NTNU
Innovation and Creativity

Constructing elliptic curves over finite fields using complex multiplication

Øystein Øvreås Thuen

Master of Science in Physics and Mathematics
Submission date: June 2006
Supervisor: Alexei Roudakov, MATH
Co-supervisor: Kristian Gjøsteen, ITEM

Norwegian University of Science and Technology
Department of Mathematical Sciences

Problem Description

Special families of elliptic curves are used in pairing-based cryptography. A method for the creation of such curves has been developed, using complex multiplication. We will study existing methods and explore possible improvements.

Assignment given: 20. January 2006
Supervisor: Alexei Roudakov, MATH

Abstract

We study and improve the CM-method for the creation of elliptic curves with specified group order over finite fields. We include a thorough review of the mathematical theory needed to understand this method. The ability to construct elliptic curves with very special group order is important in pairing-based cryptography.

Preface

In recent years a special family of elliptic curves, known as CM-curves, has been of increasingly interest in cryptography. This master thesis focuses on the construction of CM-curves, using the CM-method [1]. The mathematical theory needed to understand this method is considerable and take up a large part of this paper. The CM-method for creating elliptic curves is presented in the last chapter, where it is also generalized to work over any finite field.

In the first part this paper follows the excellent book by Borevich and Shafarevich [3]. Most of the material regarding elliptic curves is from [10], [11] and [12]. The CM-method was first developed by Atkin and Morain [1] and has been studied further in [7]. The computer system PARI/GP has been used for computations.

The author thanks supervisor prof. Alexei Rudakov for his insight and comments, and assistent supervisor Kristian Gjøsteen for introducing this topic, his continuous help and his ability to see things from a different angle.

Contents

1 Introduction

In recent years many new types of cryptographic protocols have been studied, based on bilinear pairings. Here one can especially mention identity based cryptography, see [2] for one proposed encryption scheme. The only known group structures with efficiently computable bilinear pairings usable for cryptography are special families of elliptic curves.

An elliptic curve $E(\mathbb{F}_q)$ with $q = p^r$ and $p > 3$ prime, can be represented as the solutions (x, y) over $\mathbb{F}_q$ of an equation $y^2 = x^3 + Ax + B$ where $A, B \in \mathbb{F}_q$, together with a single extra point. One can define an addition on elliptic curves, turning them into abelian groups.

When using an elliptic curve in a cryptosystem, controlling the group order $\#E(\mathbb{F}_q)$ is important as it directly determines the security of the cryptosystem. One method to find proper curves is to generate random curves and compute the group order using point counting algorithms such as Schoof's [8] or Satoh's algorithms. A different approach is known as the complex multiplication method (CM-method) and was developed by Atkin and Morain [1] and studied further by Lay and Zimmer [7]. Here one can specify the group order n and a prime p and the CM-method produces an elliptic curve E such that $\#E(\mathbb{F}_p) = n$, provided such a curve exists.

CM-curves have special properties and are usually avoided in cryptography. Pairing-friendly curves are very sparse and point counting algorithms cannot efficiently produce them. The CM-method can however do this efficiently, as one can specify properties of the curve in advance. This makes CM-curves interesting for identity based cryptography.

The purpose of this paper is to understand the mathematical theory behind the CM-method. We study generalized prime numbers in rings without unique factorization, modules and orders in algebraic number fields, class field theory and elliptic curves over the complex numbers, number fields and finite fields. We also include and extend the CM-method.

2 Number Theory

2.1 Norm, trace and modules

We start this section by introducing norm and trace of elements of extension fields. Let k be a field and K/k a finite extension of degree n. Let $\omega_1, \ldots, \omega_n$ be a basis for this extension. For any $\alpha \in K$ we can write

$$\alpha\omega_i = \sum_{j=1}^{n} a_{ij}\omega_j$$

for each i, where $a_{ij} \in k$. The set of a_{ij} then define a matrix (a_{ij}) and we define the *characteristic polynomial* $f_\alpha(x)$

$$f_\alpha(x) = \det(xI - (a_{ij}))$$

where I is the identity matrix. It can be shown that the characteristic polynomial is a power of the minimal polynomial and is independent of the basis chosen.

We also define norm and trace of the element α

$$\begin{aligned} \mathrm{N}_{K/k}(\alpha) &= \det(a_{ij}) \\ \mathrm{Tr}_{K/k}(\alpha) &= \sum_{i=1}^{n} a_{ii} \end{aligned}$$

Trace and norm are independent of the basis we have chosen for K/k and they satisfy the following properties. For any $\alpha, \beta \in K$ and any $a \in k$

$$\begin{aligned} \mathrm{N}(\alpha\beta) &= \mathrm{N}(\alpha)\mathrm{N}(\beta) \\ \mathrm{Tr}(\alpha + \beta) &= \mathrm{Tr}(\alpha) + \mathrm{Tr}(\beta) \\ \mathrm{Tr}(a\alpha) &= a\mathrm{Tr}(\alpha) \end{aligned}$$

We also have the following relation between norms, traces and the characteristic polynomial.

Theorem 2.1. *Let $f_\alpha(x)$ be the characteristic polynomial for the element $\alpha \in k/K$ and let Ω be an extension where f_α splits into linear factors*

$$f_\alpha(x) = (x - \alpha_1)\ldots(x - \alpha_n)$$

Then

$$\begin{aligned} \mathrm{N}_{K/k}(\alpha) &= \alpha_1 \ldots \alpha_n \\ \mathrm{Tr}_{K/k}(\alpha) &= \alpha_1 + \cdots + \alpha_n \end{aligned}$$

Proof. If

$$f_\alpha(x) = \det(xI - (a_{ij})) = x^n + b_1 x^{n-1} + \cdots + b_n$$

then it follows from the properties of determinants that $b_1 = -\mathrm{Tr}(a_{ij})$ and $b_n = (-1)^n \det(a_{ij})$. But from the splitting in Ω we have $b_1 = -(\alpha_1 + \cdots + \alpha_n)$ and $b_n = (-1)^n \alpha_1 \ldots \alpha_n$, and the theorem is proven. □

For the remainder of this section K will be an algebraic number field, i.e. a finite extension of $\mathbb{Q}$. Let $\mu_1, \ldots, \mu_m \in K$ be any finite set of elements. Define a set

$$M = \{c_1\mu_1 + \cdots + c_m\mu_m \colon c_i \in \mathbb{Z}\}. \tag{1}$$

This is a finitely generated $\mathbb{Z}$-module with $\{\mu_1, \ldots, \mu_m\}$ as generator set. We will only consider modules on this form and we will sometimes just write $M = \{\mu_1, \ldots, \mu_m\}$.

We say that two modules M and M' are *similar* if there exists an element $\alpha \in K$ such that $M = \alpha M'$.

If K has degree n over $\mathbb{Q}$, a module in K can not have more than n linearly independent elements over $\mathbb{Q}$. We say that a module is *full* if it contains exactly n linearly independent elements over $\mathbb{Q}$.

We know that a module has many distinct sets of generators. We are interested in finding a small set that still generates the whole module. Let $\{\alpha_1, \ldots, \alpha_m\}$ be a set of generators. We say that this set is a *basis* if its elements are linearly independent over $\mathbb{Z}$.

One can show that all modules on the form given by (2.1) are free, and thus they have a basis and any basis for a module has the same number of elements. The number of elements in a basis is known as the *rank* of the module and coincides with the number of linearly independent elements (over $\mathbb{Q}$) in the module.

2.2 Coefficient rings and orders

We will now define a few constructions related to modules. We start with orders. A full module in $K/\mathbb{Q}$ is called an *order* if it contains 1 and is a subring of K.

Let M be a full module in K. We define *the coefficient ring* of M

$$\mathbb{D}_M = \{\alpha \in K \colon \alpha M \subseteq M\}$$

It is easily shown that $\mathbb{D}_M$ is a ring with unity.

Theorem 2.2. *Let M be a full module in $K/\mathbb{Q}$. The coefficient ring of M is a full module.*

Proof. We first show that $\mathbb{D}_M$ is a module. Let $\gamma \in M$ be any non-zero element. For any $\alpha \in \mathbb{D}_M$, $\alpha\gamma \in M$. It follows that $\gamma\mathbb{D}_M \subseteq M$ and that $\gamma\mathbb{D}_M$ is a submodule of M. But then $\mathbb{D}_M = \gamma^{-1}(\gamma\mathbb{D}_M)$ is also a module.

To show that this is a full module, we pick a non-zero element $\alpha \in K$. Let $\{\mu_1, \ldots, \mu_n\}$ be a basis for M. Clearly it is also a basis for K over $\mathbb{Q}$. We can then choose rational numbers a_{ij} such that

$$\alpha\mu_i = \sum_{j=1}^{n} a_{ij}\mu_j$$

for all $1 \leq i \leq n$. We can find an integer c such that all $ca_{ij} \in \mathbb{Z}$. Since M is a $\mathbb{Z}$-module, $c\alpha\mu_i \in M$. This is true for all μ_i and thus $c\alpha \in \mathbb{D}_M$. We now let $\{\alpha_1, \ldots, \alpha_n\}$ be any basis for K. Using the above, we can find integers $\{c_1, \ldots, c_n\}$ such that all the product $c_i\alpha_i$ are in the coefficient ring. These elements are linearly independent over $\mathbb{Q}$, and it follows that $\mathbb{D}_M$ is a full module. □

Since $\mathbb{D}_M$ is a full module and a ring with unity, we have this corollary.

Corollary 2.3. *The coefficient ring of any full module in $K/\mathbb{Q}$ is an order.*

Lemma 2.4. *Let α be in the order $\mathbb{D}$. Then the characteristic polynomial and the minimal polynomial of α has integer coefficients and the norm and trace of α are integers.*

Proof. Let M be a module such that $\mathbb{D}$ is its coefficient ring. (We can always find such an M, for instance we could take $M = \mathbb{D}$.) And let $\{\mu_1, \ldots \mu_n\}$ be a basis for M. Since $\alpha \in \mathbb{D}$, we can write

$$\alpha\mu_i = \sum a_{ij}\mu_j \in M$$

for all i. It follows that a_{ij} are integers. The characteristic polynomial

$$f_\alpha(x) = \det(xI - (a_{ij}))$$

thus has integer coefficients. Using the fact that f_α is a power of the minimal polynomial and Theorem 2.1, we have shown the lemma. □

2.3 Maximal order

A number field has many orders and we will in this part show that there exists a maximal order containing all orders. We have seen that elements in an order have minimal polynomials with integer coefficients. This motivates us to look at the set of all elements whose minimal polynomial has integer coefficients. We call this set R_K. It is clear that all orders must be contained in this set. It turns out that R_K is in fact the maximal order.

Theorem 2.5. *The maximal order of a number field K is the set of elements that have minimal polynomials with integer coefficients. This is equivalent to saying that the maximal order is the integral closure of $\mathbb{Z}$ in K.*

First we prove two lemmas.

Lemma 2.6. *Let α be an element in a number field K and let $t^m + c_1 t^{m-1} + \cdots + c_m$ be the minimal polynomial of α. If all c_i are integers (i.e. $\alpha \in R_K$), then the module $M = \{1, \alpha, \ldots, \alpha^{m-1}\}$ is a ring.*

Proof. Need only to show that $\alpha^k \in M$ for all $k \geq 0$. This is clear for all $k \leq m-1$ and since α is a root of its minimal polynomial we get

$$\alpha^m = -c_1\alpha^{m-1} - c_2\alpha^{m-2} - \cdots - c_m$$

and $\alpha^m \in M$. We will show the rest by induction. Let $k > m$ and assume that $\alpha^{k-1} \in M$. Then there exists integers a_i such that

$$\alpha^{k-1} = a_1\alpha^{m-1} + a_2\alpha^{m-2} + \cdots + a_m$$

and

$$\alpha^k = \alpha\alpha^{k-1} = a_1\alpha^m + a_2\alpha^{m-1}\cdots + a_m\alpha \in M.$$

The lemma is proved. □

Lemma 2.7. *Let $\mathbb{D}$ be an order in a number field K. Let $\alpha_1, \ldots, \alpha_p \in R_K$. Then the polynomial ring $\mathbb{D}[\alpha_1, \ldots, \alpha_p]$ is an order in K.*

Proof. We first show that $\mathbb{D}[\alpha]$ is an order, for $\alpha \in R_K$. Let $\omega_1, \ldots, \omega_n$ be a basis for $\mathbb{D}$. From the previous lemma we can find integers such that $\alpha^k = a_0 + a_1\alpha + \cdots + a_{m-1}\alpha^{m-1}$ for any $k \geq 0$. An element of $\mathbb{D}[\alpha]$ can be written as a linear combination of elements on the form $\omega_i\alpha^j$, with $1 \leq i \leq n$, $0 \leq j \leq m-1$. Hence $\mathbb{D}[\alpha]$ is a finitely generated module. Since $\mathbb{D} \subseteq \mathbb{D}[\alpha]$, we see that it is a full module in K and thus an order. Repeating this procedure yields the lemma. □

Proof of theorem. Let $\mathbb{D}$ be an order. Take two elements $\alpha, \beta \in R_K$. From the previous lemma, $\mathbb{D}[\alpha, \beta]$ is an order. Lemma 2.4 states that elements of an order lies in R_K, and we get $\mathbb{D}[\alpha, \beta] \subseteq R_K$. Then $\alpha - \beta$ and $\alpha\beta$ are in R_K, which shows that R_K is a ring. Since $\mathbb{D} \subseteq R_K$, we know that R_K contains n linearly independent elements. It remains to show that it is finitely generated.

Let $\omega_1, \ldots, \omega_n$ be a basis for $\mathbb{D}$. There exists a set of elements $\omega_1^*, \ldots, \omega_n^* \in K$ such that $\mathrm{Tr}(\omega_i\omega_i^*) = 1$, $\mathrm{Tr}(\omega_i\omega_j^*) = 0$ for $i \neq j$. Consider the $\mathbb{Z}$-module $\mathbb{D}^*$ generated by $\omega_1^*, \ldots, \omega_n^*$. Let $\alpha \in R_K$ be any element. Since it is contained in K we can find rational numbers c_i such that

$$\alpha = c_1\omega_1^* + \cdots + c_n\omega_n^*$$

We multiply with ω_i and take traces.

$$\mathrm{Tr}(\alpha\omega_i) = c_1\mathrm{Tr}(\omega_i\omega_1^*) + \cdots + c_n\mathrm{Tr}(\omega_i\omega_n^*) = c_i$$

Since $\alpha\omega_i \in \mathbb{D}[\alpha]$ we can use Lemma 2.4 and get that c_i is an integer, for each i. Hence the element α is in $\mathbb{D}^*$ and $R_K \subseteq \mathbb{D}^*$ is a submodule. Since $\mathbb{D}^*$ is noetherian, any submodule is finitely generated. The theorem is proved. □

2.4 Finiteness of class number

Let $\mathbb{D}$ be an order in a number field. Similar modules have the same coefficient ring, so consider classes of similar modules in this field. The number of such classes that has $\mathbb{D}$ as coefficient ring is called the *class number of the order* $\mathbb{D}$. If R_K is the maximal order of K, we say that the *class number of the field* K is the class number of R_K.

This section is devoted to proving the following important theorem.

Theorem 2.8. *Let $\mathbb{D}$ be any fixed order in the algebraic number field K. There are only finitely many non-similar modules in K which has $\mathbb{D}$ as coefficient ring, i.e. the class number of $\mathbb{D}$ is finite.*

We first state two lemmas from the general group and module theory.

Lemma 2.9. *Let M be a free abelian group of rank n. Let $M_0 \subseteq M$ be a subgroup also with rank n. Then the index $(M : M_0)$ is finite and equals the absolute value of the determinant of the transition matrix from a basis for M to a basis of M_0.*

Lemma 2.10. *Let M be a full module in a number number field K. Then for a fixed positive integer n, there are only a finite number of submodules $M_0 \subseteq M$ such that the index $(M_0 : M) = n$.*

Earlier we defined the norm of an element. We will now look at the norm of a module. Let K be an algebraic number field. Let $M = \{\mu_1, \ldots, \mu_n\}$ be a full module with coefficient ring $\mathbb{D}_M = \{\omega_1, \ldots, \omega_n\}$. We define a matrix (a_{ij}) as the transition matrix between these bases

$$\mu_j = \sum_{i=1}^{n} a_{ij}\omega_i.$$

Any two bases for a module are connected by a matrix with determinant ± 1. Hence the determinant of (a_{ij}) is not depended on the bases chosen, up to sign, and we define *the norm of the module* M as $\mathrm{N}(M) = |\det(a_{ij})|$.

For a full module M we will now define its discriminant. Let $\mu_1, \ldots, \mu_n$ be a basis for M. Consider the matrix

$$(\mathrm{Tr}(\mu_i\mu_j)) \text{ where } 1 \leq i, j \leq n$$

We define *the discriminant of the module* M to be the determinant of this matrix and we write $D(M) = \det(\mathrm{Tr}(\mu_i\mu_j))$. Using the same argument as when we defined the norm of a module, we see that the discriminant is not dependent on the basis chosen for M.

Lemma 2.11. *Let M and αM be two similar modules. Then*

$$\mathrm{N}(\alpha M) = |\mathrm{N}(\alpha)|\mathrm{N}(M)$$

Proof. Write $M = \{\mu_1, \ldots, \mu_n\}$, $\alpha M = \{\alpha\mu_1, \ldots, \alpha\mu_n\}$. These similar modules have the same coefficient ring, $\mathbb{D}$. Let A be the transition matrix from the first basis to the second. Let B and C be the transition matrices from any basis of the coefficient ring to the bases μ_i and $\alpha\mu_i$, respectively. Now the lemma follows from the fact that $C = BA$, and $\det(A) = \mathrm{N}(\alpha)$. □

Let K be an algebraic number field of degree n. Then there are n distinct embeddings of K into $\mathbb{C}$. For a complex embedding, we can always take its complex conjugate, and get a distinct embedding. Therefore the complex embeddings come in pair. We write $2t$ for the number of complex embeddings and s for the number of real.

Lemma 2.12. *Let $K/\mathbb{Q}$ have degree $n = 2t + s$. Let M be a full module in K with discriminant D. Then there exist a non-zero element $\alpha \in M$ such that*

$$|\mathrm{N}(\alpha)| \leq (\frac{2}{\pi})^t \sqrt{|D|}$$

Proof. Let ϵ be any positive real number. We can find positive real numbers $c_1, \ldots, c_{s+t}$ such that

$$c_1 \ldots c_{s+t} = (\frac{2}{\pi})^t \sqrt{|D|} + \epsilon.$$

We now use Minkowski's Lemma (see Chapter 2, Section 4 of [3]), which ensures that we can find a non-zero number $\alpha \in M$ satisfying

$$\begin{aligned} |\sigma_k(\alpha)| &< c_k \quad \text{for} \quad 1 \leq k \leq s \\ |\sigma_{s+j}(\alpha)|^2 &< c_{s+j} \quad \text{for} \quad 1 \leq j \leq t \end{aligned}$$

where σ_i are the different embeddings. We then get

$$|\mathrm{N}(\alpha)| = |\sigma_1(\alpha)| \ldots |\sigma_s(\alpha)||\sigma_{s+1}(\alpha)|^2 \ldots |\sigma_{s+t}(\alpha)|^2 < c_1 \ldots c_{s+t}$$

Since this holds for arbitrary small ϵ, there must be such an α and the lemma is proved. □

Proof of Theorem 2.8. Let M be any module with $\mathbb{D}$ as coefficient ring. Let D be the discriminant of M and D_0 the discriminant of $\mathbb{D}$. It can be shown that there is a simple connection between these discriminants, given by

$$D = D_0 \mathrm{N}(M).$$

Using this and the previous lemma, we get

$$|\mathrm{N}(\alpha)| \leq (\frac{2}{\pi})^t \mathrm{N}(M) \sqrt{|D_0|}.$$

We now use Lemma 2.9 and get

$$(\frac{1}{\alpha} M : \mathbb{D}) = \mathrm{N}(\frac{1}{\alpha} M)^{-1} = \frac{|\mathrm{N}(\alpha)|}{\mathrm{N}(M)} \leq (\frac{2}{\pi})^t \sqrt{|D_0|}.$$

Consider now all the cases where $(\frac{1}{\alpha} M : \mathbb{D}) = r$, where $r \leq (\frac{2}{\pi})^t \sqrt{|D_0|}$ is a fixed integer. It follows that $\frac{1}{\alpha} M \subseteq \frac{1}{r} \mathbb{D}$ and we get

$$\mathbb{D} \subseteq \frac{1}{\alpha} M \subseteq \frac{1}{r} \mathbb{D}.$$

From Lemma 2.10 we get that there can only be a finite number of modules $\frac{1}{\alpha} M$ such that this is satisfied. By adjusting r to count for all the cases, we still end up with a finite number of modules. Any module M which has $\mathbb{D}$ as coefficient ring is similar to one of the modules in this finite set. The theorem is proved. □

2.5 Orders in quadradic fields

Algebraic number fields of degree 2 will be of special interest to us. Let K be such a field. It is clear that $K = \mathbb{Q}(\sqrt{d})$ for some square-free $d \in \mathbb{Z}$. Let us now consider the maximal order R_K of $\mathbb{Q}(\sqrt{d})$. An element $\alpha \in \mathbb{Q}(\sqrt{d})$ can be written as

$$\alpha = a + b\sqrt{d}$$

with $a, b \in \mathbb{Q}$. Since its characteristic polynomial is

$$x^2 - 2ax + a^2 - db^2.$$

we need $2a$ and $a^2 - db^2$ to be integers. Some simple calculations give us the following theorem.

Theorem 2.13. *Let $d \neq 1$ be a square-free integer. Let R_K be the maximal order of the quadratic field $\mathbb{Q}(\sqrt{d})$. We can then take the following as a basis for R_K*

$$\{1, \omega\} \text{ where } \begin{cases} \omega = (1+\sqrt{d})/2 & \text{if} \quad d \equiv 1 \pmod 4 \\ \omega = \sqrt{d} & \text{if} \quad d \equiv 2, 3 \pmod 4 \end{cases}$$

Further, any order is on the form $\{1, f\omega\}$, where f is a positive integer.

We now look at classes of similar modules in quadratic fields. Any module $\{\alpha, \beta\}$ is similar to a module $\{1, \gamma\}$, by simply setting $\gamma = \beta/\alpha$. We will therefore focus on the modules on this form.

Let γ be any irrational number in the field $\mathbb{Q}(\sqrt{d})$. Then there exist integers a, b, c such that $a\gamma^2 + b\gamma + c = 0$. If we require these integers to have no common divisors and $a > 0$, this induces a unique polynomial

$$\phi_\gamma(t) = at^2 + bt + c.$$

We say that the integers (a, b, c) corresponds to the element γ.

Theorem 2.14. *Let $\gamma \in \mathbb{Q}(\sqrt{d})$ with $\phi_\gamma(t) = at^2 + bt + c$. Then the module $M = \{1, \gamma\}$ has coefficient ring $\mathbb{D}_M = \{1, a\gamma\}$. Further, the discriminant of $\mathbb{D}_M$ is $b^2 - 4ac$ and the norm of M is $1/a$.*

Proof. Let $\alpha \in M$ be any element. We write $\alpha = x + y\gamma$ with $x, y \in \mathbb{Q}$. Recall that $\alpha \in \mathbb{D}_M$ is equivalent to $\alpha M \subseteq M$. $\alpha M \subseteq M$ if and only if

$$\alpha 1 = x + y\gamma \in M$$

and

$$\alpha\gamma = x\gamma + y\gamma^2 = -\frac{cy}{a} + (x - \frac{by}{a})\gamma \in M.$$

Thus we require $x, y, \frac{by}{a}, \frac{cy}{a}$ to be integers. But since a, b and c does not have common divisors, we see that a must divide y. It follows that $\mathbb{D}_M = \{1, a\gamma\}$.

A straigthforward calculation proves the rest of the theorem. □

We will now look at all the modules which have the same fixed coefficient ring, $\mathbb{D}$. Recall from the previous section that these modules are divided into a finite number of equivalence classes. We will show that one can define a multiplication on these classes, and this makes the set of classes into a finite abelian group.

Let $M = \{\alpha, \beta\}$ and $M_1 = \{\alpha_1, \beta_1\}$ be modules. We define multiplication of modules as the element-wise multiplication. The product will again be a module, independent of the bases chosen and generated by $\{\alpha\alpha_1, \alpha\beta_1, \beta\alpha_1, \beta\beta_1\}$. We write MM_1 for the product of M and M_1.

Lemma 2.15. *Let M be a full module in a quadratic field K, with coefficient ring $\mathbb{D}$. Define the* conjugate module $\overline{M}$ *to consist of the complex conjugates of all the elements of M. Then $\overline{M}$ is a full module with coefficient ring $\mathbb{D}$. We also have the following relation.*

$$M\overline{M} = \mathrm{N}(M)\mathbb{D}$$

Proof. Let $M = \{\alpha, \beta\}$. Any element $\overline{\gamma} \in \overline{M}$ is on the form $\overline{\gamma} = a\overline{\alpha} + b\overline{\beta}$, where a and b are integers. $\overline{M}$ is clearly a full module. We have

$$\gamma \in \mathbb{D}_M \Leftrightarrow \overline{\gamma} \in \overline{\mathbb{D}_M}.$$

Using Theorem 2.13, simple arithmetics shows that the conjugate of an order, is the same order. Hence, $\overline{\gamma} \in \mathbb{D}_M$ and the coefficient rings of M and its conjugate coincide.

To prove the last part of the lemma, we first assume that $M = \{1, \gamma\}$. We use the notation in Theorem 2.14 and observe that $\phi_\gamma = \phi_{\overline{\gamma}}$. Then

$$\begin{aligned} M\overline{M} &= \{1,\gamma\}\{1,\overline{\gamma}\} \\ &= \{1,\gamma,\overline{\gamma},\gamma\overline{\gamma}\} \\ &= \{1,\gamma,-\gamma-\frac{b}{a},\frac{c}{a}\} \\ &= \{1,\gamma,\frac{b}{a},\frac{c}{a}\} \\ &= \frac{1}{a}\{a,b,c,a\gamma\} \\ &= \frac{1}{a}\{1,a\gamma\}, \end{aligned}$$

where the last equality follows from the fact that $\mathrm{g.c.d}(a,b,c) = 1$. From Theorem 2.14 we get

$$M\overline{M} = \frac{1}{a}\{1,a\gamma\} = \frac{1}{a}\mathbb{D}_M = \mathrm{N}(M)\mathbb{D}_M.$$

We now show this for any module N. We can write $N = \alpha\{1,\gamma\} = \alpha M$. From 2.11 we get

$$N\overline{N} = \alpha M\overline{\alpha}\overline{M} = \alpha\overline{\alpha}\mathrm{N}(M)\mathbb{D}_M = |\mathrm{N}(\alpha)|\mathrm{N}(M)\mathbb{D}_M = \mathrm{N}(\alpha M)\mathbb{D}_M = \mathrm{N}(N)\mathbb{D}_N.$$

This completes the proof. □

Lemma 2.16. *Let $\mathbb{D}$ be a fixed order in a quadratic field. The set of modules which has $\mathbb{D}$ as coefficient ring, becomes an abelian group with the multiplication defined above.*

Proof. Let the modules M and M_1 both have $\mathbb{D}_1$ as coefficient ring. Let the product MM_1 have coefficient ring $\mathbb{D}_2$. We use the previous lemma and get

$$MM_1\overline{MM_1} = \mathrm{N}(MM_1)\mathbb{D}_2.$$

Since multiplication is associative and commutative, we can also write

$$MM_1\overline{MM_1} = M\overline{M}M_1\overline{M_1} = \mathrm{N}(M)\mathrm{N}(M_1)\mathbb{D}_1$$

But the norm of a module is simply a number, so comparing these two equations, we get

$$a\mathbb{D}_2 = b\mathbb{D}_1$$

So, these two orders are similar, which means that they must be equal (Theorem 2.13). Hence, this multiplication preserves the coefficient ring. Also observe that $\mathbb{D}_1$ acts as the identity element, and $\overline{M}/\mathrm{N}(M)$ is the inverse of M. This proves the lemma. □

Theorem 2.17. *Let $\mathbb{D}$ be a fixed order in a quadratic number field. The set of equivalence classes of similar modules which have $\mathbb{D}$ as coefficient ring becomes a finite abelian group with multiplication defined above.*

Proof. For any module M, we let $[M]$ be its equivalence class of similar modules. Observe that $(\alpha M)(\beta M_1) = \alpha\beta(MM_1)$, and we define multiplication of equivalence classes as

$$[M][M_1] = [MM_1]$$

where we choose any representative for the class. Using the previous Lemma and Theorem 2.8, we have proved this Theorem. □

2.6 Class number of an imaginary quadratic field

We now turn our focus towards imaginary quadratic fields. We have seen that for orders in number fields, the class number is finite. We will in this section show how one can compute this number for imaginary quadratic field. We start by introducing reduced modules, which will act as unique representatives for our equivalence classes.

Definition 2.18. Let ω_1 and ω_2 be two complex numbers which are linearly independent over $\mathbb{R}$. Then a lattice corresponding to $\{\omega_1, \omega_2\}$ is the discrete subgroup of $\mathbb{C}$ defined by the set

$$\{\omega_1 a + \omega_2 b \colon a, b \in \mathbb{Z}\}$$

Two lattices, M and M_1, are *similar* if there exists an element $\gamma \in \mathbb{C}$ such that $M = \gamma M_1$.

For a lattice M, we can find a special basis, called *the reduced basis*. This is the basis made up of the shortest vector $\alpha \in M$ and the shortest vector $\beta \in M$ which is not collinear to α. This basis is unique up to rotations which takes the lattice onto itself.

Lemma 2.19. *Let M and M_1 be lattices in $\mathbb{C}$. If M and M_1 are similar then their reduced bases can be transformed onto each other by a rotation and a scaling.*

Proof. Let α, β be a reduced basis for M and α_1, β_1 for M_1. Let $\xi M = M_1$. It follows that $\xi\alpha, \xi\beta$ is a reduced basis for M_1. Hence we can obtain this basis from a rotation of α_1, β_1. Let $\nu \in \mathbb{C}$ correspond to this rotation. Then $\nu\xi\alpha = \alpha_1$, $\nu\xi\beta = \beta_1$. Hence the basis given by α_1 and β_1 is obtained by a rotation with the angle $\arg(\nu\xi)$ and multiplication by the scalar $|\nu\xi|$. The Lemma follows. □

Definition 2.20. Let K be an imaginary quadratic field. An element $\gamma \in K$ is *reduced* if the following is satisfied

$$\begin{array}{lll} \mathfrak{Im}\gamma > 0 & & \\ -\frac{1}{2} < \mathfrak{Re}\gamma \leq \frac{1}{2} & & \\ |\gamma| > 1 & \text{if} & -\frac{1}{2} < \mathfrak{Re}\gamma < 0 \\ |\gamma| \geq 1 & \text{if} & 0 \leq \mathfrak{Re}\gamma \leq \frac{1}{2} \end{array} \tag{F}$$

We further say that the module M is *reduced* if $M = \{1, \gamma\}$ and γ is reduced.

Theorem 2.21. *Each equivalence class in an imaginary quadratic number field contains one and only one reduced module.*

Proof. Let M be a module in the field $\mathbb{Q}(\sqrt{d})$, where $d < 0$. We can consider M as a lattice of the complex plane. Let α, β form a reduced basis for the lattice M. From geometric considerations we get that the similar module $\frac{1}{\alpha}M = \{1, \gamma\}$, is a reduced module. This shows that any equivalence class has a module on reduced form. We now turn to the uniqueness.

Let $\gamma = x + yi$ be reduced. If we consider all the vectors on the form $k + l\gamma$, a small calculation shows that γ is the shortest of these that are not on the real line. This means that 1 and γ forms a reduced basis for the lattice $\{1, \gamma\}$. Let γ and γ_1 be reduced numbers with the module $\{1, \gamma\}$ similar to $\{1, \gamma_1\}$. Since these modules are similar as lattice, Lemma 2.19 says that we can transform the basis $\{1, \gamma\}$ into $\{1, \gamma_1\}$ by multiplying with a complex number. But this clearly implies that $\gamma = \gamma_1$, and the reduced module is unique. □

We now look at how we can find these reduced forms. For the imaginary quadratic field, $\mathbb{Q}(\sqrt{d})$, we fix an order $\mathbb{D}$ with discriminant $D < 0$. Let $M = \{1, \gamma\}$ be any module on reduced form with coefficient ring equal to $\mathbb{D}$. Let (a, b, c) be the integers corresponding to γ. We can then write, using the notation from Theorem 2.14,

$$\begin{array}{l} \gamma = \frac{-b+\sqrt{D}}{2a} \\ D = b^2 - 4ac. \end{array} \tag{$*$}$$

From the conditions of γ being reduced, we get the following restrictions on a, b and c.

$$\begin{array}{lll} -a \leq b < a & & \\ c \geq a & \text{for} & b \leq 0 \\ c > a & \text{for} & b > 0 \end{array} \tag{$**$}$$

Solutions to $(*)$ and $(**)$ give us all reduced modules with $\mathbb{D}$ as coefficient ring. From these equations, we also deduce the following bound for a and b

$$|b| \leq a < \sqrt{\frac{-D}{3}}$$

From this, it follows that there can only be a finite number of reduced modules with $\mathbb{D}$ as coefficient ring. But it also gives us an opportunity to find these modules. We show this in an example.

Example 2.22. We consider the imaginary field $\mathbb{Q}(\sqrt{-15})$. Its maximal order is $\{1, \omega\}$, $\omega = \frac{1+\sqrt{-15}}{2}$, with discriminant $D = -15$. We now calculate the reduced modules with coefficient ring equal to this order. We use the above restrictions and get

$$|b| \leq a < \sqrt{-D/3} = \sqrt{5}.$$

If b is even, we get that $c = (b^2 - D)/4a$ is not an integer, for $D = -15$. Since $b < a \leq 2$, we end up with the following possible cases

$$b = \pm 1, \quad a = 2, \quad c = \frac{1+15}{8} = 2$$
$$b = -1, \quad a = 1, \quad c = \frac{1+15}{4} = 4$$

The case $b = +1$, $a = 2$, $c = 2$ must be discarded since it violates the above conditions. This means that we have two reduced modules which have $\{1, \omega\}$ as coefficient ring, $\{1, \gamma_1\}$ and $\{1, \gamma_2\}$ where

$$\gamma_1 = \frac{1+\sqrt{-15}}{4}$$
$$\gamma_2 = \frac{1+\sqrt{-15}}{2}.$$

Thus, we have found 2 reduced modules, and the class number of the maximal order of $\mathbb{Q}(\sqrt{-15})$ is 2.

The class number for the maximal order is called the *class number of the field*. We show later that it can also be defined as the number of divisor classes of the field.

3 Divisors and Valuations

3.1 Divisors

Let $\mathbb{D}$ be an integral domain. $\mathbb{D}$ may or may not have unique factorization in prime factors. We wish to create a semi-group $\mathscr{D}$ with unique factorization and a mapping

$$\begin{aligned}(-)\colon \mathbb{D}^* &\to \mathscr{D} \\ \alpha &\mapsto (\alpha),\end{aligned}$$

such that we can study the structure of $\mathbb{D}$ by the prime decomposition in $\mathscr{D}$.

It is clear that we need this mapping to be a homomorphism, so that $(\alpha\beta) = (\alpha)(\beta)$. Hence if α divides β in $\mathbb{D}$, (α) divides (β) in $\mathscr{D}$. We also want the converse to be true. We say that $\mathfrak{a} \in \mathscr{D}$ divides $\alpha \in \mathbb{D}$ if $\mathfrak{a}$ divides the image (α), and we write $\mathfrak{a}|\alpha$.

The elements that are divisible by the element α in $\mathbb{D}$ are closed under addition. We wish to preserve this property in $\mathscr{D}$.

We also wish to make $\mathscr{D}$ as small as possible. Hence if two elements of $\mathscr{D}$ divide the same set of elements, they must be equal. We formalize this in the following definition.

Definition 3.1. Let $\mathbb{D}$ be an integral domain. $\mathbb{D}$ has a *divisor construction* if there is a semi-group $\mathscr{D}$ with unique factorization and a homomorphism $\mathbb{D}^* \to \mathscr{D}$ that satisfies the following for all $\alpha, \beta \in \mathbb{D}^*$ and $\mathfrak{a}, \mathfrak{b} \in \mathscr{D}$.

(a) $\alpha|\beta$ if and only if $(\alpha)|(\beta)$,

(b) if $\mathfrak{a}|\alpha$ and $\mathfrak{a}|\beta$, then $\mathfrak{a}|\alpha \pm \beta$,

(c) let $A \subseteq \mathbb{D}$ be the set of elements that are divisible by $\mathfrak{a}$ and $B \subseteq \mathbb{D}$ the set of elements divisible by $\mathfrak{b}$. If $A = B$, then $\mathfrak{a} = \mathfrak{b}$.

The elements of $\mathscr{D}$ are called divisors, and the elements on the form (α) principal divisors. An element of $\mathscr{D}$ is called a prime divisor if its only divisible by itself and by the units of $\mathscr{D}$.

Not all domains have a divisor construction. However, we now show that if a divisor construction exists, it will be unique.

Theorem 3.2. *Let $\mathbb{D}$ be a domain. If there are two divisor constructions $\mathbb{D}^* \to \mathscr{D}$ and $\mathbb{D}^* \to \mathscr{D}'$, then there exists an isomorphism $\mathscr{D} \to \mathscr{D}'$ in which principal divisors corresponding to the same element in $\mathbb{D}$ are identified.*

Proof. For prime divisors $\mathfrak{p} \in \mathscr{D}$ and $\mathfrak{p}' \in \mathscr{D}'$ we define corresponding sets

$\overline{\mathfrak{p}} \subseteq \mathbb{D}^*$: set of elements divisible by $\mathfrak{p}$ with respect to the divisor construction $\mathbb{D}^* \to \mathscr{D}$.
$\overline{\mathfrak{p}'} \subseteq \mathbb{D}^*$: set of elements divisible by $\mathfrak{p}$ with respect to the divisor construction $\mathbb{D}^* \to \mathscr{D}'$.

Let $\mathfrak{p}' \in \mathscr{D}'$ be a prime divisor. Assume that $\overline{\mathfrak{p}}$ is not contained in $\overline{\mathfrak{p}'}$ for all $\mathfrak{p} \in \mathscr{D}$. Choose a non-zero element $\beta \in \mathbb{D}$ such that $\mathfrak{p}'|\beta$. (Property (c) of Definition 3.1 ensures

that such an β exists for any divisor.) We can write $(\beta) = \mathfrak{p}_1^{k_1} \dots \mathfrak{p}_r^{k_r} \in \mathscr{D}$ for prime divisors $\mathfrak{p}_i$. From our assumption we have $\overline{\mathfrak{p}_i} \nsubseteq \overline{\mathfrak{p}}'$, hence for each i there exists $\gamma_i \in \mathbb{D}$ such that $\mathfrak{p}_i | \gamma_i$, $\mathfrak{p}' \nmid \gamma_i$. Define $\gamma = \gamma_1^{k_1} \dots \gamma_r^{k_r}$. We have $\mathfrak{p}_1^{k_1} \dots \mathfrak{p}_r^{k_r} | \gamma_1^{k_1} \dots \gamma_r^{k_r}$ which means that in the ring $\mathbb{D}$, $\beta | \gamma$. From the choice of β it follows that $\mathfrak{p}' | \gamma$. But $\mathfrak{p}'$ is prime and does not divide any of the γ_i, hence we have a contradiction and there must exist a prime divisor $\mathfrak{p}$ such that $\overline{\mathfrak{p}} \subseteq \overline{\mathfrak{p}}'$. By symmetry there is a prime divisor $\mathfrak{q}' \in \mathscr{D}'$ such that $\overline{\mathfrak{q}}' \subseteq \overline{\mathfrak{p}}$. Let $\xi \in \mathbb{D}$ be an element such that $\mathfrak{q}' | \xi$, $\mathfrak{q}'\mathfrak{p}' \nmid \xi$. By assuming that $\mathfrak{q}' \neq \mathfrak{p}'$, we get $\mathfrak{p}' \nmid \xi$. But $\overline{\mathfrak{q}}' \subseteq \overline{\mathfrak{p}} \subseteq \overline{\mathfrak{p}}'$, so the existance of such an element γ proves that $\mathfrak{q}' = \mathfrak{p}'$. This shows that we have a one-to-one correspondence between prime divisors in $\mathscr{D}$ and $\mathscr{D}'$.

Similar usage of the definition of the divisor construction gives that $(\alpha) \in \mathscr{D}$ and $(\alpha)' \in \mathscr{D}'$ corresponds to eachother, which proves the theorem. □

We have not yet shown when a domain have a divisor construction. Now we state one condition that needs to be satisfied. We first define a concept of integrality.

Definition 3.3. Let S be an integral domain. Let $R \subseteq S$ be a subring. We say that $s \in S$ is *integral* over R, if s is the root of a monic polynomial $f(X) \in R[X]$. The set of all such elements is called the *integral closure* of R in S.

Let now S be the quotient field of R. If R equals the integral closure of R in S, we say that R is *integrally closed* in S.

Theorem 3.4. *If a domain $\mathbb{D}$ has a divisor construction $\mathbb{D}^* \to \mathscr{D}$, then $\mathbb{D}$ is integrally closed in its quotient field K.*

Proof. Let $\xi \in K$ be an element which satisfies the equation

$$\xi^n + a_1\xi^{n-1} + \dots + a_n = 0,\ a_i \in \mathbb{D}.$$

Assume that $\xi \notin \mathbb{D}$. Writing $\xi = \alpha/\beta$ with $\alpha, \beta \in \mathbb{D}$, this means that $\beta \nmid \alpha$. The divisor (β) will then not divide (α) in $\mathscr{D}$, and there is a prime divisor $\mathfrak{p}$ which occour with a greater power in (β) than in (α). Say that $\mathfrak{p}^k | (\alpha)$, with $k \geq 0$, but no higher power of $\mathfrak{p}$ divides. We rewrite the above equation

$$\alpha^n = -a_1\beta\alpha^{n-1} - \dots - a_n\beta^n.$$

Since (β) is divisible by $\mathfrak{p}^{k+1}$, the right hand side is divisible by $\mathfrak{p}^{kn+1}$. However the left side is not divisible by powers of $\mathfrak{p}$ higher than kn. This contradiction proves the theorem. □

3.2 Valuations

We now define valuations on a field. Valuations are closely related to divisors, and we will study this connection.

Definition 3.5. Let K be any field. A function v

$$v\colon K \to \mathbb{Z} \cup \{\infty\}$$

is called a valuation of K if it satisfies:

(1) v is onto and $v(0) = \infty$

(2) $v(\alpha\beta) = v(\alpha) + v(\beta)$

(3) $v(\alpha + \beta) \geq \min\{v(\alpha), v(\beta)\}$

for any $\alpha, \beta \in K$.

For the field $\mathbb{Q}$, the p-adic valuations satisfies this definition. Motivated by this, we create a valuation using a divisor construction.

Consider a domain $\mathbb{D}$ with a divisor construction $\mathbb{D}^* \to \mathscr{D}$. Let $\mathfrak{p}$ be a prime divisor. We create a function $v_\mathfrak{p}$ which acts on $\mathbb{D}$. Let $\alpha \in \mathbb{D}$ be an arbitrary element. The divisor (α) can be written uniquely as $(\alpha) = \beta\mathfrak{p}^a$, where $a \geq 0$ is an integer and $\mathfrak{p}$ does not divide β. We define $v_\mathfrak{p}(\alpha) = a$. Alternatively, $v_\mathfrak{p}$ satisfies the following

$$\begin{aligned} \mathfrak{p}^{v_\mathfrak{p}(\alpha)} &| \alpha \\ \mathfrak{p}^{v_\mathfrak{p}(\alpha)+1} &\nmid \alpha \end{aligned}$$

Since arbitrary power of $\mathfrak{p}$ divides 0, we define $v_\mathfrak{p}(0) = \infty$. We can extend this to the quotient field of $\mathbb{D}$. For $\gamma = \alpha/\beta$ with $\alpha, \beta \in \mathbb{D}$ we define $v_\mathfrak{p}(\gamma) = v_\mathfrak{p}(\alpha) - v_\mathfrak{p}(\beta)$. This makes $v_\mathfrak{p}$ into a valuation of the quotient field.

This shows how we can get valuations from prime divisors. Its easily seen that distinct prime divisors, gives disctinct valuations, and that all these valuations satisfies $v_\mathfrak{p}(\alpha) \geq 0$ for any $\alpha \in \mathbb{D}$.

Let $\alpha \in \mathbb{D}^*$. The principal divisor (α) can be written as a product of prime divisor

$$(\alpha) = \prod_i \mathfrak{p}_i^{v_{\mathfrak{p}_i}(\alpha)} \tag{2}$$

where the product goes over the primes $\mathfrak{p}_i$ with $v_{\mathfrak{p}_i}(\alpha) > 0$. Since the prime divisors are in one-to-one correspondence with the valuations, all the divisors of $\mathscr{D}$ are determinded by the valuations. Using the above product we have a homomorphism $\mathbb{D}^* \to \mathscr{D}$ and thus valuations can be used to construct a divisor construction. We now state a theorem which shows when a set of valuations induce a divisor construction.

Theorem 3.6. *Let $\mathbb{D}$ be a domain with quotient field K. Let $\mathfrak{R}$ be a set of valuations on K. Then $\mathfrak{R}$ can induce a divisor construction on $\mathbb{D}$ if and only if the following is satisfied:*

(1) For any $\alpha \in \mathbb{D}^*$, $v(\alpha) = 0$ for almost all (i.e. all but a finite number of) $v \in \mathfrak{R}$.

(2) Let $\alpha \in K$. Then $\alpha \in \mathbb{D} \Leftrightarrow v(\alpha) \geq 0$ for all $v \in \mathfrak{R}$.

(3) Let $v_1, \ldots, v_m \in \mathfrak{R}$ be any set of valuations, and let $k_1, \ldots, k_m$ be any non-negative integers. Then there exist an element $\alpha \in \mathbb{D}$ such that

$$v_i(\alpha) = k_i \text{ for all } 1 \leq i \leq m$$

Proof. We first show that these conditions are necessary for $\mathfrak{R}$ to induce a divisor construction. For an element $\alpha \in \mathbb{D}$ we write as above $(\alpha) = \prod_i \mathfrak{p}_i^{v_{\mathfrak{p}_i}(\alpha)}$. So condition (1) must be satisfied.

We must also have $v(\alpha) \geq 0$ if $\alpha \in \mathbb{D}$. Now let $\xi = \alpha/\beta \in K$ with $v(\xi) \geq 0$ for all $v \in \mathfrak{R}$. Then $v(\alpha) \geq v(\beta)$, which means that $\beta|\alpha$ in $\mathbb{D}$. Hence $\xi \in \mathbb{D}$, and condition (2) must be satisfied.

Take any set $v_1, \ldots, v_m \in \mathfrak{R}$ of valuations corresponding to prime divisors $\mathfrak{p}_1, \ldots, \mathfrak{p}_m$. Let $k_1, \ldots, k_m$ be a set of integers. Define a divisor $\mathfrak{a} = \mathfrak{p}_1^{k_1} \ldots \mathfrak{p}_m^{k_m}$ and a set of divisors $\mathfrak{a}_i = \mathfrak{a}\mathfrak{p}_1 \ldots \mathfrak{p}_{i-1}\mathfrak{p}_{i+1} \ldots \mathfrak{p}_m$. We need condition (3) of Definition 3.1 to be satisfied, so there exists an element α_i such that $\mathfrak{a}_i|\alpha_i$, but $\mathfrak{a}_i\mathfrak{p} \not| \alpha_i$. By setting $\alpha = \alpha_1 + \cdots + \alpha_m$ we get $\mathfrak{p}_i^{k_i}|\alpha$, $\mathfrak{p}_i^{k_i+1} \not| \alpha$. Hence we have found an element α such that $v_i(\alpha) = k_i$ for each i.

This shows that all the three conditions are needed for a set of valuations to induce a divisor construction. We now let $\mathscr{D}$ be a semi-group with unique factorization, in which the prime divisors are in one-to-one correspondence with the valuations of $\mathfrak{R}$. We let the homomorphism $\mathbb{D}^* \to \mathscr{D}$ be defined by equation (2). It is now straight-forward to show that this satisfies the conditions needed to define a divisor construction. □

We now look at how a divisor construction for a domain behaves, if the domain already has unique factorization.

Theorem 3.7. *Let $\mathbb{D}$ be a domain. $\mathbb{D}$ has unique factorization if and only if there is a divisor construction $\mathbb{D}^* \to \mathscr{D}$ in which every divisor is principal.*

Proof. Let $\mathbb{D}$ have unique factorization. Let (α) denote the class of elements in $\mathbb{D}$ which are associates to $\alpha \in \mathbb{D}$. The mapping $\alpha \mapsto (\alpha)$ is easily seen to define a divisor construction, and all divisors are principal.

Assume that $\mathbb{D}$ has a divisor construction $\mathbb{D}^* \to \mathscr{D}$ where all divisors are principal. Let $\pi \neq 0 \in D$.

Claim: π is prime on $\mathbb{D}$ if and only if (π) is a prime divisor in $\mathscr{D}$. Proof of claim: Let $(\pi) = \mathfrak{p} \in \mathscr{D}$ be a prime divisor and let $\gamma|\pi$ in $\mathbb{D}$. Then $(\gamma)|\mathfrak{p}$ in $\mathscr{D}$ and either $(\gamma) = \mathfrak{p}$ or (γ) is the unit divisor. It follows that π must be prime in $\mathbb{D}$. Now let $(\alpha) \in \mathscr{D}$ be an element which is not prime and not the unit element. Then there exist a prime divisor (π) which divides (α). It follows that $\pi|\alpha$ and $\alpha \in D$ is not a prime. The claim is proved.

Take any $\alpha \in \mathbb{D}^*$ and write

$$(\alpha) = \mathfrak{p}_1 \ldots \mathfrak{p}_r$$

with $\mathfrak{p}_i$ prime divisors in $\mathscr{D}$. We have assumed all divisors principal, so we can find elements in $\mathbb{D}$ such that $\mathfrak{p}_i = (\pi_i)$. Using the claim it follows that we can write

$$\alpha = \epsilon\pi_1 \ldots \pi_r \in \mathbb{D}.$$

The unique factorization in $\mathscr{D}$ now induces a unique factorization in $\mathbb{D}$. □

We also have the following theorem, which states a necessary condition when $\mathbb{D}$ has unique factorization.

Theorem 3.8. *Let $\mathbb{D}$ be a domain. If there is a divisor construction for $\mathbb{D}$ with only a finite number of prime divisors, then $\mathbb{D}$ has unique factorization into primes. There is a finite set of elements $\pi_1, \ldots, \pi_m \in \mathbb{D}$ such that any element $\alpha \in \mathbb{D}$ can be written uniquely on the form*

$$\alpha = \epsilon \pi_1^{k_1} \ldots \pi_m^{k_m}$$

with ϵ a unit in $\mathbb{D}$.

Proof. Let $\mathbb{D}^* \to \mathscr{D}$ be a divisor construction with the prime divisors $\mathfrak{p}_1, \ldots \mathfrak{p}_m$. Let $v_1, \ldots, v_m$ be the corresponding valuatons on the quotient field of $\mathbb{D}$. Let $\mathfrak{a} = \mathfrak{p}_1^{k_1} \ldots \mathfrak{p}_m^{k_m}$ be any divisor. Using Theorem 3.6 we can find $\alpha \in \mathbb{D}$ such that $v_i(\alpha) = k_i$ for all i. But then $\mathfrak{a} = (\alpha)$. Hence, all divisors of $\mathscr{D}$ are principal and $\mathbb{D}$ has unique factorization from the previous theorem. We can then find elements in $\mathbb{D}$ such that $(\pi_i) = \mathfrak{p}_i$ for all i. It follows that the set of elements $\pi_1, \ldots, \pi_m$ are all the prime factors of $\mathbb{D}$ up to associates. π_i is characterized by $v_i(\pi_i) = 1$ and $v_j(\pi_i) = 0$ for all $j \neq i$. □

We now get back to valuations and explore some properties surrounding them. Theorem 3.6 will be very important.

Definition 3.9. Let v be a valuation of a field K. We define the *valuation ring* of v

$$\mathbb{D}_v = \{\alpha \in K \colon v(\alpha) \geq 0\} \subseteq K$$

We note that $\mathbb{D}_v$ has a divisor construction with only one prime divisor, corresponding to v. We also have the following theorem.

Theorem 3.10. *Let $\mathbb{D}_v$ be the valuation ring corresponding to the valuation v in K. $\mathbb{D}_v$ is integrally closed in K.*

Proof. If K equals the quotient field of $\mathbb{D}_v$, we can use Theorem 3.4.

The quotient field of $\mathbb{D}_v$ is the smallest field k such that $\mathbb{D}_v \subseteq k$. It is clear that $k \subseteq K$, and we need to show equality. Let $\alpha \in K$ be any element, we will now show that α must be in k. If $\alpha \in \mathbb{D}_v$, then $\alpha \in k$. Assume $\alpha \notin \mathbb{D}_v$, so there is a positive m such that $v(\alpha) = -m$. Pick an element $\beta \in \mathbb{D}_v \subseteq k$ with $v(\beta) > m$. From the definition of valuations we get $v(\alpha\beta) = v(\alpha) + v(\beta) > 0$. So the product $\alpha\beta \in \mathbb{D}_v \subseteq k$. But k is a field, so $\beta^{-1} \in k$. It follows that $\alpha \in k$ and $k = K$. The theorem is proved. □

Part (3) of Theorem 3.6 shows that valuations corresponding to prime divisors are independent. We now show that this property holds for any finite set of valuations, regardless of a divisor construction.

Theorem 3.11. *Let $v_1, \ldots, v_m$ be distinct valuations of a field K. For any set $k_1, \ldots, k_m$ of integers, there exists an element $\gamma \in K$ such that $v_i(\gamma) = k_i$ for all $1 \geq i \geq m$.*

Before we prove this theorem, we state a corollary which will be usefull.

Corollary 3.12. *Let $v_1, \ldots, v_m$ be distinct valuations of K and let $\mathbb{D}_1, \ldots, \mathbb{D}_m$ be the corresponding valuation rings. Then the intersection $\mathbb{D} = \bigcap_{i=1}^{m} \mathbb{D}_i$ is a ring with unique factorization. There are elements π_i such that $v_i(\pi_i) = 1$, $v_i(\pi_j) = 0$ for $i \neq j$ and any element $\alpha \in \mathbb{D}$ can uniquely be written as*

$$\alpha = \epsilon \pi_1^{k_1} \ldots \pi_m^{k_m}$$

with ϵ a unit in $\mathbb{D}$.

Proof. Condition (1) and (2) of Theorem 3.6 are easily seen to be fulfilled for $\mathbb{D}$ and the valuations $v_1, \ldots, v_m$. Assuming this theorem holds, condition (3) also holds. So $\mathbb{D}$ has a divisor construction with a finite number of prime divisors. Using Theorem 3.8 the corollary is proved. □

Proof of Theorem. We will prove this by induction on the number of valuations. If $m = 1$ the theorem follows from the defintion of valuations. Let $m \geq 2$ and assume that the theorem is proved for $m - 1$ valuations.

We now assume that for any $\gamma \in K$ there exist integers $c_1, \ldots, c_m$, not all zero, such that

$$c_1 v_1(\gamma) + \cdots + c_m v_m(\gamma) = 0 \tag{3}$$

It is clear that atleast two of the c_i's must be non-zero. We now show that two of the coefficients must have the same sign. If this is not the case, we must be in the situation that we only have two non-zero coefficients, say c_1 and c_2, with $c_1 < 0$ and $c_2 > 0$. Then

$$c_1 v_1(\gamma) + c_2 v_2(\gamma) = 0$$

and setting $e = -\frac{c_1}{c_2} > 0$ we have

$$v_2(\gamma) = e v_1(\gamma).$$

The surjectivity of valuations leads to $e = 1$ and thus $v_1 = v_2$. This contradiction shows that we can write (3) as

$$v_1(\gamma) = a_2 v_2(\gamma) + \cdots + a_m v_m(\gamma)$$

with $a_i \in \mathbb{Q}$ and at least one $a_i < 0$. By induction we can find elements $\beta, \beta' \in K$ such that

$$\begin{aligned} v_i(\beta) = 0 \quad v_i(\beta') = 1 \quad &\text{if } a_i \geq 0 \\ v_i(\beta) = 1 \quad v_i(\beta') = 0 \quad &\text{if } a_i < 0 \end{aligned}$$

for $i = 2, \ldots, m$. From the above equation for v_1 we get $v_1(\beta) < 0$ and $v_1(\beta') \geq 0$. Since $v_i(\beta + \beta') = \min(v_i(\beta), v_i(\beta')) = 0$ for all $i \geq 2$, we get that $v_1(\beta + \beta') = 0$. But we also have

$$v_1(\beta + \beta') = \min(v_1(\beta), v_1(\beta')) = v_1(\beta) < 0.$$

The contradiction proves that (3) is impossible.

We have assumed that the theorem is proved for the $m-1$ valuations $v_2, \dots, v_m$. Thus the corollary is also true for these valuations. We follow the notation in the corollary with these valuations. We also define E to be the set of units in the intersection ring $\mathbb{D}$. For any $\xi \in K^*$ we write

$$\xi = \epsilon \pi_2^{k_2} \dots \pi_m^{k_m}$$

with $\epsilon \in E$. Assume that $v_1(\epsilon) = 0$. Then

$$v_1(\xi) = k_2 v_1(\pi_2) + \dots + k_m v_1(\pi_m) = a_2 v_2(\xi) + \dots a_m v_m(\xi)$$

where $a_i = v_1(\pi_i)$. But this equation is on the form given in (3), and there must be an element $\epsilon \in K$ with $v_1(\epsilon) \neq 0$.

Take the element $\gamma \in E$ in which v_1 takes the smallest positive value l. It is clear that for every element $\gamma' \in E$, $l | v_1(\gamma')$. As above we set $a_2 = v_1(\pi_2), \dots, a_m = v_1(\pi_m)$. Assume that one of these is not divisible by l, say a_2. Consider the element

$$\alpha = \pi_2 (\pi_3 \dots \pi_m)^l \gamma^s$$

where $s \in \mathbb{Z}$ is chosen such that

$$a_2 + l(a_3 + \dots + a_m) + sl = l_1$$

satisfies $0 < l_1 < l$. We then have

$$\begin{aligned} v_1(\alpha) &= l_1 \\ v_i(\alpha) &> 0 \text{ for } i = 2, \dots, m \end{aligned}$$

We set $\epsilon = \gamma + \alpha$ and see that $v_i(\epsilon) = 0$ for all $i = 2, \dots, m$. Hence $\epsilon \in E$. But we also have

$$v_1(\epsilon) = \min(v_1(\gamma), v_1(\alpha)) = \min(l, l_1) = l_1 < l$$

This shows that all the a_i's are divisible by l. It follows that l must divide $v_1(\xi)$ for any $\xi \in K^*$. This is only possible for $l = 1$.

We now replace our prime elements by setting $\pi_i' = \pi_i \gamma^{-a_i}$, $i = 2, \dots, m$. Then $v_1(\pi_i') = 0$ for all $i = 2, \dots, m$. We set $\pi_1' = \gamma$ and get a set of elements such that $v_i(\pi_i) = 1$ and $v_j(\pi_i) = 0$ for $i \neq j$. We can now for any set of integers $k_1, \dots, k_m$ make the element $\xi = \pi_1'^{k_1} + \dots + \pi_m'^{k_m}$ and get

$$v_i(\xi) = k_i \text{ for all } i = 1, \dots, m$$

The theorem is proved. □

3.3 Extensions of valuations

Let k be a field and let K be a finite extension of k. If v is a valuation of K, we can look at the restriction of v to k. We first show that v can not be identically zero on k. Assume that $v(\alpha) = 0$ for all $\alpha \in k$. Then k is contained in the valuation ring $\mathbb{D}_v$.

But the minimal polynomial for α has coefficients in k, hence in $\mathbb{D}_v$. This means that α is integral, but $\mathbb{D}_v$ is integrally closed. It follows that $\alpha \in \mathbb{D}_v$ and $K \subseteq \mathbb{D}_v$. This is impossible. So v takes on non-zero values, and if $v(\alpha) > 0$ then $v(\alpha^{-1}) < 0$. Let e be the smallest positive value v takes on k. Then it is easily seen that for any non-zero $\alpha \in k$, $e|v(\alpha)$. We define

$$\begin{aligned} v_0(a) &= \tfrac{v(a)}{e} \quad \text{for any } 0 \neq \alpha \in k \\ v_0(0) &= \infty \end{aligned}$$

This makes v_0 a valuation of k, and we say that v_0 is induced from v. We also say that v is an extension of v_0. The number e is the *ramification index* of v with respect to v_0.

Theorem 3.13. *Let v_0 be a valuation of a field k, and let K be a finite extension of k of degree n. Then v_0 can be extended to K, and the number of such extensions is at most n.*

Theorem 3.14. *Let $\mathfrak{d}$ be the valuation ring of v_0 and let $\mathbb{D}$ be its integral closure in K. Let $v_1, \ldots, v_m$ be all the extensions of v_0 in K, with corresponding valuation rings $\mathbb{D}_1, \ldots, \mathbb{D}_m$. Then*

$$\mathbb{D} = \bigcap_{i=1}^{m} \mathbb{D}_i$$

Proof. We choose not to include proofs of these two Theorems, and refer the reader to Section 3.4 of [3]. □

Lemma 3.15. *Let $\mathfrak{d}$ be an integrally closed domain in its quotient field k. Let K be a finite extension of k. Then any $\alpha \in K$ is integral over $\mathfrak{d}$ if and only if the minimal polynomial of α lie in $\mathfrak{d}[x]$.*

Proof. Let $f(x) \in k[x]$ be the minimal polynomial of α.

If f has all its coefficients in $\mathfrak{d}$, it follows from the definition that α is integral over $\mathfrak{d}$.

Now let α be integral over $\mathfrak{d}$, say α is a root of the monic polynomial $g(x) \in \mathfrak{d}[x]$. It is clear that $g(x)$ is divisible by the minimal polynomial $f(x)$. $g(x)$ splits into linear factors in $\overline{K}$, the algebraic closure of K. Let $\mathbb{D}$ be the integral closure of $\mathfrak{d}$ in $\overline{K}$. All the roots of $g(x)$ are then clearly in $\mathbb{D}$, and it follows that all the roots of $f(x)$ are also in $\mathbb{D}$. Hence $f(x) \in \mathbb{D}[x]$. But $f(x) \in k[x]$ and since $\mathfrak{d}$ is integrally closed $k \cap \mathbb{D} = \mathfrak{d}$, it follows that $f(x) \in \mathfrak{d}[x]$. The lemma is proved. □

Theorem 3.16. *Let $\mathfrak{d}$ be a domain with quotient field k. Let $\mathfrak{d}^* \to \mathscr{D}$ be a divisor construction determined by a set of valuations $\mathfrak{R}_0$. If K is a finite extension of k and $\mathfrak{R}$ are all the extensions of $\mathfrak{R}_0$, then $\mathfrak{R}$ induces a divisor construction on the integral closure $\mathbb{D}$ of $\mathfrak{d}$ in K.*

Proof. We use Theorem 3.6 and need only show that $\mathfrak{R}$ satisfies the three conditions.

(2) Let $v_0 \in \mathfrak{R}_0$ be any valuation, and let $v \in \mathfrak{R}$ be an extension. It is clear that $v(\alpha) \geq 0$ for all $\alpha \in \mathfrak{d}$, so $\mathfrak{d}$ is contained in the valuation ring $\mathbb{D}_v$. We know that $\mathbb{D}_v$ is integrally closed in K, so we must have $\mathbb{D} \subseteq \mathbb{D}_v$. Hence for any $\alpha \in \mathbb{D}$, $v(\alpha) \geq 0$.

Now let $\alpha \in K$ be such that $v(\alpha) \geq 0$ for any valuation v. Let α have minimal polynomial $t^r + a_1 t^{r-1} + \ldots a_r \in k[x]$. For any valuation $v_0 \in \mathfrak{R}_0$ let $v_1, \ldots, v_m \in \mathfrak{R}$ be the extensions. Since $v_i(\alpha) \geq 0$, Theorem 3.14 says that α lies in the integral closure in K of the valuation ring of v_0. From the previous Lemma, it follows that the coefficients of the minimal polynomial a_i must lie in the ring of the valuation of v_0. So $v_0(a_i) \geq 0$ for all a_i. This argument holds for any $v_0 \in \mathfrak{R}_0$, hence all a_i lie in $\mathfrak{d}$ and it follows that $\alpha \in \mathbb{D}$. Condition (2) is satisfied.

(1) Let $\alpha \in \mathbb{D}$, $\alpha \neq 0$. Let as above $t^r + a_1 t^{r-1} + \ldots a_r$ be the minimum polynomial for α. Since the a_i's lie in $\mathfrak{d}$, we have $v_0(a_i) = 0$ for almost all $v_0 \in \mathfrak{R}_0$. Using this and the fact that $v(\alpha) \geq 0$ we can write

$$\begin{aligned} v(\alpha^{-1}) &= v(a_r^{-1}(\alpha^{r-1} + a_1\alpha^{r-2} + \cdots + a_{r-1})) \\ &= v(\alpha^{r-1} + a_1\alpha^{r-2} + \cdots + a_{r-1}) - v(a_r) \\ &= v(\alpha^{r-1} + a_1\alpha^{r-2} + \cdots + a_{r-1}) \qquad \text{for almost all } v \\ &\geq 0. \end{aligned}$$

But the only way v can be non-negative for both α and its inverse, is if $v(\alpha) = 0$. Condition (1) is proved.

(3) Let $V = \{v_1, \ldots, v_m\} \subseteq \mathfrak{R}$ be a set of distinct valuations, and let $k_1, \ldots, k_m$ be non-negative integers. Take the set of valuations in $\mathfrak{R}_0$, $V_0 = \{v_{01}, \ldots, v_{0m}\}$ which are induced by the valuations of V.Extend these valuations back up to $\mathfrak{R}$ and get a set $v_1, \ldots, v_m, v_{m+1}, \ldots, v_s$. Using Theorem 3.11 we find an element $\gamma \in K$ such that

$$\begin{aligned} v_i(\gamma) = k_i \text{ for } 1 \leq i \leq m \\ v_i(\gamma) = 0 \text{ for } m+1 \leq i \leq s. \end{aligned}$$

If $\gamma \in \mathbb{D}$ we can set $\alpha = \gamma$ and we are done. Assume that $\gamma \notin \mathbb{D}$. Let $v'_1, \ldots, v'_r$ be valuations of $\mathfrak{R}$ where $v'_j(\gamma) < 0$, say

$$v'_1(\gamma) = -l_1, \ldots, v'_r(\gamma) = -l_r$$

for positive l_j. Let these valuations induce the set $V'_0 = \{v'_{01}, \ldots, v'_{0r}\} \subseteq \mathfrak{R}_0$ on k. We see that any element $v'_{0j} \in V'_0$ must be different from any element $v_{0i} \in V_0$, so there exists an element $a \in \mathfrak{d}$ such that

$$\begin{aligned} v_{0i}(a) = 0 \text{ for } 1 \leq i \leq m \\ v'_{0j}(a) = l \text{ for } 1 \leq i \leq r \end{aligned}$$

where $l = \max(l_1, \ldots, l_r)$. We can now set $\alpha = \gamma a$ and get

$$\begin{aligned} v'_j(\alpha) &= v'_j(\gamma) + v'_j(a) \\ &\geq l_j + v'_{0j}(a) \\ &= l_j + l \\ &\geq 0. \end{aligned}$$

It follows that $\alpha \in \mathbb{D}$, and we can in any case find an element $\alpha \in \mathbb{D}$ which satisfies condition (3).

The Theorem is proved. □

When we use this theorem on algebraic number fields, we get the following corollary.

Corollary 3.17. *Let K be an algebraic number field with the maximal order R_K. Then there exists a divisor construction $\mathbb{D}^* \to \mathscr{D}$ which is induced by the valuations of K.*

Proof. $\mathbb{D}$ is the integral closure in K of $\mathbb{Z}$. We know that $\mathbb{Z}$ has unique factorization, and thus it has a divisor construction. It is easily seen that the valuation of $\mathbb{Q}$ induces this divisor construction. Since all the valuations of K are extensions of valuations on $\mathbb{Q}$, using the previous Theorem proves our corollary. □

We continue to look at extension fields and the relation between divisor constructions on the two field. Let $\mathfrak{d}$ be a domain with quotient field k which has a divisor construction $\mathfrak{d}^* \to \mathscr{D}_0$. Let K/k be a finite extension and let the integral closure $\mathbb{D}$ of $\mathfrak{d}$ in K also have a divisor construction $\mathbb{D}^* \to \mathscr{D}$. Since $\mathfrak{d} \subseteq \mathbb{D}$, every element $a \in \mathfrak{d}^*$ corresponds to divisors in both $\mathscr{D}_0$ and $\mathscr{D}$. We use the following notation to distinguish between these divisors, $(a)_k \in \mathscr{D}_0$ and $(a)_K \in \mathscr{D}$. We now show that this correspondence can be extended to all divisors of $\mathscr{D}_0$.

Theorem 3.18. *With the notation above, there is an monomorphism from the semigroup $\mathscr{D}_0$ into the semigroup $\mathscr{D}$ which identifies $(a)_k$ and $(a)_K$.*

Proof. Take any prime divisor $\mathfrak{p}$ of $\mathscr{D}_0$, with $v_\mathfrak{p}$ the corresponding valuation of k. We extend this valuation to a set of valuations $v_{\mathfrak{b}_1}, \ldots, v_{\mathfrak{b}_m}$ on K, with corresponding prime divisors $\mathfrak{b}_1, \ldots, \mathfrak{b}_m$. Let $e_1, \ldots, e_m$ be the ramification indices, and for any i we can write $v_{\mathfrak{b}_i}(a) = e_i v_\mathfrak{p}(a)$. For any $a \in \mathfrak{d}^*$ consider the divisor $(a)_k \in \mathscr{D}_0$ and the divisor $(a)_K \in \mathscr{D}$. The factor $\mathfrak{p}^{v_\mathfrak{p}(a)}$ of $(a)_k$ becomes $\mathfrak{b}_1^{\mathfrak{b}_1(a)} \ldots \mathfrak{b}_m^{\mathfrak{b}_m(a)} = (\mathfrak{b}_1^{e_1} \ldots \mathfrak{b}_m^{e_m})^{v_\mathfrak{p}(a)}$ in $(a)_K$. We create a mapping $\mathscr{D}_0 \to \mathscr{D}$ defined on the prime divisors as

$$\mathfrak{p} \mapsto \mathfrak{b}_1^{e_1} \ldots \mathfrak{b}_m^{e_m}.$$

This mapping satisfies the theorem. □

We shall identify the divisors in $\mathscr{D}_0$ with divisors in $\mathscr{D}$ using the mapping from the proof above and write simply $\mathfrak{p} = \mathfrak{b}_1^{e_1} \ldots \mathfrak{b}_m^{e_m}$.

Using the notation above, we let $\mathfrak{p} \in \mathscr{D}_0$ and $\mathfrak{b} \in \mathscr{D}$ be divisors. We see that $\mathfrak{b}$ divides $\mathfrak{p}$ if the valuation $v_\mathfrak{b}$ is an extension of the valuation $v_\mathfrak{p}$

If $\mathfrak{b}|\mathfrak{p}$, we define *the ramification index* of $\mathfrak{b}$ over $\mathfrak{p}$ as the ramification index of the corresponding valuations.

Let $\mathfrak{p}$ have the decomposition

$$\mathfrak{p} = \mathfrak{b}_1^{e_1} \ldots \mathfrak{b}_m^{e_m}.$$

If all the e_i's are equal to one, we say that $\mathfrak{p}$ is *unramified* in $\mathbb{D}$.

3.4 Degree of divisors

In this section K/k is a finite extension of fields. For any valuation v of the field K, recall that we defined the corresponding ring, $\mathbb{D}_v$, consisting of the elements of K for which v is non-negative. This ring has a theory of divisor with a single prime element π, which is unique up to associates. From Theorem 3.8, we can write any non-zero α of $\mathbb{D}_v$ in the form

$$\alpha = \epsilon\pi^m$$

where ϵ is a unit in $\mathbb{D}_v$. For a fixed π, this form is unique. We now consider congruence classes modulo the prime π. Two elements are equivalent if their difference is divisible by π, and this forms equivalence classes of the elements in $\mathbb{D}_v$. Observe that since the prime we chose was unique up to accociation, any prime gives the same equivalence classes, so this is completely determined by the ring $\mathbb{D}_v$. It is easily verified that these equivalence classes form a ring, and we write $\Sigma_v = \mathbb{D}_v/(\pi)$. For $\alpha \in \mathbb{D}_v$ with $\alpha \not\equiv 0 \pmod{\pi}$, we have $v_\pi(\alpha) = 0$. Then α has an inverse in $\mathbb{D}_v$, ξ. Since $\alpha\xi = 1$, we get $\alpha\xi \equiv 1 \pmod{\pi}$ and α has an inverse in Σ_v. This proves that Σ_v is a field, the *residue class field*. If $v_\mathfrak{p}$ is a valuation corresponding to the prime $\mathfrak{p}$, we write $\Sigma_\mathfrak{p}$ for the residue class field.

Let $\mathfrak{b}$ be a prime divisor of K and $\mathfrak{p}$ of k such that $\mathfrak{b}|\mathfrak{p}$. Consider the valuation rings $D_\mathfrak{p}$ and $D_\mathfrak{b}$, corresponding to these divisors. Let p be the prime of $D_\mathfrak{p}$ and π the prime of $D_\mathfrak{b}$. Since $D_\mathfrak{p} \subseteq D_\mathfrak{b}$, we can write $p = \epsilon\pi^m$ for a unit ϵ. It follows that if $a \equiv b \pmod{p}$ in $D_\mathfrak{p}$, then $a \equiv b \pmod{\pi}$ in $D_\mathfrak{b}$. Hence every residue class of $D_\mathfrak{p}$ is contained in a single residue class of $D_\mathfrak{b}$. This induced an monomorphism of the residue class field $\Sigma_\mathfrak{p}$ into $\Sigma_\mathfrak{b}$. This means that $\Sigma_\mathfrak{p}$ is a subfield $\Sigma_\mathfrak{b}$ and an easy calculation shows that the degree $[\Sigma_\mathfrak{b} : \Sigma_\mathfrak{p}]$ is limited by the degree of K/k. The degree $f_\mathfrak{b} = [\Sigma_\mathfrak{b} : \Sigma_\mathfrak{p}]$ is called the *degree of inertia* of the prime divisor $\mathfrak{b}$ over $\mathfrak{p}$. It is sometimes refered to as the *degree of a prime* over an extension.

We state a theorem relating ramification, degree of inertia and the degree of the fields.

Theorem 3.19. *Let $\mathfrak{d}$ be a domain with quotient field k and let K/k be a seperable extension. Let $\mathfrak{p}$ be a prime divisor of $\mathfrak{d}$. For any $\mathfrak{b}$ dividing $\mathfrak{p}$, we denote $e_\mathfrak{b}$ the ramification index and $f_\mathfrak{b}$ the degree of inertia of $\mathfrak{b}$ over $\mathfrak{p}$. If n is the degree of K/k we have the following connection,*

$$\sum_{\mathfrak{b}|\mathfrak{p}} e_\mathfrak{b} f_\mathfrak{b} = n,$$

where the sum runs over all prime divisors that divide $\mathfrak{p}$.

Proof. [3] Theorem 7, Chapter 5.3 □

It can be shown that for separable extensions, ramification is rare. That is, in a ring $\mathfrak{d}$ there are only finitely many prime divisors that ramify in a finite extension $\mathbb{D}$.

3.5 Congruences modulo divisors

We start this section by defining congruence modulo divisors. This generalizes what we did with primes in valuation rings.

Definition 3.20. Let $\mathbb{D}$ be any domain with a divisor construction $\mathbb{D}^* \to \mathscr{D}$. Two elements $\alpha, \beta \in \mathbb{D}$ are *congruent modulo* the divisor $\mathfrak{a} \in \mathscr{D}$ if the difference $\alpha - \beta$ is divisible by $\mathfrak{a}$. We denote this by

$$\alpha \equiv \beta \pmod{\mathfrak{a}}.$$

For the divisor $\mathfrak{a}$ we see that this definition divides $\mathbb{D}$ into classes of elements which are congruent modulo $\mathfrak{a}$. It is easily verified that the set of classes forms a ring. We call it *the residue class ring* modulo $\mathfrak{a}$ and write $\mathbb{D}/\mathfrak{a}$.

Theorem 3.21. *Let R_K be the maximal order in an algebraic number field K. Let $\mathfrak{p}$ be a prime divisor. Then $\mathfrak{p}$ divides precisely one prime number $p \in \mathbb{N}$. The residue class ring $R_K/\mathfrak{p}$ is a finite field of characteristic p.*

Proof. The prime divisor $\mathfrak{p}$ corresponds to a valuation $v_\mathfrak{p}$. Since K is an extension of $\mathbb{Q}$, $v_\mathfrak{p}$ induced a p-adic valuation on $\mathbb{Q}$, for some prime p. Then $v_\mathfrak{p}(p) \geq 1$ and $p \equiv 0 \pmod{\mathfrak{p}}$. For any prime $q \neq p$, $v_\mathfrak{p}(q) = 0$, meaning that $\mathfrak{p}$ does not divide any prime $q \neq p$.

Since p divides $\mathfrak{p}$, congruences that hold modulo $\mathfrak{p}$ also hold modulo p. We look at classes module p. Let $\omega_1, \ldots, \omega_n$ be a basis for R_K. It is clear that any $\alpha \in R_K$ is congruent modulo p to an element on the form

$$a_1\omega_1 + \cdots + a_n\omega_n$$

where the integers a_i are restricted by $1 \leq a_i \leq p$. Since if $a_i > p$, we can subtract the element $p\omega_i$. Hence there are only a finite number of congruence classes modulo p and also only a finite number of congruence classes modulo $\mathfrak{p}$.

Now let $\alpha, \beta \in R_K$ be elements such that $\alpha\beta \equiv 0 \pmod{\mathfrak{p}}$ and $\alpha \not\equiv 0 \pmod{\mathfrak{p}}$. This is equivalent to $\mathfrak{p}|(\alpha\beta)$, or $\mathfrak{p}|(\alpha)(\beta)$. But since $\mathfrak{p} \nmid (\alpha)$, we must have $\mathfrak{p}|(\beta)$ and $\beta \equiv 0 \pmod{\mathfrak{p}}$. Hence, $R_K/\mathfrak{p}$ is finite without zero-divisors. Take any non-zero $\gamma \in R_K/\mathfrak{p}$. Then $\gamma x_1 = \gamma x_2$ if and only if $x_1 = x_2$. Hence the map $x \mapsto \gamma x$ hit all of $R_K/\mathfrak{p}$. We can then take x such that $\gamma x = 1$ and we see that all non-zero elements γ have inverse and $R_K/\mathfrak{p}$ is a field. This field have characteristic p, since for any $\alpha \in R_K$, $\alpha p \equiv 0 \pmod{\mathfrak{p}}$. This completes the proof. □

3.6 Fractional divisors

This section is devoted to fractional divisors, which are a generalization of divisors. Earlier we used divisors to get information about the multiplicative structure of a domain, $\mathbb{D}$. We now expand the notion of divisors, to get information about the quotient field of $\mathbb{D}$.

Definition 3.22. Let $\mathbb{D}$ be an integral domain with quotient field K. Let $\mathbb{D}^* \to \mathscr{D}$ be a divisor construction for $\mathbb{D}$ and let $\mathfrak{p}_1, \ldots, \mathfrak{p}_m$ be prime divisors.

$$\mathfrak{a} = \mathfrak{p}_1^{k_1} \ldots \mathfrak{p}_m^{k_m}$$

with k_i any integers is called a *fractional divisor* of K. We see that if all the exponents are non-negative, this becomes a divisor of $\mathbb{D}$, we sometimes call these divisors *integral divisors*.

We write

$$\mathfrak{a} = \prod_{\mathfrak{p}} \mathfrak{p}^{a(\mathfrak{p})}$$

where the product runs over all the prime divisors $\mathfrak{p}$, but almost all the exponents $a(\mathfrak{p})$ are zero.

We define multiplication of fractional divisors as

$$(\prod_{\mathfrak{p}} \mathfrak{p}^{a(\mathfrak{p})})(\prod_{\mathfrak{p}} \mathfrak{p}^{b(\mathfrak{p})}) = \prod_{\mathfrak{p}} \mathfrak{p}^{a(\mathfrak{p})+b(\mathfrak{p})}.$$

We see that this makes the fractional divisors into an abelian group with $\mathfrak{e}$, the divisor with all exponents equal to zero, as the identiy element.

Let $v_{\mathfrak{p}}$ be the valuation corresponding to the prime divisor $\mathfrak{p}$. For any $\xi \in K^*$, it is clear that $v_{\mathfrak{p}}(\xi) = 0$ for almost all valuations $v_{\mathfrak{p}}$ (Theorem 3.6). A divisor on the form

$$(\xi) = \prod_{\mathfrak{p}} \mathfrak{p}^{v_{\mathfrak{p}}(\xi)}$$

is called a *principal fractional divisor*. We see that for elements of the domain $\mathbb{D}$ this definition corresponds with the previous definition of principal divisors.

It can be shown that these generalized divisors share many of the properties of the old divisors. We say that the fractional divisor $\mathfrak{a}$ divides $\mathfrak{b}$ if there exists an integral divisor $\mathfrak{c}$ of the ring $\mathbb{D}$ such that $\mathfrak{ac} = \mathfrak{b}$.

3.7 Divisors in number fields

Recall that if R_K is a maximal order in any algebraic number field, we have a divisor construction $R_K^* \to \mathscr{D}$. We can therefore study fractional divisors over any algebraic number field.

Definition 3.23. Let R_K be the maximal order in an algebraic number field K. A non-empty subset $A \subseteq K$ is called a *fractional ideal* of K if it satisfies the following.

(1) A is a group under the addition from K.

(2) $AR_K \subseteq A$ (i.e. for any $a \in A$ and $r \in R_K$, $ar \in A$.)

(3) There exists a non-zero element $\gamma \in K$ such that $\gamma A \subseteq R_K$.

We see that if $A \subseteq R_K$, then A is an ideal of the ring R_K, and we call such ideals for *integral ideals*.

We first state a small lemma, and include a sketch of a proof. Note that this lemma can be generalized to work with any Dedekind domain, not just maximal orders in number fields.

Lemma 3.24. *Let R_K be the maximal order in an algebraic number field K. Let A be a fractional ideal of K and M a torsion-free R_K-module. Then the map*

$$\begin{aligned} \phi\colon A^{-1}M &\to \operatorname{Hom}_{R_K}(A, M) \\ x &\mapsto (\phi_x\colon \alpha \mapsto \alpha x) \end{aligned}$$

is an isomorphism.

Proof. We can symbolically write $K = R/R^*$, for the quotient field K. Similarly we can construct M/R^*, in which we consider fractions of the module M. This is the same as the tensor product of M with K over R and we write

$$M_K = M \otimes_R K = M/R^*.$$

Let $\psi \in \operatorname{Hom}_R(A, M)$. We now have the situation $A \subseteq K$ and $M \subseteq M_K$. We extend ϕ to K and get a K-linear map $\overline{\phi} \in \operatorname{Hom}_K(K, M_K)$. This extension is uniquelly defined and for $\alpha \in A$

$$\psi(\alpha) = \overline{\psi}(\alpha) = \overline{\psi}(1 \cdot \alpha) = \alpha\overline{\psi}(1) \in M.$$

This shows that any map in $\operatorname{Hom}_R(A, M)$ corresponds to an element $\overline{\psi} \in A^{-1}M$, which shows that our map is surjective.

It is easily checked that the map is a monomorphism, which completes the proof. □

We now state a theorem which identifies ideals and divisors in number fields. This allows us to use the theory on divisors, when dealing with ideals.

Theorem 3.25. *Let K be an algebraic number field. For a fractional divisor $\mathfrak{a}$ we denote $A_\mathfrak{a} \subseteq K$ as the set of elements that are divisible by $\mathfrak{a}$. Then $A_\mathfrak{a}$ is a fractional ideal. Further, the fractional ideals form an abelian group and the mapping*

$$\mathfrak{a} \mapsto A_\mathfrak{a}$$

is an isomorphism from the group of fractional divisors to the group of fractional ideals of the field K.

We need a lemma.

Lemma 3.26. *Let R_K be the maximal order in an algebraic number field K with $\alpha_1, \ldots, \alpha_s \in R_K$. Let $\mathfrak{d}$ be the greatest common divisor of $(\alpha_1), \ldots, (\alpha_s)$. Then for any $\alpha \in R_K$ which is divisible by $\mathfrak{d}$ we can find a set of elements $\xi_i \in R_K$ such that*

$$\alpha = \xi_1\alpha_1 + \cdots + \xi_s\alpha_s$$

Proof. [3] Lemma 2, Section 3.6 □

Proof of Theorem. We first prove a weaker version of this theorem. We prove that for any integarl ideal $\mathfrak{a}$, the map

$$\mathfrak{a} \mapsto A_{\mathfrak{a}}$$

is an isomorphism from the semi-group of integral divisors to the semi-group of non-zero integral ideals of the ring R_K.

The third point of the definition of a divisor construction, gives that the map is one-to-one. We show that it is onto. Take any non-zero ideal A of R_K. For each prime divisor $\mathfrak{p}$ we set

$$a(\mathfrak{p}) = \min_{\alpha \in A} v_{\mathfrak{p}}(\alpha).$$

This is non-zero only for a finite number of prime divisors, and we see that

$$\mathfrak{a} = \prod_{\mathfrak{p}} \mathfrak{p}^{a(\mathfrak{p})}$$

is a divisor. We also note that $A \subseteq A_{\mathfrak{a}}$. We now show that these ideals are equal. Take any $\alpha \in A$. Since $a(\mathfrak{p})$ is zero for almost all prime divisors, we can find a finite set $\alpha_1, \ldots, \alpha_s \in A$ such that

$$a(\mathfrak{p}) = \min(v_{\mathfrak{p}}(\alpha_1), \ldots, v_{\mathfrak{p}}(\alpha_s)) \text{ for all } \mathfrak{p}.$$

It follows that $\mathfrak{a}$ is the greatest common divisor of $(\alpha_1), \ldots, (\alpha_s)$, and using the Lemma, we can find $\xi_i \in R_K$ such that

$$\alpha = \xi_1 \alpha_1 + \cdots + \xi_s \alpha_s.$$

Since A is an ideal in R_K, we have $\alpha \in A$, and $A_{\mathfrak{a}} \subseteq A$. This proves that our map is onto.

It remains to show that this is a homomorphism of groups. We need to show

$$A_{\mathfrak{a}} A_{\mathfrak{b}} = A_{\mathfrak{a}\mathfrak{b}}$$

for any divisors $\mathfrak{a}$ and $\mathfrak{b}$. Since $A_{\mathfrak{a}} A_{\mathfrak{b}}$ is an ideal, we have seen that there exist a divisor $\mathfrak{c}$ such that

$$A_{\mathfrak{a}} A_{\mathfrak{b}} = A_{\mathfrak{c}}.$$

We therefore only have to show that $\mathfrak{a}\mathfrak{b} = \mathfrak{c}$. For a prime divisor $\mathfrak{p}$ denote its power in $\mathfrak{a}$ and $\mathfrak{b}$ as a and b respectively. Then

$$\min_{\gamma \in A_{\mathfrak{c}}} v_{\mathfrak{p}}(\gamma) = \min_{\alpha \in A_{\mathfrak{a}}, \beta \in A_{\mathfrak{b}}} v_{\mathfrak{p}}(\alpha\beta) = \min_{\alpha \in A_{\mathfrak{a}}} v_{\mathfrak{p}}(\alpha) + \min_{\beta \in A_{\mathfrak{b}}} v_{\mathfrak{p}}(\beta) = a + b.$$

We see that the power of $\mathfrak{p}$ in $\mathfrak{c}$ is $a + b$. Since this holds for all prime divisors, we must have $\mathfrak{a}\mathfrak{b} = \mathfrak{c}$.

This proves the weak version of the Theorem. We now look at fractional divisors and ideals. Let $\gamma \in R_K^*$ and $\mathfrak{a} = \prod \mathfrak{p}^{a(\mathfrak{p})}$ a fractional divisor of K. For $\xi \in K$ we have

$$\begin{aligned} \xi \in A_{(\gamma)\mathfrak{a}} &\Leftrightarrow v_\mathfrak{p}(\xi) \geq v_\mathfrak{p}(\gamma) + a(\mathfrak{p}),\ \forall \mathfrak{p} \\ &\Leftrightarrow v_\mathfrak{p}(\xi/\gamma) \geq a(\mathfrak{p}),\ \forall \mathfrak{p} \\ &\Leftrightarrow \xi/\gamma \in A_\mathfrak{a} \\ &\Leftrightarrow \xi \in \gamma A_\mathfrak{a} \end{aligned}$$

Hence, $A_{(\gamma)\mathfrak{a}} = \gamma A_\mathfrak{a}$, and it is easy to verify that for a fractional divisor $\mathfrak{a}$, the set $A_\mathfrak{a}$ is a fractional ideal of K.

Let $\mathfrak{a}$ and $\mathfrak{b}$ be fractional divisors with $A_\mathfrak{a} = A_\mathfrak{b}$. It is clear that we can find a $\gamma \in R_K^*$ such that $(\gamma)\mathfrak{a}$ and $(\gamma)\mathfrak{b}$ are both integral. Some computations give us

$$\begin{aligned} A_\mathfrak{a} = A_\mathfrak{b} &\Rightarrow \gamma A_\mathfrak{a} = \gamma A_\mathfrak{b} \\ &\Rightarrow A_{(\gamma)\mathfrak{a}} = A_{(\gamma)\mathfrak{b}} \\ &\Rightarrow (\gamma)\mathfrak{a} = (\gamma)\mathfrak{b} \\ &\Rightarrow \mathfrak{a} = \mathfrak{b}, \end{aligned}$$

which proves that the map is one-to-one. We now show that it is also onto. Take any fractional ideal A. Let $\gamma \in K$ be a non-zero number such that $\gamma A \subseteq R_K$. It follows that γA is an integral ideal and from the weak version of the Theorem there is an integral divisor $\mathfrak{c}$ such that $A_\mathfrak{c} = \gamma A$. Create the fractional divisor $\mathfrak{a} = \mathfrak{c}(\gamma)^{-1}$. Then

$$\gamma A = A_\mathfrak{c} = A_{(\gamma)\mathfrak{a}} = \gamma A_\mathfrak{a},$$

which means that $A = A_\mathfrak{a}$ and the map is onto.

All that remains is to show that the map is a homomorphism. Let $\mathfrak{a}$ and $\mathfrak{b}$ be fractional divisors. Take non-zero elements $\alpha, \beta \in R_K$ such that $(\alpha)\mathfrak{a}$ and $(\beta)\mathfrak{b}$ are integral. We now use the weak version and get

$$\begin{aligned} \alpha\beta A_{\mathfrak{a}\mathfrak{b}} &= A_{(\alpha\beta)\mathfrak{a}\mathfrak{b}} \\ &= A_{(\alpha)\mathfrak{a}} A_{(\beta)\mathfrak{b}} \\ &= \alpha A_\mathfrak{a} \beta A_\mathfrak{b}. \end{aligned}$$

This shows that $A_{\mathfrak{a}\mathfrak{b}} = A_\mathfrak{a} A_\mathfrak{b}$ and we have proved the Theorem in general. We note that this makes the set of fractional ideals into an abelian group with R_K as the identity element, and the inverse of the ideal $A_\mathfrak{a}$ is $A_{\mathfrak{a}^{-1}}$. □

3.8 Divisor classes

Definition 3.27. Let $\mathfrak{a}$ and $\mathfrak{b}$ be two fractional divisors of an algebraic number field K. We say that $\mathfrak{a}$ and $\mathfrak{b}$ are *equivalent* if there exists a principal divisor (α), $\alpha \in K^*$, such that $\mathfrak{a} = (\alpha)\mathfrak{b}$. This divides all the divisors into equivalence classes, which we call *divisor classes* of K. We write $[\mathfrak{a}]$ for the divisor class containing $\mathfrak{a}$.

We define an multiplication on divisor classes by setting

$$[\mathfrak{a}][\mathfrak{b}] = [\mathfrak{a}\mathfrak{b}].$$

This is easily seen to be independent of the representative chosen from the divisor classes. This makes the set of divisor classes into an abelian group. The class consisting of all the principal divisors, $[\mathfrak{e}]$, is the identity element, and the inverse of $[\mathfrak{a}]$ is $[\mathfrak{a}^{-1}]$. This group is called *the divisor class group of* K and we write $\mathfrak{CL}(K)$. It is also known as *the Picard group.*

Theorem 3.28. *The divisor class group of an algebraic number field forms a finite abelian group.*

Proof. Let K be an algebraic number field. We use the Theorem 3.25, which identifies a fractional divisor $\mathfrak{a}$ with the fractional ideal $A_{\mathfrak{a}}$.

Next we observe that $A_{\mathfrak{a}}$ is a full module in K. Pick an element $\gamma \in K$ such that $\gamma A_{\mathfrak{a}} \subseteq R_K$, where R_K is the maximal order of K. (This element exists from the definition of fractional ideals.) Since R_K is a module, it follows that $\gamma A_{\mathfrak{a}}$ is a module, and thus also $A_{\mathfrak{a}}$. Since $A_{\mathfrak{a}} R_K \subseteq A_{\mathfrak{a}}$ it follows that $A_{\mathfrak{a}}$ contains as many linearly independent elements as R_K, and hence $A_{\mathfrak{a}}$ is a full module. It is clear that its coefficient ring is R_K. Conversely, all full modules with coefficient ring R_K, satisfies the definition of fractional ideals.

This means that dividing fractional divisors up in equivalence classes, corresponds to dividing full modules with coefficient ring R_K into equivalence classes. From Theorem 2.8 it follows that there are a finite number of divisor classes, and the Theorem is proved. □

3.9 Conductor, Artin Reciprocity and the Hilbert class field

We will in this section introduce a few new concepts. The Hilbert class field is an important extension of a number field in which every prime stays unramified. We also state a Theorem known as Artin reciprocity law, which will be useful later.

In this section K is an imaginary quadratic number field, unless otherwise stated. Let L be a finite extension of K with degree n such that $\mathrm{Gal}(L/K)$ is abelian. We denote R_K and R_L for the maximal orders of the fields respectively. Let $\mathfrak{p}$ be a prime divisor in R_K. Recall that $\mathfrak{p}$ will not normally stay prime in R_L, but we will assume that it is unramified. Let $\mathfrak{b}$ be any prime divisor of R_L that divides $\mathfrak{p}$. We can now create the residue class fields of these divisors,

$$k = R_K/\mathfrak{p}$$

and

$$l = R_L/\mathfrak{b}.$$

From Theorem 3.21, we see that l/k is an extension of finite fields.

Write the splitting of $\mathfrak{p}$ in L as

$$\mathfrak{p} = \mathfrak{b}_1 \dots \mathfrak{b}_s.$$

Then the Galois group of L/K, $G = \mathrm{Gal}(L/K)$, acts transitively on the set of divisors $X = \{\mathfrak{b}_1, \ldots, \mathfrak{b}_s\}$ ([6] 8,3.1). For each $\mathfrak{b}_i$ we consider a subgroup of the Galois group, called the *stabilizer group* of $\mathfrak{b}_i$,

$$G_{\mathfrak{b}_i} = \{\sigma \in G \colon \sigma(\mathfrak{b}_i) = \mathfrak{b}_i\}.$$

Since the Galois group actions is transitive, there exists an element $\sigma \in G$ which sends $\mathfrak{b}_j$ to $\mathfrak{b}_i$. We have also assumed that the Galois group also is abelian, and get

$$G_{\mathfrak{b}_j} = \sigma^{-1} G_{\mathfrak{b}_i} \sigma = G_{\mathfrak{b}_i}.$$

So we see that in this case all these sets consist of the same Galois elements and we write $G_{\mathfrak{b}}$.

Take an element $\sigma \in G_{\mathfrak{b}}$. Since $\sigma \in \mathrm{Gal}(L/K)$, it fixes the maximal order R_L. It is also in the stabilizer group of $\mathfrak{b}$, so it fixes this divisor as well. In this way we see that we get a mapping from $G_{\mathfrak{b}}$ to the Galois group of l/k,

$$G_{\mathfrak{b}} \to \mathrm{Gal}(l/k).$$

We now use some facts from the theory of group actions. Let $G \times X \to X$ be a transitive action. The stabilizer subgroup $G_{\mathfrak{b}} \subseteq G$ are related to G and X by the following equality,

$$|G| = |G_{\mathfrak{b}}| \cdot |X|.$$

This gives us $|G_{\mathfrak{b}}| = n/s$ =degree of the extension l/k. Using this together with the assumption that $\mathfrak{p}$ is unramified in L, it is possible to show that the mapping

$$G_{\mathfrak{b}} \to \mathrm{Gal}(l/k)$$

is an isomorphism of groups. (See Section 8,3 of [6].)

We know that $\mathrm{Gal}(l/k)$ is cyclic, generated by the Frobenius automorphism

$$x \mapsto x^{N_{\mathbb{Q}}^K \mathfrak{p}}.$$

We let $\sigma_{\mathfrak{p}} \in \mathrm{Gal}(L/K)$ be the unique element, depending on $\mathfrak{p}$, which maps to this Frobenius.

Let $\mathfrak{c}$ be an integral divisor such that ramfication in L/K are limited to primes in $\mathfrak{c}$. We first define a subgroup of the group of fractional divisors

$$I(\mathfrak{c}) = \{\mathfrak{a} \colon \gcd(\mathfrak{a}, \mathfrak{c}) = 1\},$$

and a homomorphism called the *Artin map* from this subgroup into the galois group of L/K

$$\begin{aligned} (\cdot, L/K) \colon I(\mathfrak{c}) &\to \mathrm{Gal}(L/K) \\ (\prod_{\mathfrak{p}} \mathfrak{p}^{n_{\mathfrak{p}}}, L/K) &= \prod_{\mathfrak{p}} \sigma_{\mathfrak{p}}^{n_{\mathfrak{p}}}. \end{aligned}$$

where $\sigma_{\mathfrak{p}}$ is the unique element that maps to Frobenius.

We have the following theorem regarding the Artin map, proof can be found in [5].

Theorem 3.29 (Weak Artin Reciprocity)**.** *Let K be an imaginary quadratic number field and let L/K be a finite abelian extension. Then there exists an integral divisor $\mathfrak{m}$ in R_K such that if $\alpha \in K^*$ satisfies $\alpha \equiv 1 \pmod{\mathfrak{m}}$, then the principal divisor (α) is in the kernel of the Artin map. There exists a largest such divisor which we call the* conductor *of L/K and write $\mathfrak{m}_{L/K}$.*

Definition 3.30. Let $\mathfrak{m}$ be an integral divisor of K. Let $K_{\mathfrak{m}}$ be a finite abelian extension of K. $K_{\mathfrak{m}}$ is called a *ray class field of K modulo $\mathfrak{m}$* if for any finite abelian extensions L/K there holds

$$\mathfrak{m}_{L/K} | \mathfrak{m} \Rightarrow L \subseteq K_{\mathfrak{m}}.$$

Definition 3.31. Let K still be an imaginary quadratic number field. The *Hilbert class field* of K is the ray class field of K modulo the unit divisor (1). We write H_K for this field.

We see that H_K is the maximal finite abelian extension of K in which we have no ramification. It can also be shown that the Artin map induces an isomorphism between the divisor class group of K and the Galois group of Hilbert class field of K,

$$(\cdot, H_K/K) \colon \mathfrak{CL}(K) \tilde{\to} \mathrm{Gal}(H_K/K)$$

We need another set of divisors. For any integral divisor $\mathfrak{c}$, we define a subset of $I(\mathfrak{c})$

$$P(\mathfrak{c}) = \{(\alpha) \colon \alpha \in K^* \text{ and } \alpha \equiv 1 \pmod{\mathfrak{c}}\}$$

We state a version of Dirichlets Theorem which will be needed.

Theorem 3.32 (Dirichlet)**.** *Let K be any number field and $\mathfrak{c}$ an integral divisor. Then every divisor class in $I(\mathfrak{c})/P(\mathfrak{c})$ contains infinitely many primes of inertia degree one over the extension $K/\mathbb{Q}$.*

4 Elliptic Curves

4.1 The j-invariant

Let E be an elliptic curve over a field K. Then we can represent E as the solutions to a *Weierstrass equation*

$$E\colon y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6, \quad \text{where } a_i \in K$$

together with an additional point, labeled $\mathscr{O}$.

We define some quantities related to the coefficients a_i.

$$\begin{aligned} b_2 &= a_1^2 + 4a_2 \\ b_4 &= 2a_4 + a_1a_3 \\ b_6 &= a_3^2 + 4a_6 \\ b_8 &= a_1^2a_6 + 4a_2a_6 - a_1a_3a_4 + a_2a_3^2 - a_4^2 \\ c_4 &= b_2^2 - 24b_4 \\ \Delta &= -b_2^2b_8 - 8b_4^3 - 27b_6^2 + 9b_2b_4b_6 \end{aligned}$$

We will only look on non-singular curves, and this is equivalent to $\Delta \neq 0$ ([10] Prop.1.4). We define the j-invariant to be c_4^3/Δ, and write $j(E)$ for the j-invariant corresponding to E.

Theorem 4.1. *Let $\overline{K}$ be an algebraically closed field. Let E and E' be two elliptic curves defined over $\overline{K}$. Then $j(E) = j(E')$ if and only if E and E' are isomorphic.*

Proof. It is clear that an elliptic curve can be represented by different Weierstrass equations. The change of variables however must satisfy some restrictions. From Proposition 3.1.b in [10] we have that any two Weierstrass equations for the same curve, are related by a linear change of variables of the form

$$\begin{aligned} X &= u^2X' + r \\ Y &= u^3Y' + su^2X' + t \end{aligned}$$

with $u, r, s, t \in \overline{K}, u \neq 0$. By simple arithmetics, we can verify that two equations related by such a transformation has the same j-invariant. Hence the j-invariant is not dependent on the Weierstrass equation chosen for an elliptic curve.

Let E and E' have the same j-invariant. The expressions for the j-invariant now gives us an relation between these curves. By examining this relation one can find a change of variables satisfying the above. □

Let K be a field, not necessarily algebraically closed. For a curve E/K, we can not use Theorem 4.1. Isomorphic curves will still have the same j-invariant, but it is possible to have non-isomorphic curves with the same j-invariant. For this part will we assume

that K has characteristic different from two and three. Then the curve can be written on the following Weierstrass form

$$E\colon y^2 = x^3 + Ax + B,$$

where $j(E) = \frac{1728(4A)^3}{-16(4A^3+27B^2}$. Coordinate changes which preserve this form acts the following on x, y and the coefficients,

$$\begin{aligned} x &= u^2x' \\ y &= u^3y' \\ A &= u^4A' \\ B &= u^6B', \end{aligned}$$

where $u \in \overline{K}$ and non-zero. But since K is not algebraically closed, u is not necessarily in K. This means that if $u \notin K$, $u^4, u^6 \in K$, we will get a non-isomorphic curve (over K) which has the same j-invariant. However, we also see that there are only two such isomorphism-classes, as long as $j \neq 0, 1728$ (which is equivalent to $A, B \neq 0$). Such a change of variables can be done by picking any element $\alpha = u^2$ of K which does not have a square root in K, and multiply the coefficients A and B, with α^2 and α^3 respectively. We summarize.

Definition 4.2. Let E/K be as above. Let α be any non-square in K. The *twist* of E is then,

$$E_{twist}\colon y^2 = x^3 + \alpha^2 Ax + \alpha^3 B.$$

Theorem 4.3. *Let E be an elliptic curve and E_{twist} its twist. Then $j(E) = j(E_{twist})$. If $j(E) \neq 0, 1728$, any elliptic curve with this j-invariant is isomorphic to either E or E_{twist}.*

We also have the following Theorem, which states that for any j_0, there is a corresponding elliptic curve.

Theorem 4.4. *Let K be a field, and let $j_0 \in \overline{K}$. Then there exist an elliptic curve E defined over $K(j_0)$ with $j(E) = j_0$.*

Proof. First assume $j_0 \neq 0, 1728$. Consider the curve given by

$$E\colon y^2 + xy = x^3 - \frac{36}{j_0 - 1728}x - \frac{1}{j_0 - 1728}$$

A small computation gives us $\Delta = \frac{j_0^2}{(j_0-1728)^3}$ and $j = j_0$.

The special cases are covered with these two curves

$$\begin{aligned} E\colon y^2 + y = x^3 \ ,\Delta = -27, j = 0 \\ E\colon y^2 = x^3 + x \ ,\Delta = -64, j = 1728 \end{aligned}$$

Note that in characteristic 2 and 3, $0 = 1728$, so we can choose a non-singular curve in these cases as well. □

Remark: For a finite field $\mathbb{F}_p$ with $p > 3$, there is an alternative method to get a Weierstrass form from the j-invariant. Let $j_0 \neq 0, 1728$ be in $\mathbb{F}_p$. Then the elliptic curve

$$E/\mathbb{F}_p \colon y^2 = x^2 + 3cx + 2c, \quad \text{where } c = \frac{j_0}{1728 - j_0}$$

has j-invariant j_0.

4.2 Elliptic curves over $\mathbb{C}$

We will in this section state some results from the general theory on elliptic curves over the complex numbers. For a complete understanding of this material, we refer the reader to [12], [10] or other introductory books on elliptic curves.

An elliptic function relative to a lattice Λ, is a meromorphic function on $\mathbb{C}$ which is periodic with respect to Λ. I.e. $f(z+\omega) = f(z)$ for all $\omega \in L, x \in \mathbb{C}$. We see that elliptic functions are equivalent to meromorphic functions on the quotient space $\mathbb{C}/\Lambda$.

Let Λ be a lattice in $\mathbb{C}$. Define the *Weierstrass ρ-function related to* Λ,

$$\rho(z) = \rho(z, \Lambda) = \frac{1}{z^2} + \sum_{0 \neq \omega \in \Lambda} \left(\frac{1}{(z-\omega)^2} - \frac{1}{\omega^2} \right).$$

For integers $k \geq 3$ define the *Eisenstein series*

$$G_k = G_k(\Lambda) = \sum_{0 \neq \omega \in \Lambda} \omega^{-k}.$$

It can be shown that the sum converges, and for k odd, $G_k = 0$. We have the following connection between the Eisenstein series and Weierstrass ρ-function,

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

where $g_2 = 60G_4$ and $g_3 = 140G_6$. The connection to elliptic curves is obvious and the following Theorem confirms this.

Theorem 4.5. *Let $E/\mathbb{C}$ be an elliptic curve over the complex numbers. Then there exists a lattice Λ such that E and $\mathbb{C}/\Lambda$ are isomorphic as complex-analytic groups. We say that E corresponds to the lattice Λ, and we write E_Λ.*

The converse is also true. For any lattice in $\mathbb{C}$, we can find an elliptic curve, such that these are isomorphic as complex-analytic groups.

Proof. [12] Theorem 9.19 and Theorem 9.10 □

We also note that the j-invariant for an elliptic curve over $\mathbb{C}$ can be computed directly from the corresponding lattice. For a lattice $\Lambda = \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2$ we set $\tau = \omega_1/\omega_2$, inverting if needed, such that τ lies in the upper half plane of $\mathbb{C}$. It is possible to derive a convergent sum from the Eisenstein series which allows us to compute the j-invariant. This sum in on the form

$$j(\Lambda) = j(\tau) = \frac{1}{q} + \sum_{i=0} a_i q^i$$

where a_i are integers and $q = e^{2\pi i \tau}$.

Theorem 4.6. *Let E_1 and E_2 be elliptic curves over $\mathbb{C}$ corresponding to the lattices Λ_1 and Λ_2. Then there is a bijection between the two sets*

$$\mathrm{Hom}(E_1, E_2) \cong \{\textit{holomorphic maps } \phi\colon \mathbb{C}/\Lambda_1 \to \mathbb{C}/\Lambda_2 \textit{ with } \phi(0) = 0\}$$

Proof. [10] Theorem VI.4.1.b □

Theorem 4.7. *Let E_1 and E_2 be elliptic curves over $\mathbb{C}$ corresponding to the lattices Λ_1 and Λ_2. Then E_1 and E_2 are isomorphic over $\mathbb{C}$ if and only if there exists $\alpha \in \mathbb{C}$ such that $\alpha\Lambda_1 = \Lambda_2$.*

Proof. [10] Corollary VI.4.1.1 □

Theorem 4.8. *Let E be an elliptic curve over $\mathbb{C}$ corresponding to the lattice Λ. Then the endomorphism ring of E satisfies*

$$\mathrm{End}(E) \cong \{\beta \in \mathbb{C}\colon \beta\Lambda \subseteq \Lambda\}.$$

Proof. [12] Theorem 10.1 □

Theorem 4.9. *Let E be an elliptic curve over $\mathbb{C}$. Then $\mathrm{End}(E)$ is isomorphic to either $\mathbb{Z}$ or to an order in an imaginary quadratic number field.*

Proof. [10] Theorem VI.5.5 □

We say that E has *complex multiplication* if its endomorphism ring is larger than $\mathbb{Z}$.

4.3 Reduction of elliptic curves

We will in this section see how one can reduce a curve E defined over a number field to a curve $\tilde{E}$ defined over a finite field.

Let E be a curve defined over a number field K. Let v be a valuation of the field K. We know there are many Weierstrass equations for E/K,

$$E/K\colon y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6.$$

Consider now all the Weierstrass equations in which $v(a_i) \geq 0$ for all coefficients. It follows that $v(\Delta) \geq 0$, where Δ is the discriminant of E. We say say that a Weierstrass equation is *minimal at v*, if $v(a_i) \geq 0$ and $v(\Delta)$ takes its minimal value under this constraint.

Assume now that E/K is represented by a minimal Weierstrass equation. Write $\mathbb{D}_v$ for the valuation ring of v and let $\pi \in \mathbb{D}_v$ be its prime element. Let $k = \mathbb{D}_v/(\pi)$ be the residue class field. Since $v(a_i) \geq 0$, all the coefficients will be in $\mathbb{D}_v$. We can thus reduce the coefficients a_i and get elements $\tilde{a}_i$ of k. If $v(\Delta) = 0$, the reduction $\tilde{\Delta}$ will be non-zero. This means that when we reduce the minimal Weierstrass equation, we get a reduced Weierstrass equation which defines a non-singular elliptic curve over the field k,

$$E/k\colon y^2 + \tilde{a}_1xy + \tilde{a}_3y = x^3 + \tilde{a}_2x^2 + \tilde{a}_4x + \tilde{a}_6.$$

If $v(\Delta) = 0$ we say that E has *good reduction at* v, since we get a non-singular elliptic curve. If the prime divisor $\mathfrak{p}$ of K corresponds to the divisor v, we also say that E has *good reduction at* $\mathfrak{p}$.

Theorem 4.10. *Let L be a number field and $\mathfrak{b}$ a prime divisor. Let E_1/L and E_2/L be elliptic curves with good reduction at $\mathfrak{b}$. We write $\tilde{E}_1$ and $\tilde{E}_2$ for the reduced curves. Then the map*

$$\begin{array}{rcl} \mathrm{Hom}(E_1, E_2) & \to & \mathrm{Hom}(\tilde{E}_1, \tilde{E}_2) \\ \phi & \mapsto & \tilde{\phi} \end{array}$$

preserves degree.

Proof. Take a prime l not divisible by $\mathfrak{b}$, and consider the Tate module of an elliptic curve $T_l(E)$. We know ([10] Section III.8) that there exists a bilinear, non-degenerate pairing

$$e_E \colon T_l(E) \times T_l(E) \to T_l(\mu).$$

For any isogeny $\phi \colon E_1 \to E_2$ with dual $\hat{\phi}$ this pairing satisfies

$$e_{E_1}(S, \hat{\phi}(T)) = e_{E_2}(\phi(S), T)$$

for $S \in T_l(E_1)$, $T \in T_l(E_2)$ ([10] Prop. III.8.2). These properties allows us to write two identities,

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

and

$$e_{\tilde{E}_1}(\tilde{x}, \tilde{y})^{\deg \tilde{\phi}} = e_{\tilde{E}_2}(\tilde{\phi}\tilde{x}, \tilde{\phi}\tilde{y}).$$

We also know that under reduction, the subgroups of points of a given order, is mapped isomorphic, when the order is not divisible by the prime used for reduction. It follows that

$$T_l(E) = T_l(\tilde{E}).$$

We can use the Weil pairing, and when studying its definition, we see that from the above equality it follows that

$$\widetilde{e_E(x, y)} = e_{\tilde{E}}(\tilde{x}, \tilde{y}).$$

We can now use these identities in the following computation

$$\begin{array}{rcl} e_{\tilde{E}_1}(\tilde{x}, \tilde{y})^{\deg \phi} & = & \widetilde{e_{E_1}(x, y)^{\deg \phi}} \\ & = & \widetilde{e_{E_2}(\phi x, \phi y)} \\ & = & e_{\tilde{E}_2}(\widetilde{\phi x}, \widetilde{\phi y}) \\ & = & e_{\tilde{E}_2}(\tilde{\phi}\tilde{x}, \tilde{\phi}\tilde{y}) \\ & = & e_{\tilde{E}_1}(\tilde{x}, \tilde{y})^{\deg \tilde{\phi}}. \end{array}$$

Since the pairing is non-degenerate, it follows that

$$\deg \phi = \deg \tilde{\phi}$$

and the Theorem is proved. □

A non-zero isogeny $\phi \in \mathrm{Hom}(E_1, E_2)$ cannot have degree equal to zero. We immidiatly get the following corollary.

Corollary 4.11. *Let L be a number field and $\mathfrak{b}$ a prime divisor. Let E_1/L and E_2/L be elliptic curves with good reduction at $\mathfrak{b}$. Let $\tilde{E}_1$ and $\tilde{E}_2$ be the reduced curves. Then the map*

$$\begin{array}{ccc} \mathrm{Hom}(E_1, E_2) & \to & \mathrm{Hom}(\tilde{E}_1, \tilde{E}_2) \\ \phi & \mapsto & \tilde{\phi} \end{array}$$

is injective

Corollary 4.12. *Let E be an elliptic curve over a number field. Let E have good reduction to the elliptic curve $\tilde{E}$ over a finite field. If E has complex multiplication by the maximal order of an imaginary quadratic field we have*

$$\mathrm{End}(E) \cong \mathrm{End}(\tilde{E}).$$

Proof. We have seen that $\mathrm{End}(E)$ injects into $\mathrm{End}(\tilde{E})$. We also know that the endomorphism ring is an order in an imaginary quadratic field. But since we are assuming that $\mathrm{End}(E)$ is the maximal order, it follows that $\mathrm{End}(E)$ and $\mathrm{End}(\tilde{E})$ must be isomorphic. □

4.4 Curves with complex multiplication

The following construction will be helpful, in which we identify elliptic curves which are similar.

$$\mathfrak{ECL}(R_K) = \frac{\{\text{Elliptic curves } E/\mathbb{C} \text{ with } \mathrm{End}(E) = R_K\}}{\text{Isomorphisms over } \mathbb{C}}$$

Normally, we are only interested in the study of these equivalence classes of curves. We often say that an elliptic curve E is in $\mathfrak{ECL}(R_K)$, when we mean that E is a representative for an equivalence class in $\mathfrak{ECL}(R_K)$.

If we let R_K be the maximal order in an imaginary quadratic field K, we are interested in finding elliptic curves whose endomorphism ring is R_K. If we take any fractional ideal $A_\mathfrak{a}$ in K, this is a lattice in $\mathbb{C}$ and we can take the elliptic curve $E_{A_\mathfrak{a}}$ corresponding to this lattice. This curve has the following endormorphism ring

$$\begin{array}{rcll} \mathrm{End}(E_{A_\mathfrak{a}}) & \cong & \{\alpha \in \mathbb{C} \colon \alpha A_\mathfrak{a} \subseteq A_\mathfrak{a}\} & \text{from Theorem 4.8} \\ & = & \{\alpha \in \mathbb{K} \colon \alpha A_\mathfrak{a} \subseteq A_\mathfrak{a}\} & \text{since } A_\mathfrak{a} \subset K \\ & \supseteq & R_K. & \end{array}$$

But we know that the endomorphism ring is either $\mathbb{Z}$ or an order in K. Since R_K is the maximal order of K, it follows that $\mathrm{End}(E_{A_\mathfrak{a}}) = R_K$. Hence every fractional ideal

in K gives us an elliptic curve with endomorphism ring equal to R_K. However, for any non-zero $c \in \mathbb{C}$, the ideals $A_\mathfrak{a}$ and $cA_\mathfrak{a}$ give us the same elliptic curve in $\mathfrak{ELL}(R_K)$.

Using the correspondence between fractional ideals and fractional divisors, this is equivalent to saying that any fractional divisor gives us an elliptic curve. But also that equivalent divisors give us elliptic curves in the same equivalence class. This suggests that we consider the divisor classes of K, $\mathfrak{CL}(K)$. We show this correspondence between $\mathfrak{ELL}(R_K)$ and $\mathfrak{CL}(K)$ in the following theorem.

Theorem 4.13. *Let $\Lambda \subset \mathbb{C}$ be a lattice and $E_\Lambda \in \mathfrak{ELL}(R_K)$ be an elliptic curve, representing a class. Let $A_\mathfrak{a}$ and $A_\mathfrak{b}$ be non-zero fractional ideals in K. Then*

(1) $A_\mathfrak{a}\Lambda$ is a lattice in $\mathbb{C}$,

(2) $\mathrm{End}(E_{A_\mathfrak{a}\Lambda}) \cong R_K$,

(3) $E_{A_\mathfrak{a}\Lambda} = E_{A_\mathfrak{b}\Lambda}$ in $\mathfrak{ELL}(R_K)$ if and only if $[\mathfrak{a}] = [\mathfrak{b}]$ in $\mathfrak{CL}(K)$.

This induces a well-defined group-action of $\mathfrak{CL}(K)$ on $\mathfrak{ELL}(R_K)$ defined by

$$[\mathfrak{a}] \star E_\Lambda = E_{A_\mathfrak{a}^{-1}\Lambda}.$$

This action is simply-transitive, that is for any two E_1, E_2 in $\mathfrak{ELL}(R_K)$ there exists precisely one $[\mathfrak{c}]$ in $\mathfrak{CL}(K)$ such that $[\mathfrak{c}] \star E_1 = E_2$.

Proof. (1) We have that $\mathrm{End}(E_\Lambda) = R_K$, so from Theorem 4.8 $R_K\Lambda = \Lambda$. Since $A_\mathfrak{a}$ is a fractional ideal, we can find a non-zero element $d \in \mathbb{C}$ such that $dA_\mathfrak{a} \subseteq R_K$. It follows that $A_\mathfrak{a}\Lambda \subseteq \frac{1}{d}\Lambda$, meaning that $A_\mathfrak{a}\Lambda$ is a discrete subset of $\mathbb{C}$.

We can also find a non-zero element $c \in A_\mathfrak{a} \subset \mathbb{C}$ such that $cR_K \subseteq A_\mathfrak{a}$. From this we get that $c\Lambda \subseteq A_\mathfrak{a}\Lambda$ and $A_\mathfrak{a}\Lambda$ is not contained in $\mathbb{R}$. Thus, $A_\mathfrak{a}\Lambda$ is a lattice.

(2) For $\alpha \in \mathbb{C}$ and $A_\mathfrak{a}$ a non-zero fractional ideal we have

$$\begin{array}{c} \alpha A_\mathfrak{a}\Lambda \subseteq A_\mathfrak{a}\Lambda \\ \Updownarrow \\ A_\mathfrak{a}^{-1}\alpha A_\mathfrak{a}\Lambda \subseteq A_\mathfrak{a}^{-1}A_\mathfrak{a}\Lambda \\ \Updownarrow \\ \alpha\Lambda \subseteq \Lambda. \end{array}$$

From Theorem 4.8 we have,

$$\begin{aligned} \mathrm{End}(E_{A_\mathfrak{a}\Lambda}) &= \{\alpha \in \mathbb{C} \colon \alpha A_\mathfrak{a}\Lambda \subseteq A_\mathfrak{a}\Lambda\} \\ &= \{\alpha \in \mathbb{C} \colon \alpha\Lambda \subseteq \Lambda\} \\ &= R_K. \end{aligned}$$

(3) From Theorem 4.7 we can find an element $\alpha \in \mathbb{C}$ such that

$$E_{A_\mathfrak{a}\Lambda} \cong E_{A_\mathfrak{b}\Lambda} \Leftrightarrow \alpha A_\mathfrak{a}\Lambda = A_\mathfrak{b}\Lambda.$$

We can now rewrite this in two ways and get.

$$\begin{aligned} E_{A_\mathfrak{a}\Lambda} \cong E_{A_\mathfrak{a}\Lambda} &\Leftrightarrow \Lambda = \alpha A_\mathfrak{b}^{-1} A_\mathfrak{a}\Lambda \\ &\Leftrightarrow \Lambda = (\alpha A_\mathfrak{b}^{-1} A_\mathfrak{a})^{-1}\Lambda \end{aligned}$$

We now use Theorem 4.8 and see that this is equivalent to that both $\alpha A_\mathfrak{b}^{-1} A_\mathfrak{a}$ and $(\alpha A_\mathfrak{b}^{-1} A_\mathfrak{a})^{-1}$ are contained in R_K. This can only happen if $\alpha A_\mathfrak{b}^{-1} A_\mathfrak{a}$ is the identity element and we get

$$\alpha A_\mathfrak{a} = A_\mathfrak{b}.$$

Statement (3) now follows.

It is now easy to see that the group action is well-defined,

$$[\mathfrak{a}] \star ([\mathfrak{b}] \star E_\Lambda) = [\mathfrak{a}] \star E_{A_\mathfrak{b}^{-1}\Lambda} = E_{A_\mathfrak{a}^{-1}(A_\mathfrak{b}^{-1}\Lambda)} = E_{(A_\mathfrak{a} A_\mathfrak{b})^{-1}\Lambda} = [\mathfrak{a}\mathfrak{b}] \star E_\Lambda.$$

We first show that if E_{Λ_1} and E_{Λ_2} are any elements of $\mathfrak{ELL}(R_K)$, then there is an element $[\mathfrak{a}] \in \mathfrak{CL}(K)$ that sends the first curve to the second, using our action. Choose any non-zero $\lambda_1 \in \Lambda_1$. Then $A_{\mathfrak{a}_1} = \frac{1}{\lambda_1}\Lambda_1 \subset K$ is a full module with coefficient ring R_K, and hence a fractional ideal in K. (See the proof of 3.28.) In the same way, we choose $0 \neq \lambda_2 \in \Lambda_2$ and get the fractional ideal $A_{\mathfrak{a}_2} = \frac{1}{\lambda_2}\Lambda_2$. Then

$$\frac{\lambda_2}{\lambda_1} A_{\mathfrak{a}_2} A_{\mathfrak{a}_1}^{-1} \Lambda_1 = \Lambda_2.$$

By setting $A_\mathfrak{a} = \frac{\lambda_1}{\lambda_2} A_{\mathfrak{a}_2}^{-1} A_{\mathfrak{a}_1}$, it follows that

$$[\mathfrak{a}] \star E_{\Lambda_1} = E_{A_\mathfrak{a}^{-1}\Lambda_1} = E_{\Lambda_2}$$

Hence for any two elliptic curve, we can find a divisor class that acts on the first to produce the second. We need to show that this is unique. In other words, we must show that if

$$[\mathfrak{a}] \star E_\Lambda = [\mathfrak{b}] \star E_\Lambda,$$

then $[\mathfrak{a}] = [\mathfrak{b}]$. But this follows from statement (3) above. The proof is complete. □

Remark: Let $\mathfrak{a}$ be an integral divisor with corresponding ideal $A_\mathfrak{a}$. Then $\Lambda \subseteq A_\mathfrak{a}^{-1}\Lambda$ and we have a natural homomorphism $\mathbb{C}/\Lambda \to \mathbb{C}/A_\mathfrak{a}^{-1}\Lambda$ which induces a natural map

$$E_\Lambda \to [\mathfrak{a}] \star E_\Lambda.$$

It can be shown that this map has degree equal to the norm of $A_\mathfrak{a}$. ([11] II.1.5)

Since the group-action defined in the Theorem is simply-transitive, we get this important corollary.

Corollary 4.14. *For a quadratic imaginary field K with maximal order R_K we have*

$$\#\mathfrak{ELL}(R_K) = \#\mathfrak{CL}(K).$$

This corollary is very powerful, since we know that the number of divisor classes is finite. We will use this in the following theorem, which deals with rationality of elliptic curves. If σ is any automorphism of $\mathbb{C}$ and $E/\mathbb{C}$ is an elliptic curve, we let E^σ be obtained by letting σ act on the coefficients of a Weierstrass equation for E. Then E^σ is clearly an elliptic curve.

Theorem 4.15. *(a) Let σ be a $\mathbb{C}$-automorphism and $E/\mathbb{C}$ an elliptic curve. Then*

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

(b) Let $E/\mathbb{C}$ be an elliptic curve with endomorphism ring equal to the maximal order in a quadratic imaginary field. Then the j-invariant of E is an algebraic number.

(c) The set $\mathfrak{ELL}(R_K)$ which was defined as $\mathbb{C}$-isomorphism classes, can be written as

$$\mathfrak{ELL}(R_K) \cong \frac{\{\textit{Elliptic curves } E/\overline{\mathbb{Q}} \textit{ with } \mathrm{End}(E) = R_K\}}{\textit{Isomorphisms over } \overline{\mathbb{Q}}}$$

Proof. (a) Recall that any endormophism corresponds to an element of an order in an quadratic imaginary field. It follows that we can let a $\mathbb{C}$-automorphism act on any endomorphis. Hence for any endomorphism $\phi\colon E \to E$, we get an endomorphism $\phi^\sigma\colon E^\sigma \to E^\sigma$.

(b) $j(E)$ is just a linear combination of the coefficients of a Weierstrass equation of E. From the definition of E^σ it follows that

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

From (a) we have that $\mathrm{End}(E^\sigma) = R_K$. We know that $\#\mathfrak{ELL}(R_K)$ is finite, so E^σ can only take a finite number of different isomorphism classes as σ ranges over the automorphism ring. Thus $[\mathbb{Q}(j(E)) : \mathbb{Q}] < \infty$ and $j(E)$ is an algebraic number.

(c) This follows from (b) and Theorem 4.1 and Theorem 4.4. □

4.5 Galois group action

We have seen that we have an action

$$\mathrm{Gal}(\overline{K}/K) \times \mathfrak{ELL}(R_K) \to \mathfrak{ELL}(R_K)$$

given by $\sigma \times E = E^\sigma$. We have also seen that the action

$$\mathfrak{CL}(K) \star \mathfrak{ELL}(R_K) \to \mathfrak{ELL}(R_K)$$

is simply-transitive. This means that there is a unique fractional ideal $A_\mathfrak{a}$ such that $[\mathfrak{a}] \star E = E^\sigma$, and this induces a map

$$F\colon \mathrm{Gal}(\overline{K}/K) \to \mathfrak{CL}(K)$$

defined by

$$E^\sigma = F(\sigma) \star E \quad \text{for all } \sigma \in \mathrm{Gal}(\overline{K}/K)$$

We will now show that this map is a group-homomorphism and that it is independent of the elliptic curve we have chosen.

Lemma 4.16. *Let K be a quadratic imaginary field with maximal order R_K. Then there is a group-homomorphism*

$$F\colon \mathrm{Gal}(\overline{K}/K) \to \mathfrak{CL}(K)$$

which is uniquely given by

$$E^\sigma = F(\sigma) \star E$$

for all $\sigma \in \mathrm{Gal}(\overline{K}/K)$ and all $E \in \mathfrak{ELL}(R_K)$.

We need the following Lemma

Lemma 4.17. *Let K be an imaginary quadratic field as before. Let $E/\overline{K}$ be an elliptic curve in $\mathfrak{ELL}(R_K)$, $[\mathfrak{a}]$ a divisor class in $\mathfrak{CL}(K)$ and σ an element in $\mathrm{Gal}(\overline{K}/K)$. Then*

$$([\mathfrak{a}] \star E)^\sigma = [\mathfrak{a}]^\sigma \star E^\sigma.$$

Proof. Proposition II.2.5 of [11] and Lemma 3.24. □

Proof of Lemma 4.16. We have seen that for given $\sigma \in \mathfrak{Gal}(\overline{K}/K)$ and $E \in \mathfrak{ELL}(R_K)$ we get a map which satisfies $E^\sigma = F(\sigma)\star E$. First we show that this is a homomorphism. For any $\sigma, \tau \in \mathfrak{Gal}(\overline{K}/K)$ we get

$$F(\sigma\tau) \star E = E^{\sigma\tau} = (F(\tau) \star E)^\sigma = F(\sigma) \star (F(\tau) \star E) = (F(\sigma)F(\tau)) \star E,$$

which shows that F is a group homomorphism.

We now show that this map is independent of the choice of E. So let E_1 and E_2 be in $\mathfrak{ELL}(R_K)$ and $\sigma \in \mathrm{Gal}(\overline{K}/K)$. We can find divisor classes $[\mathfrak{a}_1]$ and $[\mathfrak{a}_2]$ such that

$$E_1^\sigma = [\mathfrak{a}_1] \star E_1$$
$$E_2^\sigma = [\mathfrak{a}_2] \star E_2.$$

So we need to show that $[\mathfrak{a}_1] = [\mathfrak{a}_2]$. We have seen that $\mathfrak{CL}(K)$ acts transitively on $\mathfrak{ELL}(R_K)$, so there exists a $[\mathfrak{b}] \in \mathfrak{CL}$ such that $E_2 = [\mathfrak{b}] \star E_1$. Since $\mathfrak{b} \in K$, $[\mathfrak{b}]^\sigma = [\mathfrak{b}]$. Using this and the previous Lemma, we get

$$[\mathfrak{b}] \star E_1^\sigma = ([\mathfrak{b}] \star E_1)^\sigma = E_2^\sigma = [\mathfrak{a}_2] \star ([\mathfrak{b}] \star E_1) = [\mathfrak{a}_2][\mathfrak{b}][\mathfrak{a}_1^{-1}] \star E_1^\sigma.$$

Since $\mathfrak{CL}(K)$ acts freely on $\mathfrak{ELL}(R_K)$, there is only the identity element of $\mathfrak{CL}(K)$ that sends E_1 to E_1, and this shows that $[\mathfrak{a}_1] = [\mathfrak{a}_2]$ and proves the Lemma. □

4.6 The Hilbert class field

In this section we will prove the following Theorem

Theorem 4.18. *Let K be an imaginary quadratic field with maximal order R_K. Let E be an elliptic curve representing a class in $\mathfrak{ELL}(R_K)$. Then*

(a) $K(j(E)) = H_K$, the Hilbert class field of K.

(b) $[\mathbb{Q}(j(E)) : \mathbb{Q}] = [K(j(E)) : K] = \#\mathfrak{ELL}(R_K) = \#\mathfrak{CL}(K) = h_K =$ *the class number of* K.

(c) Let $E_1, \ldots, E_h$ *be a complete set of representatives of* $\mathfrak{ELL}(R_K)$. *Then* $\mathfrak{J} = j(E_1), \ldots, j(E_{h_K})$ *is a complete set of Galois-conjugates of* $j(E)$ *in* $\mathrm{Gal}(\overline{K}/K)$.

We start with proving a lemma which deals with the homomorphism

$$F\colon \mathrm{Gal}(\overline{K}/K) \to \mathfrak{CL}(K)$$

defined earlier.

Lemma 4.19. *Let* K *be an imaginary quadratic field. There exists a finite set of rational primes* $S \subset \mathbb{Z}$, *such that if any rational prime* $p \notin S$ *splits in* K, *say* $(p) = \mathfrak{p}\mathfrak{p}'$, *then*

$$F(\sigma_{\mathfrak{p}}) = [\mathfrak{p}],$$

where $\sigma_{\mathfrak{p}}$ *is the Frobenius element that corresponds to* $\mathfrak{p}$.

Proof. We will need the following facts.

(a) Let $L \subseteq \mathbb{C}$ be a field. Let E_1/L and E_2/L be elliptic curves. Then there exists a finite extension L'/L such that any $\phi \in \mathrm{Hom}(E_1, E_2)$ is defined over L'. ([11] II.2.2.c)

(b) Let E_1 and E_2 be elliptic curves defined over a field of non-zero characteristic. Then any $\psi\colon E_1 \to E_2$ factors as

$$E_1 \xrightarrow{\phi} E_1^{(q)} \xrightarrow{\lambda} E_2$$

where q is the inseparable degree of ψ, ϕ is the qth Frobenius map and λ is separable. This means that for non-separable maps, we can factor out the inseparability in a Frobenius map. ([10] II.2.12)

(c) Let E_1 and E_2 be curves. Any map $\phi\colon E_1 \to E_2$ induces a map on differentials $\phi^*\colon \Sigma_{E_2} \to \Sigma_{E_1}$. Further ϕ is separable if and only if ϕ^* is non-zero. ([10] II.4.2.c)

We have seen that $\mathfrak{ELL}(R_K)$ is finite and that any $E/\mathbb{C} \in \mathfrak{ELL}(R_K)$ can be represented by a curve $E/\overline{\mathbb{Q}}$. This means that we can find a finite extension L/K and elliptic curves $E_1/L, \ldots, E_n/L$ representing each class in $\mathfrak{ELL}(R_K)$. Using fact (a) we can choose L in such a way that any $\phi \in \mathrm{Hom}(E_i, E_j)$ is defined over L, for all i, j.

We now construct a finite set of rational primes, S. This set consists of all "bad" primes. More precisely, a prime p is in S if it satisfies any of the following conditions.

(i) p ramifies in L.

(ii) There is a prime divisor of L which divides p in which E_i has bad reduction, for some i.

(iii) Write v_p for the p-adic valuation of $\mathbb{Q}$.

$$v_p(\mathrm{N}_{\mathbb{Q}}^{L}(j(E_i) - j(E_j))) \neq 0$$

for some $i \neq j$.

Condition (iii) ensures that distinct E_is reduces to distinct $\tilde{E}_i$s.

Take a rational prime $p \notin S$ such that $(p) = \mathfrak{p}\mathfrak{p}'$. Let $\mathfrak{b}$ be a prime divisor of L dividing $\mathfrak{p}$. Choose an integral divisor $\mathfrak{a}$ relative prime to p such that $\mathfrak{a}\mathfrak{p}$ is principal, say $\mathfrak{a}\mathfrak{p} = (\alpha)$, $\alpha \in K$. Let $E \cong \mathbb{C}/\Lambda$ be an elliptic curve. We now use Theorem 4.6 and the fact that divisors and ideals are isomorphic and get the following commutative diagram.

$$\begin{array}{ccccccccc}
\mathbb{C}/\Lambda & \xrightarrow[z\mapsto z]{} & \mathbb{C}/A_{\mathfrak{p}}^{-1}\Lambda & \xrightarrow[z\mapsto z]{} & \mathbb{C}/A_{\mathfrak{a}\mathfrak{p}}^{-1}\Lambda & \xrightarrow{=} & \mathbb{C}/(\alpha)^{-1}\Lambda & \xrightarrow[z\mapsto \alpha z]{\sim} & \mathbb{C}/\Lambda \\
\downarrow\sim & & \downarrow\sim & & \downarrow\sim & & \downarrow\sim & & \downarrow\sim \\
E & \xrightarrow[\phi]{} & [\mathfrak{p}]\star E & \xrightarrow[\psi]{} & [\mathfrak{a}]\star[\mathfrak{p}]\star E & \xrightarrow{=} & [(\alpha)]\star E & \xrightarrow[\lambda]{\sim} & E
\end{array}$$

Choose a Weierstrass equation for E, which is minimal at $\mathfrak{b}$

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

Then the invariant differential of E is

$$\omega = \frac{\mathrm{d}x}{2y + a_1x + a_2}.$$

The differential of $\mathbb{C}/\Lambda$ which corresponds to ω is a multiple of $\mathrm{d}z$. The map in the top row of our diagram is $z \mapsto \alpha z$. We look at $\mathrm{d}z$ as a function and pull it back, getting

$$\alpha^*(\mathrm{d}z) = \mathrm{d}(\alpha z) = \alpha \mathrm{d}z.$$

Using the commutativity of the diagram, we see that

$$(\lambda \circ \psi \circ \phi)^*\omega = \alpha\omega.$$

We reduce E modulo $\mathfrak{b}$ and get the curve $\tilde{E}$. The invariant differential of $\tilde{E}$ is then

$$\tilde{\omega} = \frac{\mathrm{d}x}{\tilde{2}y + \tilde{a_1}x + \tilde{a_2}}.$$

Since $\mathfrak{b}$ divides $\mathfrak{p}$ and $(\alpha) = \mathfrak{a}\mathfrak{p}$ we get

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

Using fact (c), we see that $\tilde{\lambda} \circ \tilde{\psi} \circ \tilde{\phi}$ is inseparable. We have

$$\begin{aligned}
\deg\tilde{\phi} &= \deg\phi &&= \mathrm{N}_{\mathbb{Q}}^{\mathrm{K}}\mathfrak{p} = p \\
\deg\tilde{\psi} &= \deg\psi &&= \mathrm{N}_{\mathbb{Q}}^{\mathrm{K}}\mathfrak{a} \\
\deg\tilde{\lambda} &= \deg\lambda &&= 1 \text{ since } \lambda \text{ is an isomorphism}
\end{aligned}$$

Recall that we chose $\mathfrak{a}$ relative prime to p, so both $\tilde{\lambda}$ and $\tilde{\psi}$ are separable. So since $\tilde{\lambda} \circ \tilde{\psi} \circ \tilde{\phi}$ is inseparable, we must have that

$$\tilde{\phi} \colon \tilde{E} \to \widetilde{[\mathfrak{p}] \star E}$$

is inseparable. We can now use fact (b), and since $\deg \tilde{\phi} = p$ we get the following factorization of $\tilde{\phi}$

$$\tilde{E} \xrightarrow[\text{Frobenius}]{p\text{th}} \tilde{E}^{(p)} \xrightarrow{\sim} \widetilde{[\mathfrak{p}] \star E},$$

into a Frobenius map and an isomorphism. Hence $j(\widetilde{[\mathfrak{p}] \star E}) = j(\tilde{E}^{(p)}) = j(\tilde{E})^p$ and we get

$$j([\mathfrak{p}] \star E) \equiv j(E)^{\mathrm{N}_{\mathbb{Q}}^{K}(\mathfrak{p})} \equiv j(E)^{\sigma_{\mathfrak{p}}} = j(E^{\sigma_{\mathfrak{p}}}) = j(F(\sigma_{\mathfrak{p}}) \star E) \pmod{\mathfrak{b}}.$$

Since we chose $p \notin S$, this means that $[\mathfrak{p}] \star E = F(\sigma_{\mathfrak{p}}) \star E$. We know that the action of $\mathfrak{CL}(K)$ on $\mathfrak{ELL}(R_K$ is free, so we get

$$[\mathfrak{p}] = F(\sigma_{\mathfrak{p}})$$

□

Proof of 4.18. Let L/K be a finite extension characterized by that L is the fixed field of the kernel of

$$F \colon \mathrm{Gal}(\overline{K}/K) \to \mathfrak{CL}(K).$$

Then, using that $\mathfrak{CL}(K)$ acts simply-transitively on $\mathfrak{ELL}(R_K)$ we can write

$$\begin{aligned}
\mathrm{Gal}(\overline{K}/L) &= \ker F \\
&= \{\sigma \in \mathrm{Gal}(\overline{K}/K) \colon F(\sigma) = 1\} \\
&= \{\sigma \in \mathrm{Gal}(\overline{K}/K) \colon F(\sigma) \star E = E\} \\
&= \{\sigma \in \mathrm{Gal}(\overline{K}/K) \colon E^{\sigma} = E\} \\
&= \{\sigma \in \mathrm{Gal}(\overline{K}/K) \colon j(E)^{\sigma} = j(E)\} \\
&= \mathrm{Gal}(\overline{K}/K(j(E))),
\end{aligned}$$

and $L = K(j(E))$. From the choice of L we see that

$$F \colon \mathrm{Gal}(L/K) \to \mathfrak{CL}(K)$$

is injective. Since $\mathfrak{CL}(K)$ is abelian, it follows that $K(j(E))$ is an an abelian extension of K.

Let $\mathfrak{c}_{L/K}$ be the conductor of L/K and consider the composition of the artin map and F,

$$F((\cdot, L/K)) \colon I(\mathfrak{c}_{L/K}) \to \mathfrak{CL}(K).$$

Take any divisor $\mathfrak{a} \in I(\mathfrak{c}_{L/K})$ and let S be a finite set of "bad" primes, as in the previous Lemma. From Theorem 3.32 we can find a prime $\mathfrak{p} \in I(\mathfrak{c}_{L/K})$ of degree 1 over $\mathbb{Q}$, not lying over any prime in S and which satisfies

$$\begin{aligned} \mathfrak{a} &= (\alpha)\mathfrak{p} \\ \alpha &= 1 \pmod{\mathfrak{c}_{L/K}} \end{aligned}$$

for some $\alpha \in K$. We use this and the definition of the conductor and get,

$$\begin{aligned} F((\mathfrak{a}, L/K)) &= F(((\alpha)\mathfrak{p}, L/K)) \\ &= F((\mathfrak{p}, L/K)) \quad \text{since } (\alpha) \text{ is principal divisors} \\ &= [\mathfrak{p}] \quad \text{Lemma 4.19} \\ &= [\mathfrak{a}] \end{aligned}$$

Hence, the map $F((\cdot, L/K))$ is just the natural projection of $I(\mathfrak{c}_{L/K})$ into $\mathfrak{CL}(K)$. We see that $F(((\alpha), L/K)) = 1$ for any principal divisor $(\alpha) \in I(\mathfrak{c}_{L/K})$ and since $F\colon \mathrm{Gal}(L/K) \to \mathfrak{CL}(K)$ is injective, it follows that

$$((\alpha), L/K) = 1 \text{ for any principal divisor } (\alpha) \in I(\mathfrak{c}_{L/K}).$$

From the definition of the conductor, we must have $\mathfrak{c}_{L/K} = (1)$. Hence there are no primes of K that ramify in L. We conclude that L is contained in the Hilbert class field of K.

Now since $\mathfrak{c}_{L/K} = (1)$, the map $F((\cdot, L/K))\colon I((1)) \to \mathfrak{CL}(K)$ is clearly surjective. We thus get that

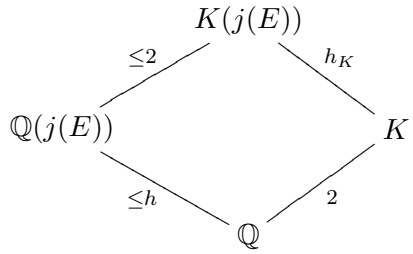
$$F\colon \mathrm{Gal}(L/K) \to \mathfrak{CL}(K)$$

is surjective, and hence an isomorphism. We can now write the following,

$$[L : K] = \#\mathrm{Gal}(L/K) = \#\mathfrak{CL}(K) = \#\mathrm{Gal}(H/K) = [H : K].$$

Since $L \subseteq H$, we see that $L = K(j(E)) = H$, which proves point (a).

We see from the arguments in the proof of Theorem 4.15(b) that the degree $[\mathbb{Q}(j(E)) : \mathbb{Q}]$ is not larger than the class number of K. We thus get this tower of fields.



We see that $[\mathbb{Q}(j(E)) : \mathbb{Q}] = h_K$ and we have proved (b).

Since $\mathfrak{CL}(K)$ acts simply-transitively on $\mathfrak{ELL}(R_K)$, we get that $\mathfrak{CL}(K)$ also acts simply-transitively on the set $\mathfrak{J} = \{j(E_1), \ldots, j(E_{h_K})\}$. We have seen that $\mathrm{Gal}(L/K)$ is isomorphic to $\mathfrak{CL}(K)$. From the definition of F, this means that $\mathrm{Gal}(\overline{K}/K)$ acts transitively on $\mathfrak{J}$. It follows that $\mathfrak{J}$ is a complete set of $\mathrm{Gal}(\overline{K}/K)$ conjugates of $E(j)$. This proves (c) and the Theorem. □

Definition 4.20. Let $K = \mathbb{Q}(\sqrt{d})$ be an imaginary quadratic field with maximal order R_K. Let $E_1, \dots E_h$ be a complete set of representatives for $\mathfrak{ECL}(R_K)$ and let $j_i = j(E_i)$. The *Hilbert polynomial* corresponding to K is

$$h_K(x) = h_d(x) = (x - j_1) \dots (x - j_h).$$

From Theorem 4.18 this polynomial splits over H_K.

Theorem 4.21. *The Hilbert polynomial has integer coefficients.*

Proof. Theorem 11.2.6 of [4] □

Example 4.22. We continue from example 2.22 and look at the quadratic field $\mathbb{Q}(\sqrt{-15})$. We let R_K be the maximal order in this field. Recall that there are two equivalence classes of modules that has R_K as coefficient ring. We found the two reduced modules corresponding to these classes

$$M_1 = \{1, \frac{1 + \sqrt{-15}}{4}\} \quad \text{and} \quad M_2 = \{1, \frac{1 + \sqrt{-15}}{2}\}.$$

Since these reduced modules are full modules in an imaginary quadratic field, they can be represented as lattices in the complex plane. We know that any lattice corresponds to an elliptic curve, and the coefficient ring of the lattice corresponds to the endomorphism ring of the elliptic curve. There is a convergent series that enables us to compute an approximation of the j-invariant of a lattice.

We can numerically compute the j-invariants for the two reduced modules and construct an approximation to the Hilbert polynomial. But since the Hilbert polynomial has integer coefficients, we can find the correct Hilbert polynomial by rounding the approximation, as long as we ensure high enough precision. We compute

$$j_1 = j(M_1) \approx 632.83286$$

and

$$j_2 = j(M_2) \approx -191657.83286$$

and construct the Hilbert polynomial

$$h_{-15}(x) = (x - j_1)(x - j_2) = x^2 + 3^3 \cdot 5^2 \cdot 283x - (3^2 \cdot 5 \cdot 11)^3.$$

5 The Complex Multiplication Method

We will in this section use the theory we have described up until now. We will see how we can create an elliptic curve with specified group order over a given finite field.

5.1 The Frobenius endomorphism

We first study the Frobenius endomorphism of elliptic curves. See Section 4.2 of [12] for complete proofs.

Let $q = p^r$, where $p > 3$ is prime. Given an integer n, we wish to find an elliptic curve $\tilde{E}/\mathbb{F}_q$ such that $\#\tilde{E}(\mathbb{F}_q) = n$.

The qth power Frobenius endomorphism π sends a point $(x, y) \in \tilde{E}(\overline{\mathbb{F}}_q)$ to $(x^q, y^q) \in \tilde{E}(\overline{\mathbb{F}}_q)$. A point P is in $\tilde{E}(\mathbb{F}_q)$ if and only if $\pi(P) = P$. Hence we can count the number of $\mathbb{F}_q$-rational points of $\tilde{E}$ with the following equation.

$$n = \#\tilde{E}(\mathbb{F}_q) = \#\ker(1 - \pi) \tag{4}$$

It can be shown that for any separable endomorphism ϕ we have $\#\ker(\phi) = \deg(\phi)$ ([10] III.4.10) and that the map $(1 - \pi)$ is separable ([10] III.5.3). We use Rosati involution, which states that $\deg(\phi) \cdot 1 = \phi\hat{\phi}$, where $\hat{\phi}$ is the dual isogeny of ϕ. We know that the norm of the Frobenius π is equal to q. From this, Theorem III.6.2 of [10] and the above equation it follows that

$$n = \#\ker(1 - \pi) = 1 - \mathrm{Tr}(\pi) + \mathrm{N}(\pi) = 1 - t + q,$$

where we define $t = \mathrm{Tr}(\pi)$.

We have seen that the endomorphism ring of an elliptic curve is contained in an imaginary quadratic field. From the definition of trace and norm of an element, we deduce the following identity for an element α in a quadratic field

$$\mathrm{N}(x - \alpha) = x^2 - \mathrm{Tr}(\alpha)x + \mathrm{N}(\alpha).$$

We can consider endomorphism as elements of an imaginary quadratic field. This allows us to use the above equation and get a polynomial

$$c(x) = x^2 - tx + q,$$

with $c(\pi) = 0$. The roots of $c(x)$ can be written as

$$\frac{t \pm \sqrt{t^2 - 4q}}{2}.$$

We write $d \cdot m^2 = t^2 - 4q$, where d is squarefree. From Hasse's Theorem, we know that $d \leq 0$. If we let $K = \mathbb{Q}(\sqrt{d})$, we see that π is an element of the maximal order R_K of an imaginary quadratic field K.

We will find an elliptic curve over $\mathbb{C}$ with endomorphism ring equal to R_K, and then reduce this to get a curve over $\mathbb{F}_q$. Since the endomorphism ring is preserved under reduction we will get an elliptic curve with a Frobenius satisfying equation (4).

We have seen that there is a correspondence between elliptic curves $E/\mathbb{C}$ and lattices $\Lambda \subset \mathbb{C}$. We consider the case when lattices are full modules in some quadratic imaginary field. From Theorem 4.8 we see that the endomorphism ring of E is isomorphic to the coefficient ring of Λ. We are therefore interested in finding full modules of the field K with coefficient ring equal to the maximal order R_K. By finding the j-invariant to any of these full modules, we get an elliptic curve with the proper endomorphism ring.

From Theorem 4.15 we know that the j-invariant of an elliptic curve $E/\mathbb{C}$ with complex multiplication by R_K is defined over $\overline{\mathbb{Q}}$. There is an convergent sum which gives us the j-invariant, but computing this directly is not feasible. Instead we create the Hilbert polynomial of K, $h_K(x)$. Recall that the Hilbert polynomial is defined as

$$h_K(x) = (x - j_1) \dots (x - j_h),$$

where the js are the j-invariants corresponding to non-isomorphic elliptic curves (or non-similar lattices), and has integer coefficients. This allows us to approximate the different j-invariants and create an approximation to the Hilbert polynomial, $\hat{h}_K(x)$. By ensuring high enough precision of this calculation, we can round the coefficients of $\hat{h}_K(x)$ and get the true $h_K(x)$.

Consider now the case where $q = p$. Then we have $4p = t^2 - dm^2$, and p splits completely into distinct primes in K, say $(p) = \mathfrak{p}\overline{\mathfrak{p}}$. However, since $p = 4\alpha\overline{\alpha}$ where $\alpha = \frac{t+\sqrt{-dm}}{2} \in K$, we see that $\mathfrak{p} = (\alpha)$ is a principal divisor. It follows that the artin map acts trivially on $\mathfrak{p}$ which implies that $x \equiv x^p \pmod{\mathfrak{b}}$ for any $x \in R_H$, where $\mathfrak{b}$ is a prime divisor dividing $\mathfrak{p}$. This means that the residue field $R_H/\mathfrak{b}$ must be equal to $\mathbb{F}_p$. From this it follows that the reduction of the Hilbert polynomial modulo p must give us a polynomial which splits completely over $\mathbb{F}_p$.

Now we look at the general case, $q = p^r$ and $4q = t^2 - dm^2$. Let $K = \mathbb{Q}(\sqrt{d})$ as usual. This means that there is some $\alpha \in K$ such that $q = \mathrm{N}(\alpha)$ and α is a root of $x^2 - tx + q$. Let H be the Hilbert class field of K and $h(x) \in \mathbb{Z}[x]$ the Hilbert polynomial, with degree $h = |\mathrm{Gal}(H/K)|$.

If p remains prime in K, the residue field $R_K/(p)$ is the field $\mathbb{F}_{p^2}$. We also have that the Artin map acts trivially on (p), since it is a principal divisor. It follows that the residue field $R_H/\mathfrak{b} = \mathbb{F}_{p^2}$, where $\mathfrak{b} \in R_H$ is a prime dividing (p). This is not the situation we want. We therefore require that p splits into two primes in K.

So let $(p) = \mathfrak{p}\mathfrak{p}'$ in K, and let $\mathfrak{p} = \mathfrak{b}_1 \dots \mathfrak{b}_s$ in H. We now use results which were presented in Section 3.9. We write $\mathbb{F}_\mathfrak{b} = R_H/\mathfrak{b}$ and $\mathbb{F}_\mathfrak{p} = R_K/\mathfrak{p}$. We have seen that all the stabilizer subgroups $G_{\mathfrak{b}_i} = \{\sigma \in G \colon \sigma(\mathfrak{b}_i) = \mathfrak{b}_i\}$ are equal and isomorphic to $\mathrm{Gal}(\mathbb{F}_\mathfrak{b}/\mathbb{F}_\mathfrak{p})$. From this we saw that $|\mathbb{F}_\mathfrak{b}/\mathbb{F}_\mathfrak{p}| = |G_\mathfrak{b}| = h/s = f_\mathfrak{b}$.

Suppose $(\alpha) = \mathfrak{a}\mathfrak{a}'$ for a prime divisior $\mathfrak{a}$ and some divisor $\mathfrak{a}'$. Then

$$\mathrm{N}(\alpha) = \mathrm{N}(\mathfrak{a}\mathfrak{a}') = \mathrm{N}(\mathfrak{a})\mathrm{N}(\mathfrak{a}') = q = p^r.$$

It follows that $\mathfrak{a} = \mathfrak{p}$ or $\mathfrak{a} = \mathfrak{p}'$, hence these are the only primes dividing (α). Now let

$$(\alpha) = \mathfrak{p}^k\mathfrak{p}'^{k'}.$$

Since $\mathrm{N}(\mathfrak{p}) = \mathrm{N}(\mathfrak{p}') = p$, we have $k + k' = r$.

Let both k and k' be non-zero and assume $k \geq k'$. Then

$$(\alpha) = (\mathfrak{p}\mathfrak{p}')^{k'}\mathfrak{p}^{k-k'} = (p)^{k'}\mathfrak{p}^{k-k'}.$$

Since p divides (α), we deduce that p must divide the trace of α, i.e. $p|t$. This implies that we are in the supersingular case, which is not what we are interested in. So we will only consider cases where $t \not\equiv 0 \pmod{p}$.

Because of symmetri, we can assume $k' = 0$ and $(\alpha) = \mathfrak{p}^r$. Let $(\mathfrak{p}, H/K) = \sigma_{\mathfrak{p}} \in G_{\mathfrak{b}}$ be the element which maps to Frobenius, i.e. $\sigma_{\mathfrak{p}}$ is the generator of the subgroup $G_{\mathfrak{b}}$. We use the Artin map on (α) and get $(\alpha, H/K) = (\mathfrak{p}^r, H/K) = \sigma_{\mathfrak{p}}^r = 1$. Thus $f_{\mathfrak{b}}|r$. The element $\sigma_{\mathfrak{p}}^r$ corresponds to the map $(x \mapsto x^{p^r})$, which is the Frobenius for $\mathbb{F}_q$. Hence, in this case, the reduced Hilbert polynomial must split completely in $\mathbb{F}_q$. We note that it may split over some smaller extension of $\mathbb{F}_p$, but we are interested in points over $\mathbb{F}_q$. Also if the number of points is prime, we can use Hasse's Theorem and see that the curve is defined over $\mathbb{F}_q$.

To complete the procedure, we reduce the Hilbert polynomial modulo p and take a root j_0 of $h_K(x) \mod p$. From the above discusssion we see that this root lies in $\mathbb{F}_q$. From Corollary 4.12 there is a curve and with j-invariant equal to j_0 with endomorphism ring R_K. We assume that we are not in the special case where $j_0 = 0$ or $j_0 = 1728$. We can then use Theorem 4.3 and quickly determine the correct curve from the reduced j-invariant.

We summarize the method to create an elliptic curve over a finite field $\mathbb{F}_q$ with order n, where $\mathrm{char}(\mathbb{F}_q) > 3$. Let $q = p^r$ and $t = q + 1 - n$. If $|t| \leq 2\sqrt{q}$ and $t \not\equiv 0 \pmod{p}$ we can find such a curve with the following steps.

(1) Write $d \cdot m^2 = t^2 - 4q$, with m integer and d square-free. Let $K = \mathbb{Q}(\sqrt{d})$.

(2) Check that p splits completely in K. Go to step (1) and find a new d if this fails.

(3) Compute $h_K(x)$, the Hilbert polynomial of K.

(4) Find a root j_0 of $h_K(x)$ over $\mathbb{F}_q$.

(5) Compute the elliptic curve with j-invariant equal to j_0, taking the twist if needed. This curve will have the correct group order over $\mathbb{F}_q$.

We note that the computation required to find and reduce the Hilbert polynomial increase with both $|d|$ and the class number of K. We are therefore interested in keeping these small. The class number can be checked before computing the Hilbert polynomial. One could also consider using Tables of class numbers to exclude certain values of d.

Remark: This can easily be generalized for $p = 2, 3$. There are only a few places we require this condition.

5.2 Pairing friendly curves

Let $E/\mathbb{F}_q$ be an elliptic curve, with $q = p^r$. Let m be an integer not divisible by p. Then the subgroup

$$E[m] = \{P \in E(\overline{\mathbb{F}}_q) \colon mP = \mathcal{O}\}$$

is isomorphic to $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$. There exists a non-degenerate bilinear pairing

$$e_m \colon E[m] \times E[m] \to \mu_m$$

where $\mu_m \in \overline{\mathbb{F}}_q$ is the mth roots of unity. The set μ_m forms a cyclic group of order m. If $E[m] \subseteq E(\mathbb{F}_{q^k})$, it can be shown that $\mu_m \subseteq \mathbb{F}^*_{q^k}$. The smallest such k is known as the *embedding degree* of $E[m]$. Pairing-based cryptography uses such a pairing and requires that the Discrete Logarithm Problem (DLP) is hard enough both in $E[m]$ and in μ_m. Since $\mu_m \subseteq \mathbb{F}^*_{q^k}$ one can use the more efficient index calculus method. Hence, we must make sure that k is sufficiently large. If k is too large however, the efficiency of the cryptosystem suffers. Current methods to solve DLP suggests that $k = 6$ is a good choice. But as computer power increases, k must also increase if the crypto system should maintain security and optimal efficiency.

Since $\#F^*_{q^k} = q^k - 1$ and the order of any subgroup must divide this, we can determine the embedding degree of $E[m]$ by

$$\begin{aligned} &m | q^k + 1 \\ &m \nmid q^s + 1 \quad \text{for any } 1 \leq s < k \end{aligned}$$

The kth cyclotomic polynomial $\Phi_k(x)$ has precisely the property that $m | \Phi_k(q)$. For $k = 6$ we have $\Phi_6(x) = x^2 - x + 1$.

This puts strict limitations on the elliptic curves which can be used.

5.3 Examples

We are now ready to find some elliptic curves.

We search only for curves over finite fields of prime order. We require the curve to have a subgroup whose embedding degree is 6. Since $\Phi_6(x) = x^2 - x + 1$ we get the following constraints, where $t = p + 1 - n$,

p	prime
$n = ur$	where r is prime and u is small
$r \mid (p^2 - p + 1)$	
$\lvert t \rvert \leq \sqrt{2p}$	
$t^2 - dm^2 = 4p$	has a solution with small d.

We limit our search to $-d < 30$. Ideally we would like $u = 1$, but there are no such curves for $100 < p < 10^7$. We loosen our requirements and accept $u < 30$.

Example 5.1. We now find many candidates and pick the following.

$$\begin{aligned} p &= 1699 \\ \Phi_6(p) &= 7 \cdot 19 \cdot 109 \cdot 199 \\ n &= 16 \cdot 109 = 1744 \\ d &= -15 \end{aligned}$$

Since $d = -15$ we need the Hilbert polynomial corresponding to $K = \mathbb{Q}(\sqrt{-15})$. We have computed this in a previous example,

$$h_{-15}(x) = x^2 + 3^3 \cdot 5^2 \cdot 283x - (3^2 \cdot 5 \cdot 11)^3.$$

We now reduce this polynomial modulo $p = 1699$ and get

$$\begin{aligned} h_{-15}(x) &\equiv x^2 + 737x + 837 \mod 1699 \\ &\equiv (x + 100)(x + 637) \mod 1699 \end{aligned}$$

We take a zero of $h_{15}(x)$ over $\mathbb{F}_{1699}$ and get the j-invariant $j_1 = 1599$. We find a curve E_1 with this j-invariant.

$$E_1 \colon y^2 = x^3 + 1104x + 736$$

But calculating the number of points on E_1 reveals that this is not the curve we are looking for. We take the twist of E_1 and get

$$E_{1T} \colon y^2 = x^3 + 1018x + 791.$$

We know that this curve is the correct one, and a calculation gives us

$$\#E_{1T} = 16 \cdot 109.$$

We have found an elliptic curve with a subgroup of order 109 over $\mathbb{F}_{1699}$. This subgroup has embedding degree 6.

Example 5.2. We pick another candidate, given by

$$\begin{aligned} p &= 73709 \\ \Phi_6(p) &= 3 \cdot 19 \cdot 43 \cdot 727 \cdot 3049 \\ n &= 24 \cdot 3049 = 73176 \\ d &= -5 \end{aligned}$$

The maximal order in $K = \mathbb{Q}(\sqrt{-5})$ is $R_K = \{1, \sqrt{-5}\}$ and has discriminant $D = -20$. We first find the reduced modules of the maximal order. We recall that the reduced modules are on the form $\{1, \gamma\}$ and $\gamma \in K$ is reduced. We denoted a triple of integers

(a, b, c) as the unique set such that $a\gamma^2 + b\gamma + c = 0$, $a > 0$ and g.c.d$(a, b, c) = 1$. This allowed us to write

$$\gamma = \frac{-b + \sqrt{D}}{2a}.$$

Since we are interested in reduced modules only, we saw that we got these constraints

$$\begin{aligned} D &= b^2 - 4ac \\ -a \leq b < a &< \sqrt{\tfrac{-D}{3}} \\ c &\geq a \qquad \text{for} \quad b \leq 0 \\ c &> a \qquad \text{for} \quad b > 0 \end{aligned}$$

Now since $D = -20$ and $c = \frac{b^2 - D}{4a}$ must be an integer, we need b to be an even integer. We see that the only valid values for b is 0 and -2. We are therefore limited to the following cases

$$\begin{array}{llll} a = 1 & b = 0 & c = 5 & \\ a = 1 & b = -2 & c = 6 & \text{not valid since } -a > b \\ a = 2 & b = 0 & c = 5/2 \notin \mathbb{Z} & \\ a = 2 & b = -2 & c = 3. & \end{array}$$

Hence, there are two different sets of triples which give us a reduced module. So we have the two reduced modules $\{1, \gamma_1\}$ and $\{1, \gamma_2\}$ where

$$\begin{aligned} \gamma_1 &= \frac{0^2 + \sqrt{-20}}{2 \cdot 1} = \sqrt{-5} \\ \gamma_2 &= \frac{(-2)^2 + \sqrt{-20}}{2 \cdot 2} = \frac{1 + \sqrt{-5}}{2}. \end{aligned}$$

To calculate the Hilbert polynomial we have seen that we need to find all non-isomorphic elliptic curve with endormophism ring equal to R_K. The correspondence between lattices and elliptic curves allowed us to find the non-similar lattices with R_K as coefficient ring. We could also calculate the j-invarient directly from the lattices using convergent sums. This means that we can calculate the j-invariant from the two reduced modules we have found and build the Hilbert polynomial. We get

$$\begin{aligned} j_1 = j(\{1, \gamma_1\}) = j(\sqrt{-5}) &\cong 1264538.9094751 \\ j_2 = j(\{1, \gamma_2\}) = j(\frac{1 + \sqrt{-5}}{2}) &\cong -538.9094772 \end{aligned}$$

and the Hilbert polynomial is

$$h_{-20} = (x - j_1)(x - j_2) = x^2 - 2^7 \cdot 5^3 \cdot 79x - 880^3.$$

We reduce the Hilbert polynomial and factor it to get

$$h_{-20} \equiv (X + 24272)(x + 38490) \pmod{73709}.$$

We take $j = -24272$ and calculate an elliptic curve over $\mathbb{F}_{73709}$ corresponding to this j-invariant,

$$\tilde{E}\colon y^2 = x^3 + 17642x + 36331.$$

This time we do not need to take the twisted curve, as a calculation of the group order reveals that $\#\tilde{E} = 2^3 \cdot 3 \cdot 3049$, and we have the subgroup we were looking for.

Example 5.3. We search for a curve with a subgroup with embedding degree 7. We find the parameters $p = 10861$, $n = 4 \cdot 2731$ and $d = -11$. Calculating the reduced modules reveal that $\mathbb{Q}(\sqrt{-11})$ has class number one, and we find the j-invariant to be $j = -32768$. With class number one, we do not need to build the Hilbert polynomial, since it has degree one. We simply reduce j modulo p. The first curve we try, is not the correct one. So after taking the twist we get the following curve

$$E_T\colon y^2 = x^3 + 10769x + 7118$$

with $\#E_T/\mathbb{F}_{10861} = 4 \cdot 2731$.

5.4 Improving the CM-method

The method we have described for generating elliptic curves has some weaknesses. If we are interested in curves which are usable in cryptography, we need a group order of atleast 160 bits. To have much hope of finding elliptic curves of this size, we need to accept much larger discriminants. The problem with this is that the coefficients of the Hilbert polynomial quickly gets huge, as they grow exponentially as the discriminant grows. To remedy this, it is possible to use Weber polynomials. This involves using different elements to generate the Hilbert class field, and by choosing these carefully one can get a polynomial with relatively small coefficients. The theory of Weber polynomials can be found in [13]. Both [1] and [7] used Weber polynomials in their algorithms.

In our examples to find pairing-friendly curves, we found suitable candidates with a naive search. This can be improved using simple number theory. Scott and Baretto [9] uses efficient solving of the Pell equation to speed up the search.

6 Concluding Comments

We have presented the CM-method and the mathematical theory needed to understand it. We have extended the method to handle any finite field.

The theory of orders, divisors and class fields is very general and has applications in both pure and applied mathematics.

This area of research has just recently found applications in cryptography, and there are still many open problems.

References

[1] "Elliptic Curves and Primality Proving", A. O. L. Atkin and F. Morain, Mathematics of Computation, Vol. 61, Number 203, pages 29-68 (1993).

[2] "Identity-Based Encryption from the Weil Pairing", Dan Boneh and Matthew Franklin, SIAM J. of Computing, Vol. 32, No. 3, pages 586-615 (2003).

[3] "Number Theory", Z. I. Borevich and I. R. Shafarevich, Academic Press (1966).

[4] "Introduction to the construction of class fields", Harvey Cohn, Cambridge University Press (1985).

[5] "Algebraic Number Theory", S. Lang, Addison Wesley (1970).

[6] "Elliptic Functions", S. Lang, Springer-Verlag (1987).

[7] "Constructing Elliptic Curves with Given Group Order over Large Finite Fields", George-Johann Lay and Horst G. Zimmer, Algorithmic Number Theory, volume 877 of Lecture Notes in Computer Science, pages 250-263, Springer-Verlag (1994).

[8] "Elliptic Curves over Finite Fields and the Computation of Square Roots mod p", R. Schoof, Math. Comp., 44(170), pages 483-494 (1985).

[9] "Generating more MNT elliptic curves", Michael Scott and Paulo S. L. M. Barreto, Design, Codes and Cryptography, Volume 38, Number 2 (2005).

[10] "The Arithmetics of Elliptic Curves", Joseph H. Silverman, Springer-Verlag (1986).

[11] "Advanced Topics in the Arithmetic of Elliptic Curves", Joseph H. Silverman, Springer-Verlag (1994).

[12] "Elliptic curves, number theory and cryptography", Lawrence C. Washington, Chapman & Hall/CRC (2003).

[13] "Lehrbuch der Algebra, Vol. III", Heinrich Weber, Chelsea Publishing Company (1908).