm{End}(\Lambda) = \mathcal{O}$. Then, there is a one-to-one correspondence between $\mathcal{O}$ and $\mathrm{End}(E)$, in which an integer number m corresponds to the multiplication-by-m endomorphism $[m]$. We explore this correspondence for any element $\alpha \in \mathcal{O}$.

Proposition 5.5. *Let E be an elliptic curve defined over $\mathbb{C}$ with complex multiplication by a subring R of $\mathbb{C}$. Then, there is an unique isomorphism*

$$[\cdot] \,:\, R \longrightarrow \mathrm{End}(E)$$

such that for all non-zero invariant differential $\omega \in \Omega_E$, we have that

$$[\alpha]^*(\omega) = \alpha\, \omega \text{ for all } \alpha \in R.$$

Proof. Let Λ be a lattice such that $E = E_\Lambda$ and let $\xi : \mathbb{C}/\Lambda \longrightarrow E_\Lambda$ be the corresponding analytic parametrization. By Corollary 4.38, there is a bijection

$$\begin{array}{ccc} \mathrm{End}(\Lambda) & \longrightarrow & \mathrm{End}(E) \\ \alpha & \longmapsto & \xi \circ \phi_\alpha \circ \xi^{-1}. \end{array}$$

Since E has complex multiplication by R, given $\alpha \in R$, we have that $\alpha\, \Lambda \subset \Lambda$. Let us define the map

$$\begin{array}{rccl} [\cdot]: & R & \longrightarrow & \mathrm{End}(E) \\ & \alpha & \longmapsto & [\alpha] := \xi \circ \phi_\alpha \circ \xi^{-1} \,:\, E \longrightarrow E. \end{array}$$

In other words, $[\alpha]$ is the map that makes the following diagram commutative:

$$\begin{array}{ccc} \mathbb{C}/\Lambda & \xrightarrow{\phi_\alpha} & \mathbb{C}/\Lambda \\ \downarrow{\scriptstyle \xi} & & \downarrow{\scriptstyle \xi} \\ E_\Lambda & \xrightarrow{[\alpha]} & E_\Lambda \end{array}$$

Let us check that $[\cdot]$ is a ring homomorphism. Given $\alpha, \beta \in R$,

$$[\alpha] \circ [\beta] = \xi \circ \phi_\alpha \circ \xi^{-1} \circ \xi \circ \phi_\beta \circ \xi^{-1} = \xi \circ \phi_\alpha \circ \phi_\beta \circ \xi^{-1} = \xi \circ \phi_{\alpha\,\beta} \circ \xi^{-1} = [\alpha\, \beta].$$

Let us prove that $[\cdot]$ is bijective. Let α, $\beta \in R$ such that $[\alpha] = [\beta]$. Since ξ is bijective, we arrive immediately to the equality $\phi_\alpha = \phi_\beta$. Using the first statement of Theorem 4.36, we obtain that $\alpha = \beta$. This proves that $[\cdot]$ is injective. For the surjectivity, let $\phi \in \mathrm{End}(E)$. Then, by the second statement of Theorem 4.36, $\rho = \xi^{-1} \circ \phi \circ \xi : \mathbb{C}/\Lambda \longrightarrow \mathbb{C}/\Lambda$ is an holomorphic map such that $\rho(0) = 0$. Now, using again Part 1 of the same result, there is an unique $\alpha \in \mathbb{C}$ with $\alpha\,\Lambda \subset \Lambda$ such that $\rho = \phi_\alpha$. Hence, we obtain that $\phi = \xi \circ \phi_\alpha \circ \xi^{-1}$, which proves the surjectivity. This proves that $[\cdot]$ is an isomorphism.

Now, we have to prove that $[\alpha]^*(\omega) = \alpha\,\omega$ for all $\omega \in \Omega_E$. We consider the pull-back $\xi^* : \Omega_E \longrightarrow \Omega(\mathbb{C}/\Lambda)$ where the latter is the space of 1-forms of $\mathbb{C}/\Lambda$. Since ξ is an analytic isomorphism, ξ^* is a linear isomorhism. Thus, given $\omega \in \Omega_E$, there is an invariant differential $dz \in \Omega(\mathbb{C}/\Lambda)$ such that $\xi^*(\omega) = c\,dz$. Then:

$$[\alpha]^*(\omega) = (\xi \circ \phi_\alpha \circ \xi^{-1})^*(\omega) = (\xi^{-1})^* \circ \phi_\alpha^* \circ \xi^*(\omega) =$$
$$(\xi^{-1})^* \circ \phi_\alpha^*(c\,dz) = (\xi^{-1})^*(c\,\alpha\,dz) = \alpha\,(\xi^{-1})^*(c\,dz) = \alpha\,\omega.$$

□

The map $[\cdot]$ is an identification between $\mathrm{End}(E)$ and R whose pull-back has a very simple expression. This will be a notable advantage for succesive computations. Note also that given $\alpha \in R$, $[\alpha]$ is the multiplication-by-α morphism in the analytic sense. This means that, fixed a parametrization $\xi : \mathbb{C}/\Lambda \longrightarrow E$, $[\alpha]$ sends a point $P = \xi(z)$ to the point that corresponds to $\xi(\alpha\,z)$. Indeed,

$$[\alpha](\xi(z)) = \xi \circ \phi_\alpha \circ \xi^{-1} \circ \xi(z) = \xi \circ \phi_\alpha(z) = \xi(\alpha\,z).$$

In particular, when we choose an integer m, we recover the multiplication-by-m morphism.

We give a name to this identification.

Definition 5.6. *With the notation of the proposition above, we say that $[\cdot]$ is the normalized identification and the pair $(E, [\cdot])$ is normalized.*

Corollary 5.7. *Let $(E_1, [\cdot]_{E_1})$ $(E_2, [\cdot]_{E_2})$ be normalized elliptic curves defined over $\mathbb{C}$ with complex multiplication by a subring $R \subset \mathbb{C}$. Let $\phi : E_1 \longrightarrow E_2$ be an isogeny. Then,*

$$\phi \circ [\alpha]_{E_1} = [\alpha]_{E_2} \circ \phi.$$

Proof. Let $\omega \in \Omega_E$ be a non-zero invariant differential. Then,

$$(\phi \circ [\alpha]_{E_1})^*(\omega) = [\alpha]_{E_1}^*(\phi^*(\omega)) = \alpha\,\phi^*(\omega) = \phi^*(\alpha\,\omega) = \phi^*([\alpha]_{E_2}^*(\omega)) = ([\alpha]_{E_2} \circ \phi)^*(\omega). \tag{5.1}$$

Since both E_1 and E_2 are defined over $\mathbb{C}$, which has charasteristic zero, any isogeny $\phi : E_1 \longrightarrow E_2$ is separable. Let us consider the map

$$\begin{array}{rccc} \Phi : & \mathrm{Hom}(E_1, E_2) & \longrightarrow & \mathrm{Hom}(\Omega_{E_2}, \Omega_{E_1}) \\ & \psi & \longmapsto & \psi^* \end{array}$$

We have that $\mathrm{Hom}(E_1, E_2)$ is a $\mathbb{Z}$-module (see [9], Chapter III, Corollary 7.5), and $\mathrm{Hom}(\Omega_{E_2}, \Omega_{E_1})$ is also a $\mathbb{Z}$-module because it is the set of linear maps between the vector spaces Ω_{E_2} and Ω_{E_1}. Now, by Theorem 5.2 of Chapter III in [9], Φ is a homomorphism of $\mathbb{Z}$-modules.

Given $\psi \in \mathrm{Hom}(E_1, E_2)$ non-zero, since ψ is separable, we have by Proposition 5.2 that ψ^* is injective, so $\psi^* \neq 0$. Equivalently, $\psi^* = 0 \Longrightarrow \psi = 0$. This says that Φ is injective.

Applying this fact to the equality (5.1), we obtain that $\phi \circ [\alpha]_{E_1} = [\alpha]_{E_2} \circ \phi$. □

Let E be an elliptic curve defined over a field F. By Section 3 of the previous chapter, $\mathrm{Gal}(\overline{F}/F)$ acts over $\mathrm{End}(E)$ in such a way that for $\sigma \in \mathrm{Gal}(\overline{F}/F)$ and $\phi \in \mathrm{End}(E)$, we have the endomorphism $\phi^\sigma \in \mathrm{End}(E)$. When we take the normalized identification, this action is related to the usual action of the Galois group over the elements of the extension.

Proposition 5.8. *Let E be an elliptic curve with complex multiplication by a subring R of $\mathbb{C}$. Let us take the normalized identifications $[\cdot]_E : R \longrightarrow \mathrm{End}(E)$ and $[\cdot]_{E^\sigma} : R \longrightarrow \mathrm{End}(E^\sigma)$. Given $\sigma \in \mathrm{Aut}(\mathbb{C})$,*

$$[\alpha]_E^\sigma = [\alpha^\sigma]_{E^\sigma} \text{ for all } \alpha \in R.$$

Proof. Fix a Weierstrass equation for E

$$E : y^2 = 4\,x^3 - g_2\,x - g_3.$$

Let $\omega = \frac{dx}{2\,y}$ be the invariant differential of E. By Proposition 5.5,

$$[\alpha]^*(\omega) = \alpha\,\omega \text{ for all } \alpha \in R.$$

Let $\sigma \in \mathrm{Aut}(\mathbb{C})$. Then, we have a Weierstrass equation for E^σ

$$E^\sigma : y^2 = 4\,x^3 - g_2^\sigma\,x - g_3^\sigma.$$

Thus, $\omega^\sigma = \frac{dx}{2^\sigma\,y} = \frac{dx}{2\,y}$ is the invariant differential of E^σ. Again by Proposition 5.5,

$$[\beta]_{E^\sigma}^*(\omega^\sigma) = \beta\,\omega^\sigma \text{ for all } \beta \in R.$$

Let $\alpha \in R$ and $\sigma \in \mathrm{Aut}(\mathbb{C})$. Then,

$$[\alpha^\sigma]_{E^\sigma}^*(\omega^\sigma) = \alpha^\sigma\,\omega^\sigma = (\alpha\,\omega)^\sigma = ([\alpha]_E^*(\omega))^\sigma = ([\alpha]_E^\sigma)^*(\omega^\sigma). \tag{5.2}$$

By using the same argument as in Corollary 5.7, we have that the map

$$\begin{array}{ccc} \mathrm{End}(E^\sigma) & \longrightarrow & \mathrm{End}(\Omega_E^\sigma) \\ \phi & \longmapsto & \phi^* \end{array}$$

is injective. Applying this to the equality (5.2), we obtain that

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

□

2 The set of elliptic curves with complex multiplication

Let K be an imaginary quadratic field and let $\mathcal{O}$ be an order in K. Let $\cong_{\mathbb{C}}$ be the relation isomorphism over $\mathbb{C}$ of elliptic curves. We denote

$$\mathcal{ELL}(\mathcal{O}) = \{E/\mathbb{C} \text{ elliptic curve} \,|\, \mathrm{End}(E) \cong \mathcal{O}\}/\cong_{\mathbb{C}} .$$

The set $\mathcal{ELL}(\mathcal{O})$ is the set of $\mathbb{C}$-isomorphisms classes of elliptic curves with complex multiplication by $\mathcal{O}$. Recall that we want to construct an abelian extension of K by adjoining to K the j-invariant of an elliptic curve with complex multiplication by $\mathcal{O}$. It is natural to think that a good knowledge of the set of classes of such curves will be so useful for our purposes. What we are going to do is to define an action of $\mathcal{C}(\mathcal{O})$ over this set, in order to prove that it is finite. This will allow us to prove that there are finitely many classes, which will be the key to prove important results in the next section.

In the sequel, we will write the elements of $\mathcal{ELL}(\mathcal{O})$ as simply elliptic curves, but we will keep in mind that in fact we are working with isomorphism classes of elliptic curves.

Let $\mathfrak{a}$ be a proper fractional ideal in $\mathcal{O}$. As we know by the previous chapter, $\mathfrak{a}$ is a lattice in $\mathbb{C}$. Hence, we can consider the corresponding elliptic curve $E_{\mathfrak{a}}$ defined over $\mathbb{C}$. By Proposition 4.45,

$$\mathrm{End}(E_{\mathfrak{a}}) \cong \mathrm{End}(\mathfrak{a}) = \mathcal{O}.$$

Hence $E_{\mathfrak{a}} \in \mathcal{ELL}(\mathcal{O})$. Thus, we have a well defined map

$$\begin{array}{ccc} \mathcal{C}(\mathcal{O}) & \longrightarrow & \mathcal{ELL}(\mathcal{O}) \\ \overline{a} & \longmapsto & [E_{\mathfrak{a}}]. \end{array}$$

Let $\mathfrak{a}$ be a proper fractional ideal of $\mathcal{O}$ and let $E_\Lambda \in \mathcal{ELL}(\mathcal{O})$. We denote

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

The following result asserts that $\mathfrak{a}\Lambda$ defined on this way is a lattice in $\mathbb{C}$ and establishes its main properties.

Proposition 5.9. *Let $E_\Lambda \in \mathcal{ELL}(\mathcal{O})$ and let $\mathfrak{a}, \mathfrak{b}$ be proper fractional ideals of $\mathcal{O}$. Then:*

1. *$\mathfrak{a}\Lambda$ is a lattice in $\mathbb{C}$.*
2. *$\mathrm{End}(E_{\mathfrak{a}\Lambda}) \cong \mathcal{O}$.*
3. *$E_{\mathfrak{a}\Lambda} \cong E_{\mathfrak{b}\Lambda} \Longleftrightarrow \overline{\mathfrak{a}} = \overline{\mathfrak{b}}$.*

Proof. 1. By definition of $\mathcal{ELL}(\mathcal{O})$, we have that $\mathrm{End}(E_\Lambda) \cong \mathcal{O}$. This implies that $\mathcal{O}\Lambda = \Lambda$. Indeed, the inclusion $\Lambda \subset \mathcal{O}\Lambda$ is trivial because $1 \in \mathcal{O}$. Conversely, if $\alpha \in \mathcal{O}$, since $\mathcal{O} \cong \mathrm{End}(E_\Lambda)$, we have that $\alpha\Lambda \subset \Lambda$. Hence, $\mathcal{O}\Lambda \subset \Lambda$.

Since $\mathfrak{a}$ is a fractional ideal, there exists $d \in \mathbb{Z}$, $d \neq 0$, such that $d\mathfrak{a} \subset \mathcal{O}$. Then,

$$\mathfrak{a}\Lambda \subset \frac{1}{d}\mathcal{O}\Lambda = \frac{1}{d}\Lambda,$$

which proves that $\mathfrak{a}\Lambda$ is a discrete subgroup of $\mathbb{C}$.

Since $|\mathcal{O}/\mathfrak{a}| < \infty$, there exists $d' \in \mathbb{Z}$ such that $d'\mathcal{O} \subset \mathfrak{a}$. Then,

$$d'\Lambda = d'\mathcal{O}\Lambda \subset \mathfrak{a}\Lambda.$$

This implies that the two generators of the lattice $d'\Lambda$ lie in $\mathfrak{a}\Lambda$. Since $\mathfrak{a}\Lambda$ is a discrete subgroup of $\mathbb{C}$, this says that it is a $\mathbb{Z}$-module of rank at least 2. But $\mathbb{C}$ is a $\mathbb{Z}$-module of rank 2, so the rank of $\mathfrak{a}\Lambda$ is exactly 2, that is, it is a lattice.

2. Given $\alpha \in \mathbb{C}$,
$$\alpha\mathfrak{a}\Lambda \subset \mathfrak{a}\Lambda \iff \mathfrak{a}^{-1}\alpha\mathfrak{a}\Lambda \subset \mathfrak{a}^{-1}\mathfrak{a}\Lambda \iff \alpha\Lambda \subset \Lambda.$$

Hence, the set of endomorphisms of $E_{\mathfrak{a}\Lambda}$ is

$$\mathrm{End}(E_{\mathfrak{a}\Lambda}) \cong \{\alpha \in \mathbb{C} \,|\, \alpha\mathfrak{a}\Lambda \subset \mathfrak{a}\Lambda\} = \{\alpha \in \mathbb{C} \,|\, \alpha\Lambda \subset \Lambda\} = \mathrm{End}(E_\Lambda) = \mathcal{O}.$$

3. Using the two equivalent definitions of $\mathcal{ELL}(\mathcal{O})$, two elliptic curves are isomorphic if and only if their corresponding lattices are homothetic. Hence:
$$\begin{aligned} E_{\mathfrak{a}\Lambda} \cong E_{\mathfrak{b}\Lambda} &\iff \mathfrak{a}\Lambda = c\mathfrak{b}\Lambda,\ c \in \mathbb{C}^* \\ &\iff \mathcal{O}\Lambda = c\mathfrak{a}^{-1}\mathfrak{b}\Lambda,\ c \in \mathbb{C}^* \\ &\iff \Lambda = c\mathfrak{a}^{-1}\mathfrak{b}\Lambda,\ c \in \mathbb{C}^* \end{aligned}$$

In a similar way, we prove that

$$E_{\mathfrak{a}\Lambda} \cong E_{\mathfrak{b}\Lambda} \iff \Lambda = c^{-1}\mathfrak{a}\mathfrak{b}^{-1}\Lambda.$$

Assume that $E_{\mathfrak{a}\Lambda} \cong E_{\mathfrak{b}\Lambda}$. Then we have the two previous equalities, and in particular, $c\mathfrak{a}^{-1}\mathfrak{b}\Lambda \subset \Lambda$ and $c^{-1}\mathfrak{a}\mathfrak{b}^{-1}\Lambda \subset \Lambda$, so they are both contained in $\mathcal{O}$. But each of these two ideals are inverse of each other, so they also coincide with $\mathcal{O}$. From here, we deduce that $\mathfrak{a} = c\mathfrak{b}$, that is, $\overline{\mathfrak{a}} = \overline{\mathfrak{b}}$.

The converse is automatic: If $\mathfrak{a}$ and $\mathfrak{b}$ are homothetic, then so are $\mathfrak{a}\Lambda$ and $\mathfrak{b}\Lambda$, so the corresponding elliptic curves $E_{\mathfrak{a}\Lambda}$ and $E_{\mathfrak{b}\Lambda}$ are isomorphic.

□

As a consequence of this result, we can define a group action

$$\begin{array}{ccc} \mathcal{C}(\mathcal{O}) \times \mathcal{ELL}(\mathcal{O}) & \longrightarrow & \mathcal{ELL}(\mathcal{O}) \\ (\overline{\mathfrak{a}}, E_\Lambda) & \longmapsto & \overline{\mathfrak{a}} * E_\Lambda := E_{\mathfrak{a}^{-1}\Lambda}. \end{array}$$

It is, indeed, a well defined action:

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

This action will be very useful because of its properties.

Proposition 5.10. *The action previously defined is simple and transitive. That is, for all $E_{\Lambda_1}, E_{\Lambda_2} \in \mathcal{ELL}(\mathcal{O})$ there is an unique class $\overline{\mathfrak{a}} \in \mathcal{C}(\mathcal{O})$ such that $\overline{\mathfrak{a}} * E_{\Lambda_1} = E_{\Lambda_2}$.*

Proof. Let us prove that the action is transitive (existence of $\overline{\mathfrak{a}}$). Take a non-zero element $\lambda_1 \in \Lambda$ and let $\mathfrak{a}_1 = \frac{1}{\lambda_1}\Lambda_1$. Then $\mathfrak{a} \subset K$ and is a finitely generated $\mathcal{O}$-module, so it is a fractional ideal of $\mathcal{O}$. Similarly, if we take $\lambda_2 \in \Lambda_2$ non-zero, $\mathfrak{a}_2 = \frac{1}{\lambda_2}\Lambda_2$ is a fractional ideal of $\mathcal{O}$. Then,

$$\frac{\lambda_2}{\lambda_1}\mathfrak{a}_2\mathfrak{a}_1^{-1}\Lambda_1 = \frac{\lambda_2}{\lambda_1}(\frac{1}{\lambda_2}\Lambda_2)(\lambda_1\Lambda_1^{-1})\Lambda_1 = \Lambda_2.$$

Let $\mathfrak{a} := \mathfrak{a}_2^{-1}\mathfrak{a}_1$. Then,

$$\overline{\mathfrak{a}} * E_{\Lambda_1} = E_{\mathfrak{a}^{-1}\Lambda_1} = E_{\frac{\lambda_1}{\lambda_2}\Lambda_2} \cong E_{\Lambda_2}.$$

This proves the transitivity.

Now, we have to prove that the action is simple. Let us take $\overline{\mathfrak{a}}, \overline{\mathfrak{b}} \in \mathcal{C}(\mathcal{O})$ and $E_\Lambda \in \mathcal{ELL}(\mathcal{O})$ such that $\overline{\mathfrak{a}} * E_\Lambda = \overline{\mathfrak{b}} * E_\Lambda$. Let us prove that $\overline{\mathfrak{a}} = \overline{\mathfrak{b}}$.

By definition of the action, $E_{\mathfrak{a}^{-1}\Lambda} \cong E_{\mathfrak{b}^{-1}\Lambda}$. Now, using the second part of the previous proposition, we obtain that $\overline{\mathfrak{a}^{-1}} = \overline{\mathfrak{b}^{-1}}$, and this gives us that $\overline{\mathfrak{a}} = \overline{\mathfrak{b}}$. □

Corollary 5.11. *With the previous notation, $\#\mathcal{C}(\mathcal{O}) = \#\mathcal{ELL}(\mathcal{O})$. In particular, $\mathcal{ELL}(\mathcal{O})$ is finite.*

3 Elliptic curves over the algebraic numbers

We are going to prove that we can see the classes in $\mathcal{ELL}(\mathcal{O})$ as classes of elliptic curves defined over the field of the algebraic numbers $\overline{\mathbb{Q}}$. We will need another result which is interesting by itself: the j-invariant of an elliptic curve with complex multiplication by an order $\mathcal{O}$ in an imaginary quadratic field is an algebraic number. These two facts will allow us to define an homorphism which will be the key ingredient for proving the main result of this chapter.

First of all, fix an elliptic curve $E \in \mathcal{ELL}(\mathcal{O})$. Let $\phi : E \longrightarrow E$ be a morphism of elliptic curves. Take also $\sigma \in \mathrm{Aut}(\mathbb{C})$. Clearly, $\phi : E \longrightarrow E$ is an isogeny if and only if $\phi^\sigma : E^\sigma \longrightarrow E^\sigma$ is an isogeny. This implies that $\mathrm{End}(E) \cong \mathrm{End}(E^\sigma)$.

Proposition 5.12. *If $E \in \mathcal{ELL}(\mathcal{O})$, then $j(E) \in \overline{\mathbb{Q}}$.*

Proof. Let $\sigma \in \mathrm{Aut}(\mathbb{C})$. Let us fix an equation

$$E : y^2 = x^3 + ax + b$$

of E and consider the elliptic curve E^σ of equation

$$E^\sigma : y^2 = x^3 + a^\sigma x + b^\sigma.$$

We claim that

$$\#\{j(E)^\sigma \,|\, \sigma \in \mathrm{Aut}(\mathbb{C})\} < \infty.$$

Since $j(E)$ is a rational combination of the coefficients of the equation of E, we have that $j(E^\sigma) = j(E)^\sigma$. But we know that two elliptic curves are isomorphic if and only if they have the same j-invariant, so

$$\#\{j(E)^\sigma \,|\, \sigma \in \mathrm{Aut}(\mathbb{C})\} = \#\{j(E^\sigma) \,|\, \sigma \in \mathrm{Aut}(\mathbb{C})\} = \#\{E^\sigma \,|\, \sigma \in \mathrm{Aut}(\mathbb{C})\},$$

where this last set refers to the isomorphism classes of elliptic curves instead of elliptic curves. Note that by the previous comment, $\mathrm{End}(E^\sigma) \cong \mathrm{End}(E) \cong \mathcal{O}$, so $E^\sigma \in \mathcal{ELL}(\mathcal{O})$ for all $\sigma \in \mathrm{Aut}(\mathbb{C})$. Hence the last set is a subset of $\mathcal{ELL}(\mathcal{O})$, and then it is bounded by its cardinal $\#\mathcal{ELL}(\mathcal{O})$. By Corollary 5.11, this number is finite, and hence we have proved the claim.

Now, assume that $j(E)$ is trascendental. Given a trascendental number r, let us define a $\mathbb{Q}$-inmersion

$$\begin{array}{rccc} \sigma_r\colon & \mathbb{Q}(j(E)) & \longrightarrow & \mathbb{C} \\ & j(E) & \longmapsto & r \end{array}$$

and extended by linearity. Since $\mathbb{Q}(j(E))$ is a subfield of $\mathbb{C}$, it can be extended to an automorphism $\sigma_r \in \mathrm{Aut}(\mathbb{C})$ such that $j(E)^{\sigma_r} = r$.

Since $\overline{\mathbb{Q}}$ is countable and $\mathbb{C}$ is not, the set of trascendental numbers is not countable. Hence, by the previous argument, we obtain an infinite subset $\{j(E)^{\sigma_r} \mid r \text{ trascendental}\}$ of $\{j(E)^\sigma \mid \sigma \in \mathrm{Aut}(\mathbb{C})\}$, which is a contradiction. □

Now, we can use the Theorem 5.12 to prove the other mentioned result. We will denote (only in the next theorem) $\mathcal{ELL}(\mathcal{O})$ by $\mathcal{ELL}_{\mathbb{C}}(\mathcal{O})$ and

$$\mathcal{ELL}_{\overline{\mathbb{Q}}}(\mathcal{O}) = \{E/\overline{\mathbb{Q}} \text{ elliptic curve} \mid \mathrm{End}(E) \cong \mathcal{O}\}/\cong_{\overline{\mathbb{Q}}}.$$

Theorem 5.13. *The natural map*

$$\begin{array}{rccc} \epsilon\colon & \mathcal{ELL}_{\overline{\mathbb{Q}}}(\mathcal{O}) & \longrightarrow & \mathcal{ELL}_{\mathbb{C}}(\mathcal{O}) \\ & E & \longmapsto & E \end{array}$$

is a bijection. In particular, every class of elliptic curves in $\mathcal{ELL}(\mathcal{O})$ has some elliptic curve defined over $\overline{\mathbb{Q}}$.

Proof. Let us prove that ϵ is surjective. Let $E/\mathbb{C} \in \mathcal{ELL}_{\mathbb{C}}(\mathcal{O})$. Since $j(E)$ is an algebraic number, by Proposition 4.7, there exists an elliptic curve $E'/\mathbb{Q}(j(E))$ such that $j(E') = j(E)$. If we regard this equality as an equality of complex numbers, we obtain that $E/\mathbb{C} = E'/\mathbb{C} = \epsilon(E'/\overline{\mathbb{Q}})$.

Now, let us see that ϵ is injective. Let $E_1/\overline{\mathbb{Q}}, E_2/\overline{\mathbb{Q}} \in \mathcal{ELL}(\mathcal{O})$ such that $\epsilon(E_1/\overline{\mathbb{Q}}) = \epsilon(E_2/\overline{\mathbb{Q}})$. This says that $E_1 \cong_{\mathbb{C}} E_2$, so $j(E_1) = j(E_2)$. Since both E_1 and E_2 are defined over $\overline{\mathbb{Q}}$, $j(E_1) = j(E_2) \in \overline{\mathbb{Q}}$, so $E_1 \cong_{\overline{\mathbb{Q}}} E_2$. This means that $E_1/\overline{\mathbb{Q}} = E_2/\overline{\mathbb{Q}}$ as $\overline{\mathbb{Q}}$-isomorphism classes. □

4 Construction of abelian extensions

In this section, we will make the explicit construction of an abelian extension of an imaginary quadratic field K by means of the j-invariant of an elliptic curve with complex multiplication by a fixed order $\mathcal{O}$ of K. That is, for each order in K we will have an abelian extension of K. Eventually, we will state that this abelian extension is just the ring class field of $\mathcal{O}$.

Let us fix, as usual, an imaginary quadratic field K and an order $\mathcal{O}$ in K. Let $E \in \mathcal{ELL}(\mathcal{O})$. By Theorem 5.13, we can choose an elliptic curve defined over $\overline{\mathbb{Q}}$ which

is isomorphism over $\mathbb{C}$ to E, so we can assume that E itself is defined over $\overline{\mathbb{Q}}$. Let $\sigma \in \mathrm{Gal}(\overline{K}/K)$. Since $\overline{K} = \overline{\mathbb{Q}}$ and E is defined over $\overline{\mathbb{Q}}$, the curve E^σ is well defined.

Now, let $\sigma \in \mathrm{Gal}(\overline{K}/K)$ and $E \in \mathcal{ELL}(\mathcal{O})$. By Proposition 5.10, the action

$$* : \mathcal{C}(\mathcal{O}) \times \mathcal{ELL}(\mathcal{O}) \longrightarrow \mathcal{ELL}(\mathcal{O})$$

is simple and transitive, so for the elliptic curves E and E^σ there is an unique class of ideals $\overline{\mathfrak{a}_\sigma} \in \mathcal{C}(\mathcal{O})$ such that $\overline{\mathfrak{a}_\sigma} * E = E^\sigma$. Thus, we have a map

$$\begin{array}{rccc} F\colon & \mathrm{Gal}(\overline{K}/K) & \longrightarrow & \mathcal{C}(\mathcal{O}) \\ & \sigma & \longmapsto & \overline{a_\sigma} \end{array}$$

which is obviously caracterized by the equality

$$F(\sigma) * E = E^\sigma.$$

Actually, we have to prove that it does not depend on the representative E of the class of elliptic curves we have chosen. We need the following lemma:

Lemma 5.14. *Let $E \in \mathcal{ELL}(\mathcal{O})$ with E defined over $\overline{\mathbb{Q}}$. Let $\mathfrak{a} \in \mathcal{C}(\mathcal{O})$ and let $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$. Then,*

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

The proof can be found in [9] (Section 2, Proposition 2.5).

Proposition 5.15. *The map F is well defined and it is an homomorphism.*

Proof. Let $E_1, E_2 \in \mathcal{ELL}(\mathcal{O})$ and let $\sigma \in \mathrm{Gal}(\overline{K}/K)$. Put $E_1^\sigma = \overline{\mathfrak{a}_1} * E_1$, $E_2^\sigma = \overline{\mathfrak{a}_2} * E_2$. We have to prove that $\overline{\mathfrak{a}_1} = \overline{\mathfrak{a}_2}$.

Since the action is simple, we have that $\overline{\mathfrak{a}_1}^{-1} * E_1^\sigma = E_1$. On the other hand, by the transitivity of the action *, we have that there exists $\overline{\mathfrak{b}} \in \mathcal{C}(\mathcal{O})$ such that $E_2 = \overline{\mathfrak{b}} * E_1$. Then,

$$(\overline{\mathfrak{b}} * E_1)^\sigma = E_2^\sigma = \overline{\mathfrak{a}_2} * E_2 = \overline{\mathfrak{a}_2} * (\overline{\mathfrak{b}} * E_1) = (\overline{\mathfrak{a}_2}\,\overline{\mathfrak{b}}\,\overline{\mathfrak{a}_1}^{-1}) * E_1^\sigma.$$

By the previous lemma, the left-hand side of the equality coincides with $\overline{\mathfrak{b}}^\sigma * E_1^\sigma$. But $\mathfrak{b}^\sigma = \mathfrak{b}$ because $\mathfrak{b} \subset K$ (because it is a fractional ideal of $\mathcal{O}$) and $\sigma \in \mathrm{Gal}(\overline{K}/K)$. Hence,

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

Now, we cancel $\overline{\mathfrak{b}}$ from both sides of the equality, obtaining that

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

Since the action is simple and

$$E_1^\sigma = 1 * E_1^\sigma,$$

we deduce that $(\overline{\mathfrak{a}_2}\,\overline{\mathfrak{a}_1}^{-1}) = 1$, and then $\overline{\mathfrak{a}_1} = \overline{\mathfrak{a}_2}$, as we wanted.

Let us prove that F is an homomorphism. Fix an elliptic curve $E \in \mathcal{ELL}(\mathcal{O})$ and let $\sigma, \tau \in \mathrm{Gal}(\overline{K}/K)$. Then,

$$F(\sigma\tau) * E = E^{\sigma\tau} = (E^\sigma)^\tau = (F(\sigma) * \tau)^\tau = F(\tau) * (F(\sigma) * E) = (F(\sigma)\,F(\tau)) * E.$$

Using again the simplicity of the action, $F(\sigma\tau) = F(\sigma)\,F(\tau)$. □

Since F is a group homomorphism, we can consider its kernel. Let $L = \overline{K}^{\mathrm{Ker}(F)}$, that is, the fixed subfield of $\overline{K}$ by $\mathrm{Ker}(F)$. Since $Ker(F)$ is a normal subgroup of $\mathrm{Gal}(\overline{K}/K)$, by the Fundamental Theorem of Galois Theory, L/K is a normal extension. This theorem also gives us that $\mathrm{Ker}(F) = \mathrm{Gal}(\overline{K}/L)$.

Proposition 5.16. *Let $E \in \mathcal{ELL}(\mathcal{O})$. Then, $L = K(j(E))$.*

Proof. We have the chain of equalities:

$$\begin{aligned}
\mathrm{Gal}(\overline{K}/L) = \mathrm{Ker}(F) &= \{\sigma \in \mathrm{Gal}(\overline{K}/K) \,|\, F(\sigma) = 1\} \\
&= \{\sigma \in \mathrm{Gal}(\overline{K}/K) \,|\, 1 * E = E\} \\
&= \{\sigma \in \mathrm{Gal}(\overline{K}/K) \,|\, E^\sigma = E\} \\
&= \{\sigma \in \mathrm{Gal}(\overline{K}/K) \,|\, j(E^\sigma) = j(E)\} \\
&= \{\sigma \in \mathrm{Gal}(\overline{K}/K) \,|\, j(E)^\sigma = j(E)\} \\
&= \mathrm{Gal}(\overline{K}/K(j(E)))
\end{aligned}$$

By the Fundamental Theorem of Galois Theory, $L = K(j(E))$. □

Proposition 5.17. *The map $F : \mathrm{Gal}(L/K) \longrightarrow \mathcal{C}(\mathcal{O})$ is injective.*

Proof. Since $\overline{K}/K$ is a normal extension, so is $\overline{K}/L$. Moreover, $\mathrm{Gal}(\overline{K}/L)$ is a normal subgroup of $\mathrm{Gal}(\overline{K}/K)$ because it is the kernel of the homomorphism F, so the extension L/K is normal. By the first isomorphism theorem,

$$\begin{array}{rccc}
\overline{F}\colon & \mathrm{Gal}(\overline{K}/K)/\mathrm{Gal}(\overline{K}/L) & \longrightarrow & \mathcal{C}(\mathcal{O}) \\
& \sigma\ \mathrm{Gal}(\overline{K}/L) & \longmapsto & F(\sigma)
\end{array}.$$

is a monomorphism. By the Fundamental Theorem of Galois Theory,

$$\begin{array}{ccc}
\mathrm{Gal}(\overline{K}/K)/\mathrm{Gal}(\overline{K}/L) & \longrightarrow & \mathrm{Gal}(L/K) \\
\sigma\ \mathrm{Gal}(\overline{K}/L) & \longmapsto & \sigma|_L
\end{array}$$

is an isomorphism. Hence, the map

$$\begin{array}{rccc}
F\colon & \mathrm{Gal}(L/K) & \longrightarrow & \mathcal{C}(\mathcal{O}) \\
& \sigma & \longmapsto & F(\tau), \tau|_L = \sigma
\end{array}$$

is injective. □

Since the group $\mathcal{C}(\mathcal{O})$ is abelian, the last two results give us what we want.

Corollary 5.18. *$L = K(j(E))$ is an abelian extension of K.*

This fullfils the first goal of this chapter: Given an imaginary quadratic field K and an order $\mathcal{O}$ in K, we have obtained an abelian extension L of K by adjoining to K the j-invariant of an elliptic curve with complex multiplication by $\mathcal{O}$.

Recall that an elliptic curve defined over $\mathbb{C}$ is defined by a lattice Λ (unique up to homothety), which is homothetic to the lattice $< 1, \alpha >$ for some $\alpha \in \mathbb{C} - \mathbb{R}$. Then, $j(E) = j(\tau)$. Thus, we have actually that

$$L = K(j(\tau))$$

is an abelian extension of K.

5 Construction of the Hilbert Class Field

Let K be an imaginary quadratic field. From now on, we will consider only the maximal order $\mathcal{O}_K$ instead of an arbitrary order $\mathcal{O}$. The main aim in this section is to prove that, in that case, the abelian extension constructed in the last section is the Hilbert Class Field of K.

We begin by introducing the group of $\mathfrak{a}$-torsion points of an elliptic curve, for $\mathfrak{a}$ an integral ideal of $\mathcal{O}_K$. This is a generalization of the group of m-torsion points of the curve, for m a non-negative integer number. All we need to generalize such group is to replace the multiplication-by-m endomorphism by other endomorphism related with $\mathfrak{a}$. What we do is to choose the image of all elements of $\mathfrak{a}$ by the normalized identification $[\cdot]$.

Definition 5.19. *Let E be an elliptic curve with complex multiplication by $\mathcal{O}_K$ and let $[\cdot]$ be the normalized identification. Let $\mathfrak{a}$ be an integral ideal of $\mathcal{O}_K$. The group of $\mathfrak{a}$-torsion points of E is*

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

We have that $\Lambda \subset \mathfrak{a}^{-1}\,\Lambda$. Using the one-to-one correspondence in 1 of Theorem 4.36, 1 is associated to the holomorphic map

$$\begin{array}{ccc} \mathbb{C}/\Lambda & \longrightarrow & \mathbb{C}/\mathfrak{a}^{-1}\,\Lambda \\ z & \longmapsto & z \end{array}.$$

Now, using the bijection in 2 of Proposition 4.36, this map induces a natural isogeny $E_\Lambda \longrightarrow \overline{\mathfrak{a}} * E_\Lambda$. This isogeny allows us to obtain information of the group of $\mathfrak{a}$-torsion points.

Proposition 5.20. *Let $E \in \mathcal{ELL}(\mathcal{O}_K)$ and let $\mathfrak{a}$ be an ideal of $\mathcal{O}_K$. Then,*

$$E[\mathfrak{a}] \cong \mathrm{Ker}(E \longrightarrow \overline{\mathfrak{a}} * E).$$

Proof. By definition,

$$E[\mathfrak{a}] = \{P \in E \,|\, [\alpha]\, P = 0\, \forall \alpha \in \mathfrak{a}\}.$$

Let Λ be a lattice such that $E = E_\Lambda$ and let $\xi : \mathbb{C}/\Lambda \longrightarrow E$ be an analytic parametrization. Then,

$$E[\mathfrak{a}] \cong \{z \in \mathbb{C}/\Lambda \,|\, \alpha\, z = 0 \text{ for all } \alpha \in \mathfrak{a}\}/\Lambda.$$

Let us consider the restriction of ξ

$$\begin{array}{ccc} \{z \in \mathbb{C}/\Lambda \,|\, \alpha\, z = 0 \text{ for all } \alpha \in \mathfrak{a}\} & \longrightarrow & E[\mathfrak{a}] \\ z & \longmapsto & \xi(z) \end{array}.$$

It is well defined: If $z \in \mathbb{C}/\Lambda$ satisfies $\alpha\, z = 0$ for all $\alpha \in \mathfrak{a}$, then $[\alpha](\xi(z)) = \xi(\alpha\, z) = 0$ for all $\alpha \in \mathfrak{a}$. Then this map is an isomorphism.

Now, it is clear that the map

$$\begin{array}{ccc} \{z \in \mathbb{C} \,|\, \alpha\, z \in \Lambda \text{ for all } \alpha \in \mathfrak{a}\} & \longrightarrow & \{z \in \mathbb{C}/\Lambda \,|\, \alpha\, z = 0 \text{ for all } \alpha \in \mathfrak{a}\} \\ z & \longmapsto & z + \Lambda \end{array}.$$

is an epimorphism with kernel Λ. By the first isomorphism theorem,

$$\{z \in \mathbb{C}/\Lambda \,|\, \alpha\, z = 0 \text{ for all } \alpha \in \mathfrak{a}\} \cong \{z \in \mathbb{C} \,|\, \alpha\, z \in \Lambda \text{ for all } \alpha \in \mathfrak{a}\}/\Lambda.$$

Observe that the condition $\alpha\, z \in \Lambda$ for all $\alpha \in \mathfrak{a}$ means that $z\,\mathfrak{a} \subset \Lambda$. Then,

$$\{z \in \mathbb{C} \,|\, \alpha\, z \in \Lambda \text{ for all } \alpha \in \mathfrak{a}\} = \{z \in \mathbb{C} \,|\, z\,\mathfrak{a} \subset \Lambda\} = \mathfrak{a}^{-1}\,\Lambda.$$

Joining the equalities and isomorphisms obtained, we have proved that

$$E[\mathfrak{a}] \cong \mathfrak{a}^{-1}\,\Lambda/\Lambda.$$

But this last quotient is just the kernel of the holomorphic map $\mathbb{C}/\Lambda \longrightarrow \mathbb{C}/\mathfrak{a}^{-1}\,\Lambda$ that sends a class $z \in \mathbb{C}/\Lambda$ to the class $z \in \mathbb{C}/\mathfrak{a}^{-1}\,\Lambda$. By using the one-to-one correspondence in 2 of Theorem 4.36, this map coincides with $E \longrightarrow \overline{\mathfrak{a}} * E$. Hence,

$$E[\mathfrak{a}] \cong \operatorname{Ker}(E \longrightarrow \overline{\mathfrak{a}} * E).$$

□

Proposition 5.21. *With the conditions of the previous proposition, $E[\mathfrak{a}]$ is a free $\mathcal{O}_K/\mathfrak{a}$-module of rank* 1.

The $\mathcal{O}_K/\mathfrak{a}$-module structure of $E[\mathfrak{a}]$ is given by the operation

$$(\alpha + \mathfrak{a})\, P = [\alpha](P).$$

We skip the proof of this result because it is quite technical and uses techniques of commutative algebra that would take us too far afield. This proof can be found in [10] (Chapter II, Corollary 1.5).

Corollary 5.22. *Let $E \in \mathcal{ELL}(\mathcal{O}_K)$.*

1. *Given an ideal $\mathfrak{a}$ of $\mathcal{O}_K$,* $\deg(E \longrightarrow \overline{\mathfrak{a}} * E) = N(\mathfrak{a})$.
2. *If $\alpha \in \mathcal{O}_K$,* $\deg([\alpha]) = |N(\alpha)|$.

Proof. 1. Since E and $\overline{\mathfrak{a}} * E$ are defined over $\mathbb{C}$, the natural isogeny $E \longrightarrow \overline{\mathfrak{a}} * E$ is separable. By Theorem 4.26,

$$\deg(E \longrightarrow \overline{\mathfrak{a}} * E) = |\operatorname{Ker}(E \longrightarrow \overline{\mathfrak{a}} * E)|.$$

Now, by Proposition 5.20, we have that $|\operatorname{Ker}(E \longrightarrow \overline{\mathfrak{a}} * E)| = |E[\mathfrak{a}]|$. Finally, by Proposition 5.21, $E[\mathfrak{a}]$ is a free $\mathcal{O}_K/\mathfrak{a}$-module of rank 1, so $E[\mathfrak{a}] \cong \mathcal{O}_K/\mathfrak{a}$. In particular, $|E[\mathfrak{a}]| = |\mathcal{O}_K/\mathfrak{a}| = N(\mathfrak{a})$. Joining the equalities obtained, we conclude that

$$\deg(E \longrightarrow \overline{\mathfrak{a}} * E) = N(\mathfrak{a}).$$

2. Let $\alpha \in \mathcal{O}_K$. Then

$$\deg([\alpha]) = |\operatorname{Ker}([\alpha])| = |E[\alpha\,\mathcal{O}_K]| = N(\alpha\,\mathcal{O}_K) = |N(\alpha)|.$$

□

To close the section, we see a result related to the field of definition of isogenies defined over fields of charasteristic 0.

Theorem 5.23. *Let E_1, E_2 be elliptic curves defined over a subfield $L \subset \mathbb{C}$. Then, there is a finite extension L' of L such that every isogeny from E_1 to E_2 is defined over L'.*

The proof can be found in [10] (Chapter II, Theorem 2.2.c).

Now, let us prove the mentioned explicit construction of the Hilbert Class Field.

Theorem 5.24. *Let E be an elliptic curve with complex multiplication by $\mathcal{O}_K$. Then, the Hilbert Class Field of K is*

$$H = K(j(E)).$$

Proof. Let $L = K(j(E))$. We proved that L is an abelian extension of K by using the group homomorphism

$$F \,:\, \mathrm{Gal}(\overline{K}/K) \longrightarrow \mathcal{C}(\mathcal{O}_K).$$

Let $\mathfrak{f}$ be the conductor of the abelian extension L/K. Recall that $\mathcal{C}(\mathcal{O}_K) \cong I_K/P_K$.

We claim that

$$F\left(\left(\frac{L/K}{\mathfrak{a}}\right)\right) = \overline{\mathfrak{a}} \text{ for all } \mathfrak{a} \in I_K(\mathfrak{f}), \tag{5.3}$$

where $\overline{\mathfrak{a}}$ denotes the class of $\mathfrak{a}$ in I_K/P_K.

Eventually, we will prove that L is the Hilbert Class Field of K. Then, Artin Reciprocity Theorem gives us that $\left(\frac{L/K}{\mathfrak{a}}\right)$ runs through $\mathrm{Gal}(L/K)$ as $\mathfrak{a}$ runs through $\mathcal{C}(\mathcal{O}_K)$. Hence, if we complete the proof, automatically we will obtain that the claim (5.3) determines completely F.

We will first prove that the equality (5.3) holds for a special class of finite primes of K. What we will do is to establish a set S of *bad* rational primes (see conditions 1, 2 and 3 bellow) and to choose the finite primes P of K for which the rational prime under P does not lie in S.

We proved that $\mathcal{ELL}(\mathcal{O}_K)$ is finite and all its classes have some representative which is defined over $\mathbb{Q}$. Then, there are representatives $E_1, ..., E_n$ defined over $\overline{\mathbb{Q}}$ for the distinct $\overline{\mathbb{Q}}$-isomorphism classes in $\mathcal{ELL}(\mathcal{O}_K)$. We can also assume that every isogeny from E_i to E_j with $i \neq j$ is defined over L. Otherwise, we replace L by a finite extension L' given by Theorem 5.23. This is not a problem because the restriction of the Artin symbol of L'/K over a finite prime P of K to L is the Artin symbol of L/K over P. Let S be the set of prime numbers that satisfy any of the following three conditions:

1. p ramifies in L.
2. There is $i \in \{1, ..., n\}$ such that E_i has bad reduction at some prime L over p.
3. p divides either the numerator or the denominator of any one of the numbers

$$N_{\mathbb{Q}}^{L}(j(E_i) - j(E_k)),\ i \neq k.$$

The third condition means that if p is a prime number and Q is a prime in L over p, then, for $i \neq k$, $j(E_i) \not\equiv j(E_k) \pmod{Q}$, so $\widetilde{E_i} \ncong \widetilde{E_k}$.

In the sequel, S will denote the set of rational primes we have just defined. Now, we need another technical lemma.

Lemma 5.25. *Let $E \in \mathcal{ELL}(\mathcal{O}_K)$ be an elliptic curve defined over a subfield L of $\mathbb{C}$. Given a finite prime P of K over a rational prime $p \notin S$ that splits completely at K, the natural isogeny*

$$\phi : E \longrightarrow \overline{P} * E$$

has degree p and its reduction

$$\widetilde{\phi} : \widetilde{E} \longrightarrow \widetilde{\overline{P} * E}$$

modulo a prime Q of L over P is inseparable of degree p.

Proof. Fix a finite prime P of K over $p \notin S$. Since p splits completely at K, P is a degree 1 prime. Let Q be a prime in L which lies over P. Let $\mathfrak{a}$ be an ideal of $\mathcal{O}_K$ such that $\mathfrak{a}\, P =< \alpha >$, $\alpha \in \mathcal{O}_K$.

Let Λ be a lattice in $\mathbb{C}$ such that $E = E_\Lambda$. Since $P\,\Lambda \subset \Lambda$, we have that $\Lambda \subset P^{-1}\,\Lambda$. Now, using part 1 of Theorem 4.36, there is a holomorphic map associated to 1

$$\begin{array}{ccc} \mathbb{C}/\Lambda & \longrightarrow & \mathbb{C}/P^{-1}\,\Lambda \\ z+\Lambda & \longmapsto & z+P^{-1}\,\Lambda \end{array}$$

Using part 2 of 4.36, this map is associated to an isogeny $\phi : E \longrightarrow \overline{P} * E$.

Similarly, using these two results with the inclusion $P^{-1}\,\Lambda \subset \mathfrak{a}^{-1}\,P^{-1}\,\Lambda$, we obtain an holomorphic map

$$\begin{array}{ccc} \mathbb{C}/P^{-1}\,\Lambda & \longrightarrow & \mathbb{C}/\mathfrak{a}^{-1}\,P^{-1}\,\Lambda \\ z+P^{-1}\,\Lambda & \longmapsto & z+\mathfrak{a}^{-1}\,P^{-1}\,\Lambda \end{array} ,$$

and this map is associated to an isogeny $\psi : \overline{P} * E \longrightarrow \overline{\mathfrak{a}} * \overline{P} * E$.

Now, recall that $\mathfrak{a}\,P =< \alpha >$, so $\mathfrak{a}^{-1}\,P^{-1} =< \alpha^{-1} >$. Using parts 1 and 2 of Theorem 4.36 with the inclusion $\alpha\ < \alpha^{-1} >\ \Lambda \subset \Lambda$, we obtain an holomorphic map

$$\begin{array}{ccc} \mathbb{C}/\mathfrak{a}^{-1}\,P^{-1}\,\Lambda & \longrightarrow & \mathbb{C}/\Lambda \\ z+\mathfrak{a}^{-1}\,P^{-1}\,\Lambda\,\Lambda & \longmapsto & \alpha\,z+\Lambda \end{array} ,$$

We obtain the commutative diagram

$$\begin{array}{ccccccc} \mathbb{C}/\Lambda & \longrightarrow & \mathbb{C}/P^{-1}\,\Lambda & \longrightarrow & \mathbb{C}/\mathfrak{a}^{-1}\,P^{-1}\,\Lambda & \longrightarrow & \mathbb{C}/\Lambda \\ \downarrow & & \downarrow & & \downarrow & & \downarrow \\ E & \xrightarrow{\phi} & \overline{P} * E & \xrightarrow{\psi} & \overline{\mathfrak{a}} * \overline{P} * E & \xrightarrow{\lambda} & E \end{array}$$

Let us take a Weierstrass equation for E/L that is minimal over Q (see [9], Chapter VII, Section 1). Let $\omega = \frac{dx}{2\,y+a_1\,x+a_2}$ be the associated invariant differential on E. If we consider on E the normalized identification, by Proposition 5.5 and its corollary, since the composition of the pull-backs of top maps is $z \mapsto \alpha\,z$, the composition of the pull-backs of botton maps satisfies

$$(\lambda \circ \phi \circ \psi)^*(\omega) = \alpha\,\omega.$$

Since the equation of E/L is minimal over Q, we can reduce the coefficients of the equation modulo Q to obtain an equation for the reduction $\widetilde{E}$ of E modulo Q (see [9], Chapter VII, Section 2), and

$$\widetilde{\omega} = \frac{dx}{\widetilde{2}\,y+\widetilde{a_1}\,x+\widetilde{a_3}}$$

is also a non-zero invariant differential on $\widetilde{E}$. Since $<\alpha>=\mathfrak{a}\,P$ and P lies under Q,

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

Then $(\widetilde{\lambda}\circ\widetilde{\psi}\circ\widetilde{\phi})^*$ is not injective. By Proposition 5.2, the map $\lambda\circ\phi\circ\psi$ is inseparable. Using the Proposition 4.56 and Corollary 5.22, we obtain that

$$\deg(\widetilde{\phi})=\deg(\phi)=N^K(P)=p,$$

$$\deg(\widetilde{\psi})=\deg(\psi)=N^K(\mathfrak{a}),$$

$$\deg(\widetilde{\lambda})=\deg(\lambda)=1,$$

where the last equality is due to

$$\deg(\lambda)=|\mathrm{Ker}(\lambda)|=|E[\mathfrak{a}\,P]|=|E[<\alpha>]|=1.$$

Since $\mathfrak{a}$ is coprime with p, $N^K(\mathfrak{a})$ is coprime with p. Then, $\widetilde{\psi}$ is non-zero, so it is injective. Hence, $\widetilde{\psi}$ is separable. Furthermore, the equality $\deg(\widetilde{\lambda})=1$ says that $\widetilde{\lambda}$ is separable. Necessarily,

$$\widetilde{\phi}\,:\,\widetilde{E}\longrightarrow\widetilde{\overline{P}*E}$$

is inseparable.

Now, by Proposition 4.27, there is a separable map $\varphi\,:\,\widetilde{E}^{(p)}\longrightarrow\widetilde{\overline{P}*E}$ such that $\widetilde{\phi}=\varphi\circ\mathrm{Frob}_p$. Since $\widetilde{\phi}$ is inseparable, $\deg(\widetilde{\phi})=\deg_i(\widetilde{\phi})$. But

$$p=\deg(\widetilde{\phi})=\deg_i(\widetilde{\phi})\,\deg_s(\widetilde{\phi})=p\,\deg(\varphi),$$

so $\deg(\varphi)=1$. This says that $\mathrm{Ker}(\phi)$ has a single element. Since φ is separable, it is non-constant. Then, φ is an isomorphism.

Since Frob_p is purely inseparable of degree p and φ is an isomorphism, we obtain that $\widetilde{\phi}$ is purely inseparable of degree p. □

After this, to determine $F\left(\left(\frac{L/K}{P}\right)\right)$ for P finite prime of K over $p\notin S$ is nothing but a corollary.

Corollary 5.26. *If $p\notin S$ splits completely at K and P is a finite prime of K over p, then $F\left(\left(\frac{L/K}{P}\right)\right)=\overline{P}$.*

Proof. Let P be such a prime and let $\phi\,:\,E\longrightarrow\overline{P}*E$ be the natural isogeny. First of all, note that the Artin symbol $\left(\frac{L/K}{P}\right)$ is defined in this case because p splits completely in K and then it is unramified. Moreover, we know by the previous lemma that its reduction $\widetilde{\phi}\,:\,\widetilde{E}\longrightarrow\widetilde{\overline{P}*E}$ is inseparable and has degree p. Looking at the proof of the previous lemma, we know that $\widetilde{E}^{(p)}\cong\widetilde{\overline{P}*E}$. Let us call $\sigma_P=\left(\frac{L/K}{P}\right)$. From this, we deduce that

$$j(\overline{P}*E)\cong j(E)^p=j(E)^{N(P)}=j(E)^{\sigma_P}=j(E^{\sigma_P})=j(F(\sigma_P)*E).$$

Since $p \notin S$, the third condition (for primes in S) implies that $\overline{P} * E \cong F\left(\left(\frac{L/K}{P}\right)\right) * E$. Now, we use that the action $*$ is simple, obtaining that

$$F\left(\left(\frac{L/K}{P}\right)\right) = \overline{P}.$$

□

Now, we are ready to prove the claim (5.3). Let $\mathfrak{a} \in I_K(\mathfrak{f})$ and let S be the set of prime numbers of the previous proof. By Dirichlet Theorem 3.30, there are infinitely many degree 1 primes in the same class as $\mathfrak{a}$. But we know also that S is a finite set, because it is contained in the set of ramified number primes in K, which is finite (see [4], Theorem 34). Then there is a degree 1 prime P with $\overline{P} = \overline{\mathfrak{a}}$ such that the prime number p under P is not in S. Since the conductor $\mathfrak{f}$ is divisible by all primes of K that ramify in L, the Artin map of L/K for $\mathfrak{f}$ induces an isomorphism, and then the previous equality implies that $\left(\frac{L/K}{P}\right) = \left(\frac{L/K}{\mathfrak{a}}\right)$.

On the other hand, p does not ramify in L because $p \notin S$. Since the ramification index is multiplicative by towers (see [4], Chapter 3, Exercise 10), it follows that p does not ramify neither in K. Moreover, P is a degree 1 prime, so it holds that p splits completely at K. Thus, we can apply Corollary 5.26, obtaining that

$$F\left(\left(\frac{L/K}{\mathfrak{a}}\right)\right) = F\left(\left(\frac{L/K}{P}\right)\right) = \overline{P} = \overline{\mathfrak{a}}.$$

This proves the claim.

Let $< \alpha > \in I_K(\mathfrak{f})$ be a principal ideal (non-necessarily such that $\alpha \equiv 1 \pmod{\mathfrak{f}}$). Then, the claim 5.3 in this case becomes

$$F\left(\left(\frac{L/K}{< \alpha >}\right)\right) = 1.$$

But $F : \mathrm{Gal}(L/K) \longrightarrow \mathcal{C}(\mathcal{O}_K)$ is injective, so

$$\left(\frac{L/K}{< \alpha >}\right) = 1 \text{ for all } < \alpha > \in I_K(\mathfrak{f}). \tag{5.4}$$

Using this equality, we can prove that $L \subset H$. With the notation used in Chapter 3, Corollary 3.9 gives us that $P_K = S_{H/K}$. Now, let $P \in P_K$. If $P \in I_K(\mathfrak{f})$, by the equaility (5.4), $\left(\frac{L/K}{P}\right) = 1$, and by Proposition 1.8, $P \in S_{L/K}$. Otherwise, we have that P and $\mathfrak{f}$ are not coprime, so P divides $\mathfrak{f}$. By definition of conductor, this says that P is ramified in L. Thus, we have proved that

$$S_{H/K} \subset S_{L/K} \cup \{P \in \mathcal{P}_K \mid P \text{ is ramified in } L\}.$$

But the set of primes of K that ramify in L is finite (see [4], Corollary 3 of Page 73). Hence, $S_{H/K} \dot{\subset} S_{L/K}$. By Theorem 3.31, we have that $L \subset H$.

Moreover, the map

$$\begin{array}{ccc} I_K(\mathfrak{f}) & \longrightarrow & \mathcal{C}(\mathcal{O}_K) \\ \mathfrak{a} & \longmapsto & \overline{\mathfrak{a}} \end{array}$$

is surjective. Indeed, if $\overline{\mathfrak{a}} \in I_K/P_K$, we obtain by Corollary 3.29 with $\mathfrak{m} = \mathfrak{f}$ (which is divisible by all primes of K that ramify in L) and $\sigma = \left(\frac{L/K}{\mathfrak{a}}\right)$ that there exists $P \in \mathcal{P}_K$ such that P does not divide $\mathfrak{f}$ and $\left(\frac{L/K}{P}\right) = \left(\frac{L/K}{\mathfrak{a}}\right)$. By Artin Reciprocity Theorem 3.14, this last equality imply that $\overline{P} = \overline{\mathfrak{a}}$. Since P is a prime and does not divide $\mathfrak{f}$, this means that P is coprime to $\mathfrak{f}$. Hence $P \in I_K(\mathfrak{f})$ and the image of P by the natural map is $\overline{P} = \overline{\mathfrak{a}}$.

Then, given $\overline{\mathfrak{a}} \in \mathcal{C}(\mathcal{O}_K)$, we can choose a representative $\mathfrak{a} \in I_K(\mathfrak{f})$. By the claim 5.3, $F\left(\left(\frac{L/K}{\mathfrak{a}}\right)\right) = \overline{\mathfrak{a}}$, which proves that F is surjective.

We have obtained that F is bijective. Then, $\mathrm{Gal}(L/K) \cong \mathcal{C}(\mathcal{O}_K)$. Using this isomorphism and the isomorphism $\mathcal{C}(\mathcal{O}_K) \cong \mathrm{Gal}(H/K)$ given by Theorem 3.7,

$$[L : K] = |\,\mathrm{Gal}(L/K)| = |\mathcal{C}(\mathcal{O}_K)| = |\,\mathrm{Gal}(H/K)| = [H : K].$$

Since $L \subset H$, this equality says that $L = H$, which finishes the proof. □

To close the chapter, we state the result that identifies the abelian extension obtained $K(j(E))$ when E is an elliptic curve with complex multiplication by any order $\mathcal{O}$.

Theorem 5.27. *Let K be an imaginary quadratic field and let $\mathcal{O}$ be an order of K with conductor f. Let E be an elliptic curve with complex multiplication by $\mathcal{O}$. Then, the Ring Class Field of conductor f of $\mathcal{O}$ is*

$$L = K(j(E)).$$

The proof can be found in [7]. We will not give it in this thesis because we will not need this result in the next chapter, in which we will finish the proof of the *Kronecker's Jugendtraum* for the imaginary-quadratic case. The importance of this result is that it allows us to identify the abelian extension that we obtain when we adjoin to an imaginary quadratic field the j-invariant of an elliptic curve E.

As in the case of the Hilbert Class Field, we can rewrite the equality obtained as $L = K(j(\tau))$ where $\tau \in \mathbb{C} - \mathbb{R}$. We can observe again the analogy with the cyclotomic case.

Chapter 6

The maximal abelian extension

Let K be an imaginary quadratic field. The main aim in this chapter is to give an explicit construction of K^{ab}, that is, to solve the *Kronecker's Jugendtraum* in the imaginary-quadratic case. We will prove that, essentially, we have

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

where E is an elliptic curve defined over the Hilbert Class Field H of K and with complex multiplication by $\mathcal{O}_K$ (in the cases $K = \mathbb{Q}(\sqrt{-1})$ and $K = \mathbb{Q}(\sqrt{-3})$ the expression is a bit different). For a given non-zero point $P \in E$, $x(P)$ denotes the first coordinate of P.

Eventually, we will prove that K^{ab} is the compositum of all Ray Class Fields of K. This is an important reduction in our problem: we have nothing to compute but, for each modulus $\mathfrak{m}$ of K, the Ray Class Field of K for $\mathfrak{m}$ and then compute the compositum of all of them.

For computing the Ray Class Field of K for each modulus, we will need the main result of the previous chapter: the Hilbert Class Field of K (i.e, the maximal abelian unramified extension of K) is $K(j(E))$, where E is any elliptic curve with complex multiplication by $\mathcal{O}_K$. Recall that the Hilbert Class Field of K is the Ray Class Field of conductor $< 1 >$. Thus, the Ray Class Field for a given modulus contains the Hilbert Class Field of K. This suggests that in order to obtain the Ray Class Field of K for $\mathfrak{m}$ we have to adjoin to $K(j(E))$ more elements. Indeed, we will prove that

$$K_{\mathfrak{m}} = K(j(E), h(E[\mathfrak{m}])),$$

where h is what we call a Weber function for E (see Definition 6.8). When $j(E) \neq 0, 1728$, this function is essentially the first-coordinate function.

The main reference used in this chapter is [10].

1 The cyclotomic case

Before proving the mentioned result, we will illustrate our theory with the well known cyclotomic case. We are going to construct the Ray Class Field of any conductor of $\mathbb{Q}$ and use this result to prove the Kronecker-Weber theorem.

Since we are going to use Class Field Theory in the case of $\mathbb{Q}$ we will deal with primes of $\mathbb{Q}$. The finite ones are the prime ideals of $\mathbb{Z}$ (which is the ring of integers of $\mathbb{Q}$). Those

ideals are of the form $p\mathbb{Z}$ with p a rational prime. To ease notation, we will consider the rational prime p instead of $p\mathbb{Z}$. On the other hand, the unique infinite prime of $\mathbb{Q}$ is the inclusion $\mathbb{Q} \hookrightarrow \mathbb{C}$, which is a real infinite prime.

Set $N \in \mathbb{Z}_{>0}$. Using the previous identification, we can consider N as a modulus of $\mathbb{Q}$. Let $\omega = e^{\frac{2\pi i}{N}}$ and consider the N-th cyclotomic field $\mathbb{Q}(\omega)$. Then, $\mathbb{Q}(\omega)/\mathbb{Q}$ is an abelian extension. Indeed, we have the isomorphism

$$\begin{array}{ccc} (\mathbb{Z}/N\mathbb{Z})^* & \longrightarrow & \mathrm{Gal}(\mathbb{Q}(\omega)/\mathbb{Q}) \\ k + N\mathbb{Z} & \longmapsto & \omega \mapsto \omega^k \end{array} .$$

Theorem 6.1. *$\mathbb{Q}(\omega)$ is the Ray Class Field of $\mathbb{Q}$ for N.*

Proof. For a given rational prime p unramified in $\mathbb{Q}(\omega)$, let us denote $\sigma_p = \left(\frac{\mathbb{Q}(\omega)/\mathbb{Q}}{p}\right)$. It is enough to prove that

$$\sigma_p = 1 \Longleftrightarrow p \equiv 1 \,(\mathrm{mod}\, N) \tag{6.1}$$

for all rational primes p that are unramified in $\mathbb{Q}(\omega)$.

If we prove this, for all unramified rational primes p we have the following:

$$\begin{aligned} p \text{ splits completely in } \mathbb{Q}(\omega) &\Longleftrightarrow \sigma_p = \left(\frac{\mathbb{Q}(\omega)/\mathbb{Q}}{p}\right) = 1 \\ &\Longleftrightarrow p \equiv 1 \,(\mathrm{mod}\, N) \\ &\Longleftrightarrow p \in P_{\mathbb{Q},1}(N) \\ &\Longleftrightarrow \left(\frac{\mathbb{Q}_N/\mathbb{Q}}{p}\right) = 1 \\ &\Longleftrightarrow p \text{ splits completely in } \mathbb{Q}_N. \end{aligned}$$

Since there are finitely many ramified primes of $\mathbb{Q}$ (see [4], Corollary 2 of Theorem 24), the equivalence (6.1) holds for all but finitely many rational primes. With the notation of Chapter 3, this proves that $S_{\mathbb{Q}(\omega)/\mathbb{Q}} \doteq S_{\mathbb{Q}_N/\mathbb{Q}}$. By Part 2 of Theorem 3.31, this equality implies that $\mathbb{Q}(\omega) = \mathbb{Q}_N$, as we wanted.

Let us prove the equivalence (6.1). Let p be a rational prime unramified in $\mathbb{Q}(\omega)$. For proving the previous equivalence, we will determine the action of σ_p over a primitive N-th root of the unity ξ. By definition of σ_p, if P is a prime of $\mathbb{Q}(\omega)$ over p, we have that

$$\xi^{\sigma_p} \equiv \xi^{N(p)} \,(\mathrm{mod}\, P).$$

But $N(p)$ is nothing but the order of the additive group $\mathbb{Z}/p\mathbb{Z}$, which is p. Then,

$$\xi^{\sigma_p} \equiv \xi^{p} \,(\mathrm{mod}\, P).$$

Let us consider the polynomial $f(X) = X^N - 1 \in \mathbb{Q}(\omega)[X]$. Then, the set of roots of f is $\{1, \omega, ..., \omega^{N-1}\}$ (the N-th roots of unity). But all of them are algebraic integers, so $f \in \mathbb{Z}[\omega][X]$. Now, we consider the polynomial $\overline{f} \in (\mathbb{Z}[\omega]/P)[X]$ obtained by reducing the coefficients of f modulo P. If $\overline{f}$ is not separable, then it has some multiple root, so its formal derivative

$$\overline{f}'(X) = \overline{N}\, X^{N-1} \in (\mathbb{Z}[\omega]/P)[X]$$

has some non-zero root. But $\gcd(p, N) = 1$, so $\overline{N} \neq 0$ and then the unique root of $\overline{f}$ is 0, which is a contradiction. This says that $\overline{f}$ is separable.

Since $\overline{f}$ is separable, $1, \xi, ..., \xi^{N-1}$ are distinct modulo P. Hence, the previous congruence is actualy an equality, that is,

$$\xi^{\sigma_p} = \xi^p.$$

Then,

$$\sigma_p = 1 \iff \xi^p = \xi \iff p \equiv 1 \,(\mathrm{mod}\, N).$$

The uniqueness of Existence Theorem gives us that $\mathbb{Q}_N = \mathbb{Q}(\omega)$. □

Note that in that case the multiplicative group $\mathbb{C}^*$ plays the role of the elliptic curve $E \in \mathcal{ELL}(\mathcal{O}_K)$ in the imaginary-quadratic case in the following sense: In order to generate abelian extensions of K, we adjoin to $K(j(E))$ some coordinates of the torsion points of E. In that case, in order to generate abelian extensions of $\mathbb{Q}$, we adjoin to $\mathbb{Q}$ the roots of unity, that are the torsion points of $\mathbb{C}^*$. This parallelism is far from being exact: if we adjoin to $K(j(E))$ both first and second coordinates of torsion points of E, in general we do not obtain an abelian extension of K. This situation will be discussed in the next section.

Now, the Kronecker-Weber Theorem is an easy consequence of this result.

Corollary 6.2 (Kronecker-Weber Theorem)**.** *Let L be an abelian extension of $\mathbb{Q}$. Then, there is some $N \in \mathbb{Z}_{\geq 0}$ such that $L \subset \mathbb{Q}(\omega)$, where $\omega = e^{\frac{2\pi i}{N}}$.*

Proof. Let N be the conductor of $L/\mathbb{Q}$. By the previous theorem, the Ray Class Field of $\mathbb{Q}$ for N is $\mathbb{Q}_N = \mathbb{Q}(\omega)$. By definition of Ray Class Field, this means that

$$P_{\mathbb{Q},1}(N) = \mathrm{Ker}(\Phi_{\mathbb{Q}(\omega)/\mathbb{Q},N}).$$

By definition of conductor, N is divisible by all primes of $\mathbb{Q}$ that ramify in L. By Artin Reciprocity Theorem, $\mathrm{Ker}(\Phi_{L/\mathbb{Q},N})$ is a congruence subgroup for N. Then,

$$P_{\mathbb{Q},1}(N) = \mathrm{Ker}(\Phi_{\mathbb{Q}(\omega)/\mathbb{Q},N}) \subset \mathrm{Ker}(\Phi_{L/\mathbb{Q},N}).$$

Finally, by Corollary 3.22, we obtain that $L \subset \mathbb{Q}(\omega)$. □

2 Abelian extensions of the Hilbert Class Field

Let K be an imaginary quadratic field. We know that the Ray Class Field of $\mathbb{Q}$ for $N \geq 0$ is obtained by adjoining to $\mathbb{Q}$ the N-torsion points of $\mathbb{C}^*$ (that is, the primitive N-th roots of the unity in $\mathbb{C}$). As a first approximation to the problem of constructing the maximal abelian extension of K, we would try to adjoin to $K(j(E))$ all coordinates of torsion points of E. This will not work in general: the field $K(j(E), E_{\mathrm{tors}})$ is not in general an abelian extension of K. What we are going to prove is that it is an abelian extension of the Hilbert Class Field $H = K(j(E))$. We need the following technical lemma.

Lemma 6.3. *Let M be an imaginary quadratic field and let L be subfield of $\mathbb{C}$. Let E be an elliptic curve defined over L and with complex multiplication by $\mathcal{O}_M$. Then, every endomorphism of E is defined over $L\,M$.*

Proof. Let $\sigma \in \mathrm{Aut}(\mathbb{C})$ be an automorphism that fixes L. Since E is defined over L, we have that $E^\sigma = E$. Let $\alpha \in \mathcal{O}_M$. By Proposition 5.8,

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

Let $\sigma \in \mathrm{Aut}(\mathbb{C})$ that fixes $L\,M$. Then $\alpha^\sigma = \alpha$ for all $\alpha \in \mathcal{O}_M$, so the previous equality becomes

$$[\alpha]_E^\sigma = [\alpha]_E \text{ for all } \alpha \in \mathcal{O}_M.$$

Let $\phi \in \mathrm{End}(E)$. Then, there is an unique $\alpha \in \mathcal{O}_M$ such that $\phi = [\alpha]_E$. Then, $\phi^\sigma = \phi$. This proves that ϕ is defined over $L\,M$. □

Now, we are ready to prove the mentioned result.

Theorem 6.4. *Let K be an imaginary quadratic field and let $E \in \mathcal{ELL}(\mathcal{O}_K)$. Then, $L = K(j(E), E_{\mathrm{tors}})$ is an abelian extension of the Hilbert Class Field $H = K(j(E))$, where E_{tors} denotes the set of all coordinates of the torsion points of E.*

Proof. Let m be a non-negative integer and let $L_m = K(j(E), E[m])$. It is enough to prove that L_m is an abelian extension of K, because L is the compositum of all L_m for $m \in \mathbb{Z}_{\geq 0}$.

Let $\sigma \in \mathrm{Gal}(\overline{K}/H)$ and $T \in E[\mathfrak{m}]$. By definition, $[m](T) = \infty$. Then, $[m](T^\sigma) = ([m](T))^\sigma = \infty$, so $T^\sigma \in E[m]$. Since σ is bijective, it follows that the map $T \mapsto T^\sigma$ is an automorphism of $E[m]$. Thus, there is a representation

$$\begin{array}{rccc} \rho: & \mathrm{Gal}(\overline{K}/K) & \longrightarrow & \mathrm{Aut}(E[m]) \\ & \sigma & \longmapsto & T \mapsto T^\sigma \end{array}.$$

The group $E[m]$ of m-torsion points has structure of $\mathcal{O}_K/m\,\mathcal{O}_K$-module with the external product

$$(\alpha + m\,\mathcal{O}_K)\,T = [\alpha](T) \text{ for all } \alpha + m\,\mathcal{O}_K \in \mathcal{O}_K/m\,\mathcal{O}_K,\ T \in E[m].$$

Note that for each $\alpha + m\,\mathcal{O}_K \in \mathcal{O}_K/m\,\mathcal{O}_K$ and $T \in E[m]$, $[\alpha](T)$ is also a m-torsion point because $[m] \circ [\alpha](T) = [m\,\alpha](T) = [\alpha] \circ [m](T) = \infty$. This proves that the previous external product is well defined.

Now, we claim that $\mathrm{Im}(\rho) \subset \mathrm{Aut}(E[m])$ is a $\mathcal{O}_K/m\,\mathcal{O}_K$-module. Since E is defined over H and has complex multiplication by $\mathcal{O}_K$, the previous lemma gives us that every endomorphism of E is defined over $K\,H = H$. Hence,

$$([\alpha](T))^\sigma = [\alpha]^\sigma(T^\sigma) = [\alpha](T^\sigma) \text{ for all } \sigma \in \mathrm{Gal}(L_m/H),\ T \in E[m] \text{ and } \alpha \in \mathcal{O}_K. \quad (6.2)$$

Given $\rho(\sigma) \in \mathrm{Im}(\rho)$ and $\alpha + m\,\mathcal{O}_K \in \mathcal{O}_K/m\,\mathcal{O}_K$,

$$\rho(\sigma)((\alpha + m\,\mathcal{O}_K)\,T) = \rho(\sigma)([\alpha](T)) = ([\alpha](T))^\sigma = [\alpha](T^\sigma) = [\alpha](\rho(\sigma)(T)),$$

which proves that the automorphism $\rho(\sigma)$ is $\mathcal{O}_K/m\,\mathcal{O}_K$-linear. Thus, the claim follows.

Now, let us compute $\mathrm{Ker}(\rho)$. Given $\sigma \in \mathrm{Gal}(\overline{K}/H)$, $\rho(\sigma)$ is the identity if and only if σ fixes all points of $E[m]$, which is the same as σ fixing all the coordinates of points

of $E[m]$. Then, σ lies in the kernel of ρ if and only if it also fixes $E[m]$, that is, it fixes $H(E[m]) = K(j(E), E[m]) = L_m$. This proves that $\mathrm{Ker}(\rho) = \mathrm{Gal}(L_m/H)$.

The Fundamental Theorem of Galois Theory gives us that

$$\mathrm{Gal}(\overline{K}/H)/\,\mathrm{Gal}(\overline{K}/L_m) \cong \mathrm{Gal}(L_m/H).$$

By using the First Isomorphism Theorem, we have that ρ induces a monomorphism

$$\phi : \mathrm{Gal}(L_m/H) \longrightarrow \mathrm{Aut}_{\mathcal{O}_K/m\,\mathcal{O}_K}(E[m]).$$

Now, by Proposition 5.21, $E[m]$ is a free $\mathcal{O}_K/m\,\mathcal{O}_K$-module of rank 1. Then

$$\mathrm{Aut}_{\mathcal{O}_K/m\,\mathcal{O}_K}(E[m]) \cong (\mathcal{O}_K/m\,\mathcal{O}_K)*,$$

which proves that $\mathrm{Gal}(L_m/H)$ is abelian. Hence, L_m/H is an abelian extension. □

We note here the analogy with the cyclotomic case: In order to obtain abelian extensions of $K(j(E))$, what we do is to adjoin the coordinates of the torsion points of E. The previous proof says also that we obtain an abelian extension of $K(j(E))$ by adjoining to it the m-torsion points of E for fixed m. In the cyclotomic case, we replace the elliptic curve E by the multiplicative group $\mathbb{C}^*$ and the torsion points of E by the roots of unity. We obtain an abelian extension of $\mathbb{Q}$ by adjoining the m-th roots of unity for fixed m (in that case it is enough to adjoin any of these roots because all of them are conjugate and generate the same extension).

3 Construction of the maximal abelian extension

Let K be an imaginary quadratic field. We proved that the field $K(j(E), E_{\mathrm{tors}})$ is an abelian extension of $K(j(E))$ but in general it is not an abelian extension of K. To construct the maximal abelian extension of K, we may give additional restrictions to that field. What we will do essentially is to restrict the set of coordinates of rational points that we consider.

3.1 Lifting isogenies

Let E be an elliptic curve with complex multiplication by $\mathcal{O}_K$. We know that $H = K(j(E))$ is the Hilbert Class Field of K. In particular, $j(E) \in H$. By Proposition 4.7, we can assume that E is defined over H.

Let P be a finite prime of K and let Q be a prime of H that lies over P and such that E has good reduction at Q. Let p be the rational prime under P. We begin with an important result which says that we can lift the p-th Frobenius map $\mathrm{Frob}_p : \widetilde{E} \longrightarrow \widetilde{E}^{(p)}$ in charasteristic p to an isogeny $\lambda : E \longrightarrow E^{\sigma_P}$ in charasteristic 0. Before proving this, we need the following lemma.

Lemma 6.5. *Let $E \in \mathcal{ELL}(\mathcal{O}_K)$ defined over a number field L. Let Q be a prime of L such that E has good reduction over Q and let us consider the restriction morphism*

$$\begin{array}{rccc} \theta : & \mathrm{End}(E) & \longrightarrow & \mathrm{End}(\widetilde{E}) \\ & \phi & \longmapsto & \widetilde{\phi} \end{array}.$$

Then, the centralizer $C_{\mathrm{End}(\widetilde{E})}(Im(\theta))$ of $Im(\theta)$ inside $\mathrm{End}(\widetilde{E})$ coincides with $\mathrm{Im}(\theta)$.

Proof. Since E has complex multiplication by $\mathcal{O}_K$, we have that $\mathrm{End}(E) \cong \mathcal{O}_K$. By Proposition 4.56, θ is injective, so $\mathrm{Im}(\theta) \cong \mathcal{O}_K$. In particular, $\mathrm{Im}(\theta)$ is a commutative ring. This means that $\mathrm{Im}(\theta) \subset C_{\mathrm{End}(\widetilde{E})}(Im(\theta))$.

We have that the reduction $\widetilde{E}$ is defined over a finite field. By Theorem 4.53, $\mathrm{End}(\widetilde{E})$ is either an order in an imaginary quadratic field or an order in a quaternion algebra.

In the first case, we have that

$$\mathrm{Im}(\theta) \subset \mathrm{End}(\widetilde{E}) \cong \mathcal{O} \subset \mathcal{O}_K \cong \mathrm{End}(E) \cong \mathrm{Im}(\theta).$$

We conclude that $\mathrm{Im}(\theta) = \mathrm{End}(\widetilde{E})$. Since we have also that

$$\mathrm{Im}(\theta) \subset C_{\mathrm{End}(\widetilde{E})}(Im(\theta)) \subset \mathrm{End}(\widetilde{E}),$$

necessarily $\mathrm{Im}(\theta) = C_{\mathrm{End}(\widetilde{E^{\sigma_P}})}(Im(\theta))$.

Let us assume that $\mathrm{End}(\widetilde{E})$ is an order in a quaternion algebra $\mathcal{H}$. Since the reduction behaves well with the sum and the product, θ is a monomorphism of rings. Hence, it is a monomorphism between the additive groups. Now, the isomorphism $\mathrm{End}(E) \cong \mathcal{O}_K$ gives us that $\mathrm{End}(E)$ is a $\mathbb{Z}$-module of rank 2. Since θ is a monomorphism of groups, $\mathrm{Im}(\theta)$ is a $\mathbb{Z}$-module of rank 2. Then $\mathcal{K} := \mathrm{Im}(\theta) \otimes \mathbb{Q}$ is isomorphic to a quadratic subfield of $\mathcal{H}$. Let $\{1, \alpha\}$ be a $\mathbb{Q}$-basis of $\mathcal{K}$ with $\alpha^2 \in \mathbb{Q}$. Then, there exists $\beta \in \mathcal{H}$ such that $\beta^2, (\alpha\,\beta)^2 \in \mathbb{Q}$, $\alpha\,\beta = -\beta\,\alpha$ and $\{1, \alpha, \beta, \alpha\,\beta\}$ is a $\mathbb{Q}$-basis of $\mathcal{H}$ (see [9], Chapter III, proof of Theorem 9.3).

We are going to compute the commutator of $\mathcal{K}$ in order to compute that of $\mathrm{Im}(\theta)$. Let $\gamma \in \mathcal{H}$. Then, there exist $a, b, c, d \in \mathbb{Q}$ such that $\gamma = a + b\,\alpha + c\,\beta + d\,\alpha\,\beta$. Hence,

$$\begin{aligned}
\gamma \in C_{\mathcal{H}}(\mathcal{K}) &\iff \gamma\,\alpha = \alpha\,\gamma \\
&\iff d\,\alpha + a\,\alpha^2 + b\,\beta\,\alpha + c\,\alpha\,\beta\,\alpha = d\,\alpha + a\,\alpha^2 + b\,\alpha\,\beta + c\,\alpha^2\,\beta \\
&\iff 2(b\,\alpha\,\beta + c\,\alpha^2\beta) = 0 \\
&\iff b = c = 0 \\
&\iff \gamma = d + a\,\alpha \in \mathcal{K}
\end{aligned}$$

This proves that $C_{\mathcal{H}}(\mathcal{K}) = \mathcal{K}$.

Let $\delta \in C_{\mathcal{H}}(\mathcal{K})$. Since $\mathbb{Q}$ is a commutative ring, $\delta \in C_{\mathcal{H}}(\mathcal{K}) = \mathcal{K}$. But δ belongs to an order in a quaternion algebra, so is integral over $\mathbb{Z}$. Moreover, $\mathrm{Im}(\theta) \cong \mathcal{O}_K$, so $\delta \in \mathrm{Im}(\theta)$. □

Let us denote S the set described in the proof of Theorem 5.24. Note that the field L used in that definition is actually the Hilbert Class Field H, but this fact was what we were proving at that moment.

Now, we are ready to prove the mentioned result.

Proposition 6.6. *Let K be an imaginary quadratic field. Let H be the Hilbert Class Field of K and let $E \in \mathcal{ELL}(\mathcal{O}_K)$ defined over H. Let P be a degree 1 prime of K such that the rational prime p that lies under P does not belong to S. Let Q be a prime of H over P. Let us call $\sigma_P = \left(\frac{H/K}{P}\right)$. Then, there is an isogeny $\lambda : E \longrightarrow E^{\sigma_P}$ that makes*

the following diagram commutative:

$$\begin{array}{ccc} E & \xrightarrow{\lambda} & E^{\sigma_P} \\ \downarrow & & \downarrow \\ \widetilde{E} & \xrightarrow{\mathrm{Frob}_p} & \widetilde{E}^{(p)} \end{array}$$

where the vertical maps are the correspoding reductions modulo Q.

Proof. First of all, note that E has good reduction over Q because $p \notin S$ and we use the definition of S.

Next, let us consider the natural isogeny $\phi : E \longrightarrow \overline{P} * E$. By using Lemma 5.25, we obtain that its reduction $\widetilde{\phi} : \widetilde{E} \longrightarrow \widetilde{\overline{P} * E}$ is purely inseparable of degree p.

On the other hand, in the proof of Corollary 5.26, we proved that $\overline{P} * E \cong F(\sigma_P) * E = E^{\sigma_P}$. If we reduce modulo Q, we obtain an isomorphism $\widetilde{\overline{P} * E} \cong \widetilde{E^{\sigma_P}}$. The composition of $\widetilde{\phi}$ with this isomorphism is an isogeny

$$\psi : \widetilde{E} \longrightarrow \widetilde{E^{\sigma_P}}$$

which is also purely inseparable of degree p. Since the reduction behaves well with the composition of isogenies, we find that ψ is the reduction modulo Q of the isogeny $\lambda : E \longrightarrow E^{\sigma_P}$ which is the composition of ϕ with the isomorphism $\overline{P} * E \cong E^{\sigma_P}$, that is, $\psi = \widetilde{\lambda}$.

By Proposition 4.27, there is a separable isogeny $\epsilon : \widetilde{E}^{(p)} \longrightarrow \widetilde{E^{\sigma_P}}$ such that $\widetilde{\lambda} = \epsilon \circ \mathrm{Frob}_p$. Using the same argument as in the proof of Lemma 5.25, we obtain that $\deg(\epsilon) = 1$, that is, ϵ is an isomorphism.

Let us take a model for E

$$E : y^2 = x^3 + a\,x + b.$$

If we apply σ_P, we obtain the elliptic curve

$$E^{\sigma_P} : y^2 = x^3 + \sigma_P(a)\,x + \sigma_P(b).$$

But by definition of σ_P, given $x \in L$, $\sigma_P(x) \equiv x^{N(P)} \pmod{Q}$. Since P is a degree 1 prime, $N(P) = p$. Then, $\widetilde{\sigma_P(x)} = \widetilde{x}^p$ in the residue field. Thus, the reduction of E^σ modulo Q is

$$\widetilde{E^{\sigma_P}} : y^2 = x^3 + \widetilde{a}^p\,x + \widetilde{b}^p,$$

which is a model for $\widetilde{E}^{(p)}$. This proves that $\widetilde{E^{\sigma_P}} = \widetilde{E}^{(p)}$, and hence ϵ is an automorphism.

The next task in the proof is to find $\epsilon_0 \in \mathrm{Aut}(E^{\sigma_P})$ such that $\widetilde{\epsilon_0} = \epsilon$. This will be enough because then the isogeny $\epsilon_0^{-1} \circ \lambda$ satisfies

$$\widetilde{\epsilon_0^{-1} \circ \lambda} = \epsilon^{-1} \circ \widetilde{\lambda} = \mathrm{Frob}_p\,.$$

Actually, it is enough to prove that if $\theta : \mathrm{End}(E^{\sigma_P}) \longrightarrow \mathrm{End}(\widetilde{E^{\sigma_P}})$ is the reduction map, then $\epsilon \in C_{\mathrm{End}(\widetilde{E^{\sigma_P}})}(Im(\theta))$. By the previous result, this means that $\epsilon \in \mathrm{Im}(\theta)$, so there is an endomorphism $\epsilon_0 \in \mathrm{End}(E^\sigma)$ such that $\widetilde{\epsilon_0} = \epsilon$. By Proposition 4.56, $\deg(\epsilon_0) = \deg(\epsilon) = 1$, so $\epsilon_0 \in \mathrm{Aut}(E^{\sigma_P})$ and we are done.

Let us prove that $\epsilon \in C_{\mathrm{End}(\widetilde{E^{\sigma_P}})}(Im(\theta))$. We take the normalized identifications $[\cdot]_E : \mathcal{O}_K \longrightarrow \mathrm{End}(E)$ and $[\cdot]_{E^{\sigma_P}} : \mathcal{O}_K \longrightarrow \mathrm{End}(E^{\sigma_P})$. By applying Corollary 5.7 to the isogeny $\lambda : E \longrightarrow E^{\sigma_P}$, we have that

$$\lambda \circ [\alpha]_E = [\alpha]_{E^{\sigma_P}} \circ \lambda \text{ for all } \alpha \in \mathcal{O}_K.$$

We claim that $\mathrm{Frob}_p \circ \widetilde{[\alpha]_E} = \widetilde{[\alpha]_E^{\sigma}} \circ \mathrm{Frob}_p$. Indeed, recall that $\widetilde{[\alpha]_E}$ is a rational map, so $\widetilde{[\alpha]_E} = [f_0, f_1, f_2]$, where f_k are polynomials with coefficients in the residue field, say $f_k(x,y) = \sum_{i,j} \widetilde{a_{ij}^{(k)}}\, x^i\, y^j$. Then,

$$\mathrm{Frob}_p \circ f_k(x,y) = f_k(x,y)^p = (\sum_{i,j} \widetilde{a_{ij}^{(k)}} x^i\, y^j)^p = \sum_{i,j} \widetilde{a_{ij}^{(k)}}^p\, x^{i\,p}\, y^{j\,p} = f_k^{\sigma_P}(x^p, y^p) = f_k^{\sigma_P} \circ \mathrm{Frob}_p(x,y),$$

which proves the claim.

Now, by Proposition 5.8, we have that $[\alpha]_E^{\sigma_P} = [\alpha^{\sigma_P}]_{E^{\sigma_P}}$. But α belongs to K and hence is fixed by σ_P. Using this fact, we obtain that

$$\mathrm{Frob}_p \circ \widetilde{[\alpha]_E} = \widetilde{[\alpha]_E^{\sigma_P}} \circ \mathrm{Frob}_p = \widetilde{[\alpha]_{E^{\sigma_P}}} \circ \mathrm{Frob}_p\,.$$

Hence, we have the following chain of equalities:

$$\begin{aligned}
\widetilde{[\alpha]_{E^{\sigma_P}}} \circ \epsilon \circ \mathrm{Frob}_p &= \widetilde{[\alpha]_{E^{\sigma_P}}} \circ \widetilde{\lambda} = \widetilde{[\alpha]_{E^{\sigma_P}} \circ \lambda} \\
&= \widetilde{\lambda \circ [\alpha]_E} = \widetilde{\lambda} \circ \widetilde{[\alpha]_E} \\
&= \epsilon \circ \mathrm{Frob}_p \circ \widetilde{[\alpha]_E} \\
&= \epsilon \circ \widetilde{[\alpha]_{E^{\sigma_P}}} \circ \mathrm{Frob}_p\,.
\end{aligned}$$

Applying the uniqueness in Theorem 4.27 to this equality, we deduce that $\widetilde{[\alpha]_{E^{\sigma_P}}} \circ \epsilon = \epsilon \circ \widetilde{[\alpha]_{E^{\sigma_P}}}$, which finishes the proof. □

When we take P a principal prime ideal, then $\sigma_P = 1$ and λ is an endomorphism. The following corollary describes the form of this endomorphism.

Corollary 6.7. *With the conditions of Theorem 6.6, assume that P is a principal degree 1 prime. Then, there is an unique element $\pi \in \mathcal{O}_K$ such that $P = \pi\,\mathcal{O}_K$ and the diagram*

$$\begin{array}{ccc}
E & \xrightarrow{[\pi]} & E \\
\downarrow & & \downarrow \\
\widetilde{E} & \xrightarrow{\mathrm{Frob}_p} & \widetilde{E}
\end{array}$$

is commutative.

Proof. First, by Theorem 6.6, there is a commutative diagram

$$\begin{array}{ccc}
E & \xrightarrow{\lambda} & E^{\sigma_P} \\
\downarrow & & \downarrow \\
\widetilde{E} & \xrightarrow{\mathrm{Frob}_p} & \widetilde{E^{(p)}}
\end{array}.$$

By the hypothesis, P is a principal ideal, so $\sigma_P = 1$. This says that $E^{\sigma_P} = E$ and $\widetilde{E^{(p)}} = \widetilde{E^{\sigma_P}} = \widetilde{E}$. In particular, $\lambda \in \mathrm{End}(E)$. By using the normalized identification $[\cdot]_E : \mathcal{O}_K \longrightarrow \mathrm{End}(E)$, there exist an unique $\pi \in \mathcal{O}_K$ such that $[\pi] = \lambda$. Then, the commutative diagram above is

$$\begin{array}{ccc} E & \xrightarrow{[\pi]} & E \\ \downarrow & & \downarrow \\ \widetilde{E} & \xrightarrow{\mathrm{Frob}_p} & \widetilde{E} \end{array}.$$

Now, since P is a degree 1 prime,

$$N^K(P) = p = \deg(\mathrm{Frob}_p) = \deg([\pi]) = |N^K(\pi)|,$$

where we have used Corollary 5.22.

But both $N^K(\pi\,\mathcal{O}_K)$ and $N^K(\overline{\pi}\,\mathcal{O}_K)$ coincide with $|N^K(\pi)| = p$, so $\pi\,\mathcal{O}_K$ and $\overline{\pi}\,\mathcal{O}_K$ are prime ideals of $\mathcal{O}_K$ over p. Since P is also a prime ideal of $\mathcal{O}_K$ over p and there are exactly two prime ideals of $\mathcal{O}_K$ over p, we have that either $P = \pi\,\mathcal{O}_K$ or $P = \overline{\pi}\,\mathcal{O}_K$.

Let us take a model for E/H such that E has good reduction over Q. Let $\omega \in \Omega_E$ be a non-zero invariant differential such that its reduction $\widetilde{\omega} \in \Omega_{\widetilde{E}}$ is a non-zero invariant differential. Then,

$$\widetilde{\pi}\,\widetilde{\omega} = \widetilde{\pi}\widetilde{\omega} = \widetilde{[\pi]^*(\omega)} = \widetilde{[\pi]}^*(\widetilde{\omega}) = \mathrm{Frob}_p^*(\widetilde{\omega}) = 0,$$

where the last equality is due to the inseparability of Frob_p. But $\widetilde{\omega}$ generates the K-vector space Ω_E, so $\widetilde{\pi} = \widetilde{0}$. This means that $\pi \in Q$. Hence, $\pi \in Q \cap K = P$, so $P = \pi\,\mathcal{O}_K$.

We have proved the existence of π. Let us see the uniqueness. We mentioned before that π is the unique element in $\mathcal{O}_K$ such that $[\pi] = \lambda$. Now, we have by Proposition 4.56 that the reduction map $\mathrm{End}(E) \longrightarrow \mathrm{End}(\widetilde{E})$ is injective and $\widetilde{\lambda} = \mathrm{Frob}_p$. Then, π is the unique element of $\mathcal{O}_K$ such that $\widetilde{[\pi]} = \mathrm{Frob}_p$. □

3.2 Construction of Ray Class Fields

As usual, let K be an imaginary quadratic field and let $E \in \mathcal{ELL}(\mathcal{O}_K)$ defined over the Hilbert Class Field $H = K(j(E))$ of K. We used torsion points in order to generate abelian extension of H. In this section, we will give the explicit construction of the Ray Class Field of K for a modulus $\mathfrak{m}$. Before doing this, we will introduce the Weber function $h : E \longrightarrow \mathbb{P}^1$ attached to E, which will be an essential ingredient in our explicit construction. After this, we will prove a corollary that gives us the explicit form of the maximal abelian extension of K.

Definition 6.8. *Let $E \in \mathcal{ELL}(\mathcal{O}_K)$. We will say that a map $h : E \longrightarrow E/\mathrm{Aut}(E) \cong \mathbb{P}^1$ is a Weber function for E provided that it is finite (i.e, for all $Q \in \mathbb{P}^1$, the set $h^{-1}(Q)$ is finite) and defined over H.*

By $E/\mathrm{Aut}(E)$ we mean the quotient set corresponding to the equivalence relation $(x, y)\mathcal{R}\phi(x, y)$, $\phi \in \mathrm{Aut}(E)$. To understand why this quotient is isomorphic to $\mathbb{P}^1$, we may determine $\mathrm{Aut}(E)$. Since E has complex multiplication by $\mathcal{O}_K$, this means that $\mathrm{End}(E) \cong \mathcal{O}_K$. Hence, $\mathrm{Aut}(E) \cong \mathcal{O}_K^*$, where the isomorphism is the normalized identification. The explicit expression of $\mathcal{O}_K^*$ is proved in [9] (Chapter III, Corollary 10.2):

1. If $j(E) \neq 0, 1728$, $\mathrm{Aut}(E) \cong \{1, -1\}$.
2. If $j(E) = 1728$, $\mathrm{Aut}(E) \cong \{1, -1, i, -i\}$.
3. If $j(E) = 0$, $\mathrm{Aut}(E) \cong \{1, -1, \omega, -\omega, \omega^2, -\omega^2\}$.

In the first case, it is clear that $[-1](x, y) = (x, -y)$. One can check easily that $[i](x, y) = (-x, iy)$ in the second case and $[\omega](x, y) = (\omega\, x, y)$ in the third case (by computing the pull-back evaluated at the invariant differential and using Proposition 5.5). This determines completely $\mathrm{Aut}(E)$.

After this, it is not difficult to establish the isomorphism between $E/\mathrm{Aut}(E)$ and $\mathbb{P}^1$ in each of the previous three cases. We consider homogeneous coordinates $[x_0, x_1]$ in $\mathbb{P}^1$ in such a way that the point of infinity in $\mathbb{P}^1$ has homogeneous coordinates $[1, 0]$. The class of the point $\infty \in E$ in $E/\mathrm{Aut}(E)$ (which only contains the point ∞ itself) is identified with the point of infinity in $\mathbb{P}^1$. If $j(E) \neq 0, 1728$ (resp. $j(E) = 1728$, resp. $j(E) = 0$), each class $\overline{(x, y)} \in E/\mathrm{Aut}(E)$ is identified with the point of $\mathbb{P}^1$ with homogeneous coordinates $[x, 1]$ (resp. $[x^2, 1]$, resp. $[x^3, 1]$).

Note that the non-trivial points of the curve correspond to points on $\mathbb{P}^1$ that are different from the point of infinity. Thus, these points can be given in a single affine coordinate. Namely, $[x_0, x_1] \in \mathbb{P}^1$ with $x_1 \neq 0$ is identified with $\frac{x_0}{x_1} \in \mathbb{A}^1$. We can give the definition of a Weber function on that way when it sends the point $\infty \in E$ to the point of infinity in $\mathbb{P}^1$. For example, if we take a model for E

$$E : y^2 = x^3 + A\, x + B,$$

the following is a Weber function:

$$h(x, y) = \begin{cases} x & \text{if } A\, B \neq 0 \\ x^2 & \text{if } B = 0 \\ x^3 & \text{if } A = 0 \end{cases}.$$

Indeed, it is clearly finite and defined over H. When $A, B \neq 0$, note that h is the first-coordinate-function for points of E.

In the sequel, h will be this example of Weber function.

We will need the following lemma, which says that the Weber function E is $\mathrm{Aut}(E)$-invariant. It can be consulted in [11].

Lemma 6.9. *Let E be an elliptic curve over $\mathbb{C}$ and let $P, P' \in E$. Then, $h(P) = h(P')$ if and only if there is some $\epsilon \in \mathrm{Aut}(E)$ such that $P' = \epsilon(P)$.*

Proof. Let us fix a model

$$E : y^2 = x^3 + A\, x + B$$

and write $P = (x, y)$ and $P' = (x', y')$. We will only prove it for $j(E) \neq 0, 1728$ (the other cases are analogous). In that case, $h(P) = h(P')$ if and only if $x = x'$. Now, since $P, P' \in E$, we have that

$$x = x' \Longleftrightarrow y^2 = x^3 + A\, x + B = x'^3 + A\, x' + B = y'^2,$$

and the latter is equivalent to $y' = \pm y$. Hence,

$$h(P) = h(P') \Longleftrightarrow (x', y') = (x, \pm y).$$

□

Now, we are ready to give the explicit construction of the Ray Class Field of K for any modulus $\mathfrak{m}$.

Theorem 6.10. *Let K be an imaginary quadratic field, $E \in \mathcal{ELL}(\mathcal{O}_K)$ and $h : E \longrightarrow \mathbb{P}^1$ be a Weber function for E/H as before. Let $\mathfrak{m}$ be a modulus of K. Then, the Ray Class Field of K for $\mathfrak{m}$ is*

$$K_{\mathfrak{m}} = K(j(E), h(E[\mathfrak{m}])).$$

Proof. Let $L = K(j(E), h(E[\mathfrak{m}]))$.

It is enough to prove that

$$\left(\frac{L/K}{P}\right) = 1 \Longleftrightarrow P \in P_{K,1}(\mathfrak{m}) \tag{6.3}$$

for all but finitely many of the degree 1 primes P of K. Indeed, let us assume that we have proved this. Then, for all but finitely many primes of L/K, we have the following equivalences:

$$\begin{aligned} P \text{ splits completely in } L &\Longleftrightarrow \left(\frac{L/K}{P}\right) = 1 \\ &\Longleftrightarrow P \in P_{K,1}(\mathfrak{m}) \\ &\Longleftrightarrow \left(\frac{K_{\mathfrak{m}}/K}{P}\right) = 1 \\ &\Longleftrightarrow P \text{ splits completely in } K_{\mathfrak{m}} \end{aligned}$$

With the notation of Chapter 3, $S_{L/K} \doteq S_{K_{\mathfrak{m}}/K}$. Then, Theorem 3.31 gives us that $L = K_{\mathfrak{m}}$ and we are done.

Let us assume that $P \in P_{K,1}(\mathfrak{m})$ satisfies that the rational prime p that lies under P does not belong to S and does not divide $\#E[\mathfrak{m}]$. Note that the set of primes that do not satisfy some of these conditions is finite, so there is no problem with these assumptions. By definition, $P = \mu\,\mathcal{O}_K$, where $\mu \in \mathcal{O}_K$ and $\mu \equiv 1 \pmod{m}$. Let H be the Hilbert Class Field of K and $\sigma_P = \left(\frac{H/K}{P}\right)$. Since P is principal, by Artin Reciprocity Theorem, $\sigma_P = 1$. By Corollary 6.7, there is an unique $\pi \in \mathcal{O}_K$ such that $P = \pi\,\mathcal{O}_K$ and the diagram

$$\begin{array}{ccc} E & \xrightarrow{[\pi]} & E \\ \downarrow & & \downarrow \\ \widetilde{E} & \xrightarrow{\mathrm{Frob}_p} & \widetilde{E} \end{array}$$

is commutative.

Since $\mu\,\mathcal{O}_K = P = \pi\,\mathcal{O}_K$, there is a unit $\beta \in \mathcal{O}_K^*$ such that $\pi = \beta\,\mu$. Now, we have that $[\beta] \in \mathrm{Aut}(E)$ because β is a unit and $[\cdot]$ is an isomorphism. Moreover, we have that

$$[\pi] = [\beta\,\mu] = [\beta] \circ [\mu].$$

We want to prove that $\left(\frac{L/K}{P}\right)$ fixes L. First, we show that it fixes $H = K(j(E))$. Since $j(E) \in H$ and the restriction of $\left(\frac{L/K}{P}\right)$ to H is $\sigma_P = 1$, $j(E)^{\left(\frac{L/K}{P}\right)} = j(E)$, and this gives us what we wanted.

Now, let us prove that $\left(\frac{L/K}{P}\right)$ fixes $h(E[\mathfrak{m}])$. Let $T = (x, y) \in E[\mathfrak{m}]$. In order to prove that $h(T)^{\left(\frac{L/K}{P}\right)} = h(T)$, it is enough to prove

$$T^{\left(\frac{L/K}{P}\right)} = [\pi](T). \tag{6.4}$$

Indeed, since h is defined over H, $h(T)^{\left(\frac{L/K}{P}\right)} = h(T^{\left(\frac{L/K}{P}\right)})$. Now, by using (6.4), we have that $h(T^{\left(\frac{L/K}{P}\right)}) = h([\pi](T))$. But we also proved that $[\pi] = [\beta] \circ [\mu]$. Then, $h([\pi](T)) = h([\beta] \circ [\mu](T))$. Since $[\beta] \in \mathrm{Aut}(E)$, by the previous lemma, $h([\beta] \circ [\mu](T)) = h([\mu](T))$. Finally, since $T \in E[\mathfrak{m}]$ and $\mu \equiv 1 \pmod{\mathfrak{m}}$, we have that $\mu - 1 \in \mathfrak{m}$, so $[\mu - 1](T) = \infty$. Then $\mu(T) = T$, which implies that $h([\mu](T)) = h(T)$. This proves the desired equality.

So let us prove (6.4). Since P is a degree 1 prime,

$$T^{\left(\frac{L/K}{P}\right)} = (x^{N(P)}, y^{N(P)}) = (x^p, y^p).$$

Reducing modulo Q, $\widetilde{T^{\left(\frac{L/K}{P}\right)}} = \mathrm{Frob}_p(\widetilde{T})$. By using the commutative diagram, the latter equals to $\widetilde{[\pi](T)}$.

Let us prove that the reduction $E[\mathfrak{m}] \longrightarrow \widetilde{E}[\mathfrak{m}]$ is injective. By Proposition 4.56, given an integer number m coprime with p, the reduction $E[m] \longrightarrow \widetilde{E}$ is injective. Given $P \in E[\mathfrak{m}]$, the order of P divides $\#E[\mathfrak{m}]$. Since p does not divide $\#E[\mathfrak{m}]$, we deduce that the order of P is coprime with p. Let $d = \mathrm{lcm}(\{\mathrm{ord}(P) \mid P \in E[\mathfrak{m}]\})$. Then, d is again coprime with p and clearly $E[\mathfrak{m}] \subset E[d]$. Thus, the reduction $E[d] \longrightarrow \widetilde{E}$ is injective and its restriction $E[\mathfrak{m}] \longrightarrow \widetilde{E}[\mathfrak{m}]$ is also injective, as we claimed.

Since $\widetilde{T^{\left(\frac{L/K}{P}\right)}} = \widetilde{[\pi](T)}$ and the reduction $E[\mathfrak{m}] \longrightarrow \widetilde{E}[\mathfrak{m}]$ is injective, we obtain that

$$T^{\left(\frac{L/K}{P}\right)} = [\pi](T). \tag{6.5}$$

Since $\left(\frac{L/K}{P}\right)$ fixes both H and $h(E[\mathfrak{m}])$, it coincides with the trivial automorphism.

Conversely, let us assume that $\left(\frac{L/K}{P}\right) = 1$. Again, the restriction of this automorphism to H is σ_P, which equals 1. We use Corollary 6.7, obtaining that there is an unique $\pi \in \mathcal{O}_K$ such that $P = \pi\,\mathcal{O}_K$ and the diagram

$$\begin{array}{ccc} E & \xrightarrow{[\pi]} & E \\ \downarrow & & \downarrow \\ \widetilde{E} & \xrightarrow{\mathrm{Frob}_p} & \widetilde{E} \end{array}$$

is commutative.

Let $\sigma \in \mathrm{Gal}(\overline{K}/K)$ be an extension of the Artin symbol

$$\left(\frac{K^{ab}/K}{P}\right) \in \mathrm{Gal}(K^{ab}/K).$$

Then, the restriction of σ to L is the trivial automorphism. In particular, the restriction of σ to H is also the trivial automorphism.

Let $T \in E[\mathfrak{m}]$. Then the coordinates of T lie in K^{ab}. Let us consider the reduction of h modulo Q

$$\widetilde{h} \,:\, \widetilde{E} \longrightarrow \widetilde{E}/\widetilde{\mathrm{Aut}(E)}.$$

Let us show that $\widetilde{h}(\widetilde{[\pi]}(\widetilde{T})) = \widetilde{h}(\widetilde{T})$. By using the commutative diagram, $\widetilde{h}(\widetilde{[\pi]}(\widetilde{T})) = \widetilde{h}(\widetilde{[\pi](T)}) = \widetilde{h}(\mathrm{Frob}_p(\widetilde{T}))$. Since σ restricts to $\left(\frac{K^{ab}/K}{P}\right) \in \mathrm{Gal}(K^{ab}/K)$, $\widetilde{h}(\mathrm{Frob}_p(\widetilde{T})) = \widetilde{h}(\widetilde{T^\sigma})$. This trivially coincides with $\widetilde{h(T^\sigma)}$. Now, since h is defined over H and $\sigma|_H = 1$, $\widetilde{h(T^\sigma)} = \widetilde{h(T)^\sigma}$. But $h(T) \in L$ and also $\sigma|_L = 1$, so $\widetilde{h(T)^\sigma} = \widetilde{h(T)} = \widetilde{h}(\widetilde{T})$. Then, the desired equality holds.

Since the reduction behaves well with sum and product and the image of h lies in $\widetilde{E}/\widetilde{\mathrm{Aut}(E)}$, we have a version of the previous lemma in charasteristic p: given $\widetilde{P}, \widetilde{P'} \in \widetilde{E}$, $\widetilde{h}(\widetilde{P}) = \widetilde{h}(\widetilde{P'})$ if and only if there is $\widetilde{\epsilon} \in \widetilde{\mathrm{Aut}(E)}$ such that $\widetilde{P'} = \widetilde{\epsilon}(\widetilde{P})$. Thus, there is an automorphism $[\beta] \in \mathrm{Aut}(E)$ such that $\widetilde{[\pi]}(\widetilde{T}) = \widetilde{[\beta]}(\widetilde{T})$. Since the reduction map $E[\mathfrak{m}] \longrightarrow \widetilde{E}[\mathfrak{m}]$ is injective, $[\pi - \beta](T) = \infty$.

Note that β might depend on T, so the last equality holds for that concrete T. Recall that by Proposition 5.21, $E[\mathfrak{m}]$ is a $\mathcal{O}_K/\mathfrak{m}$-module of rank 1. Then, given $T' \in E[\mathfrak{m}]$, there is $\alpha \in \mathcal{O}_K$ such that $T' = (\alpha + \mathfrak{m})\, T = [\alpha](T)$. Thus,

$$[\pi - \beta](T') = [\pi - \beta]([\alpha](T)) = [\alpha]([\pi - \beta](T)) = \infty.$$

We have proven, then, that $[\pi - \beta](T) = \infty$ for all $T \in E[\mathfrak{m}]$. By definition of $E[\mathfrak{m}]$, this means that $\pi - \beta \in \mathfrak{m}$, so $\pi \equiv \beta \,(\mathrm{mod}\, \mathfrak{m})$. Equivalently,

$$\beta^{-1}\, \pi \equiv 1 \,(\mathrm{mod}\, \mathfrak{m}).$$

Since β is a unit, $P = \pi\, \mathcal{O}_K = \beta^{-1} \pi\, \mathcal{O}_K$, which proves that $P \in P_{K,1}(\mathfrak{m})$. This finishes the proof. □

We have constructed the explicit expression of the Ray Class Field of K for any modulus $\mathfrak{m}$. After this, the construction of the maximal abelian extension of K is nothing but a corollary.

Corollary 6.11. *Let K be an imaginary quadratic field and let $E \in \mathcal{ELL}(\mathcal{O}_K)$. Then, $K^{\mathrm{ab}} = K(j(E), h(E_{\mathrm{tors}}))$.*

Proof. Recall that K^{ab} is the compositum of all abelian extensions of K. Given a modulus $\mathfrak{m}$ of K, by Proposition 3.25, $K_{\mathfrak{m}}$ contains all the abelian extensions of K whose conductor divides $\mathfrak{m}$. Hence, it is the compositum of such abelian extensions. For any abelian extension L/K there exist a modulus $\mathfrak{m}$ such that $L \subset K_{\mathfrak{m}}$ (indeed, it suffices to take a multiple of $\mathfrak{f}(L/K)$). By rearrenging the fields in the compositum K^{ab}, we obtain that K^{ab} is the compositum of all Ray Class Fields $K_{\mathfrak{m}}$ of K.

But by the previous theorem, $K_{\mathfrak{m}} = K(j(E), h(E[\mathfrak{m}]))$. Since $\bigcup_{\mathfrak{m}} E[\mathfrak{m}] = E_{\mathrm{tors}}$, we deduce that

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

□

We deduce that in the case where $j(E) \neq 0, 1728$, the maximal abelian extension of K is obtained by adjoining to K the j-invariant $j(E)$ and the first coordinates of the torsion points of E. This completes the proof of *Kronecker's Jugendtraum* in the imaginary-quadratic case.

3.3 Examples of computation of Hilbert and Ray Class Fields

Let K be an imaginary quadratic field. We know explicitely the form of the Hilbert Class Field and the Ray Class Field for any conductor of K, in the sense that we know their generators. However, this is a theoretical answer and we would like to compute explicitely these class fields for a concrete field K. In this section we will see how to do this.

We begin with the Hilbert Class Field H of K. We proved at the end of Chapter 5 that $H = K(j(E))$, where $E \in \mathcal{ELL}(\mathcal{O}_K)$. If we know the exact value of $j(E)$, then the problem will be solved. We could compute the elliptic curve E and then compute its j-invariant. But then we get an approximation of $j(E)$ and we look for an algebraic description of H. We may take another approach. What we will do is to compute the irreducible polynomial f of $j(E)$ over K. This is enough because H is the splitting field of f over K. In other words, $H = K(z)$ where z has minimal polynomial f.

Let $N \in \mathbb{Z}_{>0}$ such that $K = \mathbb{Q}(\sqrt{-N})$. Put $\mathcal{C}(\mathcal{O}_K) = \{\overline{\mathfrak{a}_1}, ..., \overline{\mathfrak{a}_n}\}$. Let us denote $\mathcal{T} = \{j(\mathfrak{a}_1), ..., j(\mathfrak{a}_n)\}$. Now, there is a one-to-one correspondence

$$\begin{array}{ccc} \mathcal{C}(\mathcal{O}_K) & \longrightarrow & \mathcal{T} \\ \overline{\mathfrak{a}} & \longmapsto & j(\mathfrak{a}) \end{array}.$$

In the proof of Theorem 5.12, we proved that $j(\mathfrak{a}_1), ..., j(\mathfrak{a}_n)$ are the conjugates roots of the same polynomial. Then, the polynomial f we want to compute has roots $j(\mathfrak{a}_1), ..., j(\mathfrak{a}_n)$. Thus, it is just

$$f(X) = \prod_{i=1}^{n} (X - j(\mathfrak{a}_i)).$$

Thus, the procedure we follow in order to compute the Hilbert Class Field of an imaginary quadratic field is the following:

1. We compute a system of representatives $\mathfrak{a}_1, ..., \mathfrak{a}_n$ of the classes in the ideal class group $\mathcal{C}(\mathcal{O}_K)$ of K.

2. We compute the j-invariant of each one of the representatives of $\mathcal{C}(\mathcal{O}_K)$.

3. We use the values obtained in order to compute the coefficients of the polynomial $f = \prod_{i=1}^{n} (X - j(\mathfrak{a}_i))$.

We can implement these steps easily in some mathematics software. The values obtained for the coefficients may not be exact, but we can get the correct values by using that the j-invariant of an elliptic curve with complex multiplication is an algebraic integer (see [10], Chapter II, Theorem 6.1). This implies that the coefficients of the irreducible polynomial are integer numbers (see [4], Theorem 1).

In the following examples, we use Sage to do the computations.

Example 6.12. *Let us compute the Hilbert Class Field of* $K = \mathbb{Q}(\sqrt{-13})$. *A system of representatives of* $\mathcal{C}(\mathcal{O}_K)$ *is given by*

$$\mathfrak{a}_1 =< 1, \sqrt{-13} >,$$

$$\mathfrak{a}_2 =< 2, 1 + \sqrt{-13} > .$$

The j*-invariants we obtain are*

$$j(\mathfrak{a}_1) \approx 6.89696230631497 \cdot 10^9 - 9.56731793025273 \cdot 10^{-6}\, i,$$

$$j(\mathfrak{a}_2) \approx -82306.3149816314 + 5.79305787577049 \cdot 10^{-11}\, i.$$

Actually, both values are real (see [10], Exercise 2.9*), and this is the reason because of which the approximations have imaginary parts very close to* 0.

The next step is to use the previous values to compute $f(X) = (X - j(\mathfrak{a}_1)) \cdot (X - j(\mathfrak{a}_2))$. *By the previous comment, we can erase the imaginary parts in this computation. Then, we obtain the polynomial*

$$X^2 - 6.89687999999999 \cdot 10^9\, X - 5.67663551999999 \cdot 10^{14}$$

whose coefficients are approximations of the coefficients of f. *Using that* f *has integer coefficients, we obtain that*

$$f(X) = X^2 - 6896880000 \cdot X - 567663552000000.$$

Using the same procedure to compute the Hilbert Class Field of $K = \mathbb{Q}(\sqrt{-34})$, *we obtain* 4 *classes of ideals and from here the irreducible polynomial*

$$\begin{aligned} f(X) = X^4 &- 8151279336430848\, X^3 + 735960027609078992953344\, X^2 \\ &- 183460711128247205102931 1488\, X + 24228291694285725040875216 56832. \end{aligned}$$

Note that the degree of the polynomial obtained coincides with the number of classes of ideals. This fact is general and follows from Artin Reciprocity Theorem, which gives us that $|\mathcal{C}(\mathcal{O}_K)| = [H : K] = \deg(f)$.

Finally, we explain how to compute the Ray Class Field of an imaginary quadratic field K for a modulus $N\,\mathcal{O}_K$, $N \in \mathbb{Z}_{>0}$. This is enough in order to compute K^{ab}. Indeed, given an arbitrary modulus $\mathfrak{m}$ of K, then $\mathfrak{m}\,\overline{\mathfrak{m}} = N(\mathfrak{m})\,\mathcal{O}_K$, and hence $\mathfrak{m}$ divides $N(\mathfrak{m})\,\mathcal{O}_K$, which implies by Proposition 3.25 that $K_{\mathfrak{m}} \subset K_{N\,\mathcal{O}_K}$. We deduce that K^{ab} is the compositum of all Ray Class Fields $K_{N\,\mathcal{O}_K}$, $N \in \mathbb{Z}_{>0}$.

We proved that $K_{N\,\mathcal{O}_K} = K(j(E), h(E[N]))$, where E is an elliptic curve defined over H and with complex multiplication by $\mathcal{O}_K$. We only deal with elliptic curves such that $j(E) \neq 0, 1728$, so h is the x-coordinate function. We saw that H is the splitting field of an irreducible polynomial f over K and we computed explicitely this polynomial. Now, for obtaining the Ray Class Field of K for the modulus N, we may add all the x-coordinates of N-torsion points of E.

Fixed N and a model of E, there is a polynomial D_N, called the N-th division polynomial, defined recursively in terms of the coefficients of the model fixed for E (see

[9], Exercise 3.7). This polynomial has the property that its roots are the x-coordinates of the N-torsion points of E. Then, computing this polynomial solves the problem.

Note that this involves computing some elliptic curve E with the required properties. Remember that the roots of the polynomial f we computed are the j-invariants of the representatives of the different classes of ideals. What we do is to take some of them and compute an elliptic curve whose j-invariant is that value.

Then, the steps we follow are:

1. We compute the polynomial f whose roots generate the Hilbert Class Field of K by using the previous procedure.
2. We take some root α of f and compute an elliptic curve E whose j-invariant is α.
3. We compute the N-th division polynomial associated to E.

Example 6.13. *Let us compute the Ray Class Field of $K = \mathbb{Q}(\sqrt{-13})$ for the modulus $3\,\mathcal{O}_K$. In the previous example, we computed the polynomial f whose roots generate the Hilbert Class Field H of K. Fix $z \in H$ with minimal polynomial f, so $H = K(z)$. We do all computations in terms of z, this is no problem because we can compute an approximation of its value. We obtain that $\alpha = -z + 6896880000$ is a root of f in H. An elliptic curve E with $j(E) = \alpha$ is the following:*

$$\begin{aligned} E\,:\, y^2 =& x^3 + (20690634816\,z - 142702528440430080000)\,x \\ &+ (95134995124675411968\,z - 65614247538634470034243584000 0). \end{aligned}$$

Once we have computed E, we can compute the third division polynomial D_3 associated to E, which is

$$\begin{aligned} D_3(x) =& 3\,x^4 + (124143808896\,z - 856215170642580480000)\,x^2 \\ &+ (1141619941496104943616\,z - 787370970463613640410923008 0000)\,x \\ &+ 29526411392385511515409612800 00\,z \\ &- 203642546414032125577122467146629120000 00. \end{aligned}$$

Then, $K_{3\,\mathcal{O}_K} = H(a)$, where a has minimal polynomial D_3.

Let $K = \mathbb{Q}(\sqrt{-15})$. Let $z \in H$ such that $H = K(z)$. Then z has minimal polynomial

$$f(x) = x^2 + 191025\,x - 121287375.$$

Now, $K_{2\,\mathcal{O}_K} = H(a)$, where a has minimal polynomial

$$D_2(x) = 4\,x^3 + (-2313036\,z - 443303150400)\,x + 298200051072\,z + 57152369475847800.$$

Bibliography

[1] N. Schappacher; *On the history of Hilbert's twelfth problem: a comedy of errors,* Société Mathématique de France, pp. 243-273, 1998

[2] S.G. Vladut; *Kronecker's Jugentraum and Modular Functions,* Gordon and Breach Publishers, Luxembourg, 1995

[3] P. Breiding and D. Samart; *Kronecker's Jugendtraum,* International Summer School on Number Theory, Penn-State, 2012

[4] D.A. Marcus; *Number Fields,* Springer-Verlag, 1977

[5] M. F. Atiyah, I. G. McDonald; *Introduction to Commutative Algebra,* Addison-Wesley Series in Mathematics, 1969

[6] D. A. Cox; *Primes of the form $x^2 + ny^2$,* Pure and Applied Mathematics, Canada, 1989

[7] K. S. Kedlaya; *Complex Multiplication and Explicit Class Field Theory,* Harvard University, Cambridge, 1966

[8] N. Koblitz; *Introduction to elliptic curves and modular forms,* Springer-Verlag, Seattle, 1984

[9] J.H. Silverman; *The arithmetic of elliptic curves,* Graduate texts in Mathematics, Springer, San Francisco, 1986

[10] J.H. Silverman; *Advanced topics in the arithmetic of elliptic curves,* Graduate texts in Mathematics, Springer, New York, 1994

[11] E. Ghate; *Complex multiplication,* Winter School of Elliptic Curves, HRI, November 8-25, 2000