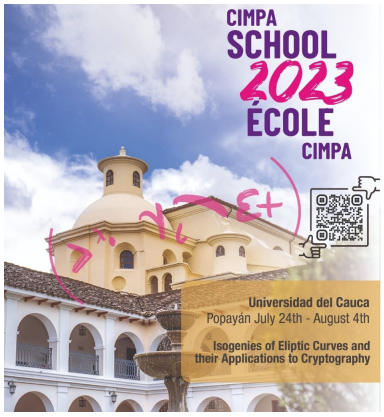

Algebraic Number Theory

Lecture Notes for CIMPA School
Isogenies of elliptic curves and their applications to cryptography

Amalia Pizarro Madariaga
Universidad de Valparaíso
amalia.pizarro@uv.cl

July 26, 2023

Contents

1 Introduction

The beginning of the *Number Theory* is related to the problem of finding integer solutions to algebraic equations $F(x_1, \ldots, x_n) = 0$, where arise the algebraic numbers. For example, find the integer solutions of the *Pell equation* $x^2 - d \cdot y^2 - 1 = 0$, where $d > 1$ and square-free. If we write $x^2 - d = (x - \sqrt{d} \cdot y) \cdot (x + \sqrt{d} \cdot y)$, it is known that the integer solutions (m, n) of this equation corresponds to the invertible elements $m + n \cdot \sqrt{d}$ of the ring $\mathbb{Z}[\sqrt{d}]$ with norm equals to 1. Something similar happens when we study the equation $x^p + y^p - z^p = 0$, which is a case of the Last Fermat Theorem. Here, the proper ring to be considered is $\mathbb{Z}[\zeta_p]$ where ζ_p is a p-th root of unity. From here, to see the importance to study the algebraic and arithmetic properties of this kind of ring. Like a generalization of the integers, arise the concept of *ring of algebraic integers* of a number field.

2 Number fields and ring of integers

Algebraic number theory studies the arithmetic aspects of the number fields. Such fields are involved in the solution of many rational problems, such as the following diophantine problems.

Pell Equation Find integer numbers x, y such that $x^2 - dy^2 - 1 = 0$, with $d > 1$ squarefree. Note that $x^2 - dy^2 = (x - \sqrt{d}y)(x + \sqrt{d}y)$, if we consider the ring $\mathbb{Z}[\sqrt{d}] = \{a + b\sqrt{d} : a, b \in \mathbb{Z}\}$. So, to solve this diophantine equation is equivalent to looking into $\mathbb{Z}[\sqrt{d}]^*$.

Pythagorean triples :Find integers numbers without common factors x, y, z such that $x^2 + y^2 = z^2$.
Observe that $x^2 + y^2 = (x + yi)(x - iy)$ in $\mathbb{Z}[i]$.]It is known that $\mathbb{Z}[i]$ in a unique factorization domain (exercise), so each element in $\mathbb{Z}[i]$ can be written uniquely (unless order and multiplication by units) as the product of irreducible elements. By using this fact, it is possible to prove that $x + iy = u\alpha^2$, with $\alpha, u \in \mathbb{Z}[i]$ and u a unit (i.e $u \in \{\pm 1, \pm i\}$.) (exercise).
If $\alpha = m + ni$, with $m, n \in \mathbb{Z}$, then

$$x + iy = \pm(m + ni)^2 = \pm(m^2 + 2mni - n^2),$$

i.e., $x = \pm(m^2 - n^2), y = \pm 2mn$. Therefore, $z^2 = (m^2 + n^2)^2$ and $z = \pm(m^2 + n^2)$. m and n must be relatively primes and not both odd.
A natural question is whether it is possible to apply this idea to solve the general case $x^n + y^n = z^n$, with $n > 2$.
Fermat [1] conjectured that there is no integer solution non zero for $n > 2$. To study this problem,

[1] Now it is known as the Last Fermat Theorem and was proved by Andrew Wiles in 94

it is enough to consider the case $n = p$, with p an odd prime.
Suppose that for some odd prime p there is a solution $x, y, z \in \mathbb{Z} - \{0\}$ with no common factors. Let us consider the following cases:

(a) p does not divide any x, y, z.

(b) p divides exactly one of them.

We will only see case (a).

- Suppose $p = 3$.If x, y, z are not multiples of 3, then $x^3, y^3, z^3 \equiv \pm 1 \pmod 9$ and $x^3 + y^3 \not\equiv z^3 \pmod 9$, so it cannot have a non-trivial solution.

- Suppose $p > 3$. Then,

$$x^p + y^p = (x + y)(x + \zeta_p y)(x + \zeta_p^2 y) \cdots (x + \zeta_p^{p-1} y) = z^p,$$

  where $\zeta_p = e^{2\pi i/p}$ in $\mathbb{Z}[\zeta_p] = \{a_{p-2}\zeta_p^{p-2} + \ldots a_1\zeta_p + a_0\}$ (exercise). Kummer claimed that $\mathbb{Z}[\zeta_p]$ is a unique factorization domain and from here, he obtained a proof of the Fermat Theorem. However, his assertion only is valid if $p < 23$. Idea: If we assume that $\mathbb{Z}[\zeta_p]$ is a UFD, it is possible to prove that $x + \zeta_p y = u\alpha^p$, for some $\alpha \in \mathbb{Z}[\zeta_p]$ and $u \in \mathbb{Z}[\zeta_p]^*$ and also that if x, y are not divisible by p, then $x \equiv y \pmod p$. Putting $x^p + (-z)^p = (-y)^p$, we obtain that $x \equiv -z \pmod p$. This implies

$$2x^p \equiv x^p + y^p \equiv z^p \equiv -x^p \pmod p,$$

  so $p \mid 3x^p$, but $p \neq 3$ and p do not divide x, which is a contradiction, and then there are no solutions to the case (a).

More general case: Dedekind discovered that although the elements of $\mathbb{Z}[\zeta_p]$ may not factor uniquely in irreducibles, the ideals of this ring always factor in a product of prime ideals. From here, it is possible to prove that the principal ideal generated by $x + \zeta_p y$ may be written as $(x + \zeta_p y) = I^p$, for some I ideal.
There are certain primes p (regular primes) for which I may be a principal ideal $I = (\alpha)$, then

$$(x + \zeta_p y) = I^p = (\alpha)^p = (\alpha^p),$$

and again $(x + \zeta_p y) = u\alpha^p$, for u a unit. Then $x \equiv y \pmod p$, which is a contradiction. For a historical approach to this concept, see [1].

2.1 Number Fields

Definition 2.1. *A field K is an **algebraic number field** if is a finite extension of $\mathbb{Q}$. Their elements will be called **algebraic numbers**, that is, they are roots of nonzero polynomials with rational coefficients. The monic polynomial $P_\alpha(x)$ of the lowest degree of which $\alpha \in K$ is a root is called de **minimal polynomial** of α.*

If α is root of $g(x) \in \mathbb{Q}[x]$, then $P_\alpha(x) | g(x)$.

Example 1. ***Quadratic fields.***
Quadratic fields are degree two extensions K of $\mathbb{Q}$ and then have the form $\mathbb{Q}(\sqrt{d})$, where we can assume that d is a square-free integer. If $d < 0$ we say that $\mathbb{Q}(\sqrt{d})$ is an imaginary quadratic field and of $d > 0$ a real quadratic field.

Example 2. ***Cyclotomic fields.***

Let $n \geq 1$ and let ζ_n be a primitive n-th root of unity in $\mathbb{C}$. The n-th cyclotomic field is the field $\mathbb{Q}(\zeta_n)$. The degree of this field over $\mathbb{Q}$ is $\phi(n)$, where ϕ is the Euler's phi function.
The minimal polynomial of ζ_n over $\mathbb{Q}$ is called the cyclotomic polynomial $\Phi_n(x)$ and it verifies the following:

(i) Let U_n be the group of n-th roots of unity in $\mathbb{C}$ and let $U_n' = \{\zeta_n^a : 0 \leq a < n, \ \ gcd(a, n) = 1\}$. Then

$$\Phi_n(x) = \prod_{\zeta \in U'} (x - \zeta).$$

(ii) $\Phi_n(x)$ is a monic polynomial with integer coefficients and irreducible over $\mathbb{Q}$. Its degree is $\phi(n)$.

(ii) $\prod_{d|n} \Phi_d(x) = x^n - 1$.

2.2 Algebraic Integers

Definition 2.2. *An element α in a number field will be called **algebraic integer** if there exists a monic polynomial $f(x) \in \mathbb{Z}[x]$ such that $f(\alpha) = 0$.*

Example 3. *$\sqrt[3]{2}, \sqrt{2} + 2$ are algebraic integers. $\frac{\sqrt{2}}{3}$ is algebraic, but it is not an algebraic integer.*

Theorem 2.1. *Let α be an algebraic integer. Then, the minimal polynomial of α has integer coefficients.*

Proof. Let $P_\alpha(x) \in \mathbb{Q}[x]$ the minimal polynomial of α and $g(x) \in \mathbb{Z}[x]$ with $g(\alpha) = 0$. Then $g = P_\alpha h$, for some $h(x) \in \mathbb{Q}[x]$. If $P_\alpha(x) \notin \mathbb{Z}[x]$, then there is a prime p dividing the denominator of some coefficient of P_α. Let p^i be the biggest power of p with this property and p^j the biggest power dividing the coefficients of h. Then:

$$p^{i+j} g = (p^i P_\alpha)(p^j h) \equiv 0 \pmod{p}.$$

Since $\mathbb{Z}/_p\mathbb{Z}[x]$ is an integral domain, we obtain that $p^i P_\alpha$ or $p^j h$ are zero mod p, which is a contradiction. □

From now, we will denote by $\mathcal{O}_K$ the set of algebraic integers in the number field K.

Corollary 2.1. *$\mathcal{O}_\mathbb{Q} = \mathbb{Z}$.*

2.3 Characterization of Algebraic Integers

Theorem 2.2. *The following assertions are equivalents:*

(i) α is algebraic integer.

(ii) $\mathbb{Z}[\alpha] = \{f(\alpha) : f(x) \in \mathbb{Z}[x]\}$ is a finitely generated $\mathbb{Z}$-module.

(iii) There exists a finitely generated $\mathbb{Z}$-module M such that $\alpha M \subseteq M$ and $\gamma M \neq \{0\}$ for all $\gamma \in \mathbb{Z}[\alpha] - \{0\}$.

Proof. *i)* $\Rightarrow$ *ii)* Let $f(x) = x^n + a_1 x + \dots a_0 \in \mathbb{Z}[x]$ and $f(\alpha) = 0$. Let us consider the following $\mathbb{Z}$-module: $M = \mathbb{Z} + \mathbb{Z}\alpha + \dots \mathbb{Z}\alpha^{n-1}$. It is clear that $M \subseteq \mathbb{Z}[\alpha]$. By induction: suppose that $\alpha^k \in M$, then:

$$\begin{aligned} \alpha^{n+k} &= \alpha^k \alpha^n \\ &= \alpha^k[-(a_{n-1}\alpha^{n-1} + \dots + a_0] \\ &= (-\alpha^k a_{n-1})\alpha^{n-1} + \dots + (-\alpha^k a_0). \end{aligned}$$

Because $-\alpha^k a_i \in \mathbb{Z}[\alpha]$ for $i = 0, 1, \dots, n-1$, we have that $\alpha^{n+k} \in M$, therefore $M = \mathbb{Z}[\alpha]$.
ii) $\Rightarrow$ *iii)*. We take $M = \mathbb{Z}[\alpha]$. As $\alpha \in M$, then $\alpha M \subseteq M$ and $\gamma = \gamma \cdot 1 \in \gamma M$.
iii) $\Rightarrow$ *i)*. Let $\{x_1, x_2 \dots x_r\}$ be a generators of M. By hypothesis $\alpha x_i \in M$, then there exists a set of integers numbers c_{ij} such that $\alpha x_i = \sum_{j=1}^{r} c_{ij} x_j$, for all $i = 1, \dots, r$. Let $C = (c_{ij})_{ij}$, then

$$C \cdot \begin{pmatrix} x_1 \\ . \\ . \\ . \\ x_r \end{pmatrix} = \alpha \cdot \begin{pmatrix} x_1 \\ . \\ . \\ . \\ x_r \end{pmatrix} \Leftrightarrow (C - \alpha I_d) \begin{pmatrix} x_1 \\ . \\ . \\ . \\ x_r \end{pmatrix} = 0.$$

There is at least one x_i non zero, so $det(C - \alpha I_d) = 0$ and then $det(C - xI_d) \in \mathbb{Z}[x]$. □

Theorem 2.3. *Let K be a number field. Then $\mathcal{O}_K$ is a ring.*

Proof. If α, β are algebraic integers, then $\mathbb{Z}[\alpha]$ and $\mathbb{Z}[\beta]$ are a finitely generated as $\mathbb{Z}$-modules. From here, we have that $M = \mathbb{Z}[\alpha, \beta]$ also is a finitely generated $\mathbb{Z}$-module. Moreover, $(\alpha \pm \beta)M \subseteq M$ and $(\alpha\beta)M \subseteq M$, and then $\alpha \pm \beta$ and $\alpha\beta$ belong to the set of algebraic integers. □

2.4 Discriminant of Number Fields

Let K be a number field with $[K : \mathbb{Q}] = n$ and let $\sigma_1, \dots, \sigma_n$ be the complex embeddings of K. For $\alpha_1, \dots, \alpha_n \in K$ we define the **discriminant of** $\alpha_1, \dots, \alpha_n$ by

$$D_K(\alpha_1, \dots, \alpha_n) = \det(\sigma_i(\alpha_j))^2. \tag{2.1}$$

Theorem 2.4.

$$D_K(\alpha_1, \dots, \alpha_n) = \det(T_{K/\mathbb{Q}}(\alpha_i \alpha_j)).$$

Lemma 2.1. *Let $\{\gamma_1, \dots, \gamma_n\}$ be a subset of K. If $\gamma_i = \sum_{j=1}^{n} c_{ij}\alpha_j$, with $c_{ij} \in \mathbb{Q}$, then*

$$D_K(\gamma_1, \dots, \gamma_n) = \det(c_{ij})^2 D_K(\alpha_1, \dots, \alpha_n).$$

Proof. The proof follows from the fact that $\gamma_k\gamma_m = \sum_{i,j=1}^{n} c_{ki}c_{mj}\alpha_i\alpha_j$. □

Theorem 2.5. *$D_K(\alpha_1, \dots, \alpha_n) \neq 0$ if and only if the set $\{\alpha_1, \dots, \alpha_n\}$ is linearly independent over $\mathbb{Q}$.*

Proof. If $\{\alpha_1, \ldots, \alpha_n\}$ is linearly dependent over $\mathbb{Q}$ then the columns if the matrix $(\sigma_i(\alpha_j))_{ij}$ are linearly dependent, so $D_K(\alpha_1, \ldots, \alpha_n) = 0$. Reciprocally, if $D_K(\alpha_1, \ldots, \alpha_n) = 0$ then the columns of $(T_{K/\mathbb{Q}}(\alpha_i\alpha_j))_{ij}$ are lineraly dependent. Let us suppose that $\{\alpha_1, \ldots, \alpha_n\}$ is linearly independent and fix rational numbers (not all zero) such that $a_1R_1 + \ldots + a_nR_n = 0$, where R_ℓ are the columns of $(T_{K/\mathbb{Q}}(\alpha_i\alpha_j))_{ij}$ and let $\alpha = a_1\alpha_1 + \ldots + a_n\alpha_n \neq 0$. Looking at the j-th coordinate of each row, we see that $T_{K/\mathbb{Q}}(\alpha\alpha_j) = 0$ for all j. Note that $\{\alpha_1, \alpha_2, \ldots, \alpha_n\}$ is in fact, a basis for K over $\mathbb{Q}$ and then $\{\alpha\alpha_1, \alpha\alpha_2, \ldots, \alpha\alpha_n\}$ is a also a basis, then $T_K(\beta) = 0$ for all $\beta \in K$, which is a contradiction.

□

Theorem 2.6. *Let $K = \mathbb{Q}(\alpha)$, and $\alpha_1, \alpha_2, \ldots, \alpha_n$ the conjugated of α over $\mathbb{Q}$. Then*

$$D_K(1, \alpha, \alpha^2, \ldots, \alpha^{n-1}) = \prod_{1 \leq r < s \leq n} (\alpha_r - \alpha_s)^2 = \pm N_K(f'(\alpha)),$$

where f is the minimal polynomial of α over $\mathbb{Q}$ and the sign is $+$ if and only if $n \equiv 0$ or $1 \pmod 4$.

Proof. It is not difficult to prove that

$$D_K(1, \alpha, \alpha^2, \ldots, \alpha^{n-1}) = \det \begin{pmatrix} 1 & \alpha_1 & \alpha_1^2 & \cdots & \alpha_1^{n-1} \\ 1 & \alpha_2 & \alpha_2^2 & \cdots & \alpha_2^{n-1} \\ \vdots & \vdots & \cdots & \vdots & \vdots \\ 1 & \alpha_n & \alpha_n^2 & \cdots & \alpha_n^{n-1} \end{pmatrix}^2 = \prod_{1 \leq r < s \leq n} (\alpha_r - \alpha_s)^2.$$

By using that $N_K(f'(\alpha)) = \prod_{i=1}^n \sigma_i(f'(\alpha))$, we prove the second equality. □

2.5 Integral basis

Let K be a number field with $[K : \mathbb{Q}] = n$. By using discriminant, we can prove that the ring of integers $\mathcal{O}_K$ of is a free abelian group of rank n, that is, isomorphic to $\mathbb{Z}^n$. It is known that if A and C are free abelian groups of rank n, and $A \subseteq B \subseteq C$, then so is B. If $\alpha \in K$, then there exists an integer $m \in \mathbb{Z}$ such that $m\alpha$ is an algebraic integer. Then, we can find a basis of K over $\mathbb{Q}$, say $\{\alpha_1, \ldots, \alpha_n\}$, contained in $\mathcal{O}_K$. So, the free abelian group of rank n given by $A = \mathbb{Z}\alpha_1 + \ldots + \mathbb{Z}\alpha_n$ is contained in $\mathcal{O}_K$.

Theorem 2.7. *Let $\{\alpha_1, \ldots, \alpha_n\}$ be a basis for K over $\mathbb{Q}$ consisting entirely of algebraic integers, and set $D = D_K(\alpha_1, \ldots, \alpha_n)$. Then, every $\alpha \in \mathcal{O}_K$ can be expressed in the form*

$$\frac{1}{D}(m_1\alpha_1 + \ldots + m_n\alpha_n)$$

with $m_j \in \mathbb{Z}$ and m_j^2 are divisible by D.

It follows that $\mathcal{O}_K$ is containded in the free abelian group $B = \mathbb{Z}\frac{\alpha_1}{D} + \ldots + \frac{\alpha_n}{D}$, so we have the following corollary:

Corollary 2.2. *$\mathcal{O}_K$ is a free abelian group of rank n.*

It means that there exits $\beta_1, \ldots, \beta_n$ in $\mathcal{O}_K$ such that every $\alpha \in \mathcal{O}_K$ has unique representation

$$m_1\beta_1 + \ldots + m_n\beta_n,$$

where $m_i \in \mathbb{Z}$. The set $\{\beta_1, \ldots, \beta_n\}$ is called **integral basis** for $\mathcal{O}_K$.

Although the ring of integers has many integral basis, their discriminants are the same.

Theorem 2.8. *Let $\{\beta_1, \ldots, \beta_n\}$ and $\{\alpha_1, \ldots, \alpha_n\}$ be two integral bases for $\mathcal{O}_K$. Then*

$$D_K(\beta_1, \ldots, \beta_n) = D_K(\alpha_1, \ldots, \alpha_n).$$

Proof. It is enough to apply Lemma (2.1). □

Definition 2.3. *Let K be a number field of degree n over $\mathbb{Q}$. We define the discriminant of K by*

$$D_K := D_K(\alpha_1, \ldots, \alpha_n),$$

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

3 Some explicit computations

3.1 Ring of Integers of Quadratic Number Fields

Let us consider a quadratic number field $K = \mathbb{Q}(\sqrt{d})$ with d a square-free integer. Let $\alpha = a+b\sqrt{d} \in \mathcal{O}_K$, then its conjugate $\alpha' = a-b\sqrt{d}$ is also in $\mathcal{O}_K$. We have that $\alpha+\alpha' = 2a \in \mathcal{O}_K \cap \mathbb{Q}$, so $2a$ is in fact an integer and $a = \dfrac{a'}{2}$, with $a' \in \mathbb{Z}$. Note that α satisfies the following equation over $\mathbb{Q}$

$$0 = (x-\alpha)(x-\alpha') = x^2 - (\alpha+\alpha')x + \alpha\alpha',$$

where $\alpha\alpha' \in \mathbb{Z}$ (because $\alpha\alpha' \in \mathcal{O}_K \cap \mathbb{Q}$). Moreover,

$$\alpha\alpha' = a^2 - b^2 d = \left(\frac{a'}{2}\right)^2 - b^2 d \in \mathbb{Z}$$

and $(a')^2 - 4b^2 d \in 4\mathbb{Z}$. Because $a' \in \mathbb{Z}$, $4b^2 d \in \mathbb{Z}$ and so $4b^2 \in \mathbb{Z}$ due to d is square free. Now it follows that $2b \in \mathbb{Z}$ and so $b = \dfrac{b'}{2}$, with $b' \in \mathbb{Z}$. Now, we can see that α has the following representation:

$$\alpha = \frac{a'}{2} + \frac{b'\sqrt{d}}{2}.$$

Note that

$$\left(\frac{a'}{2}\right)^2 - \left(\frac{b'}{2}\right)^2 d = \alpha\alpha' \in \mathbb{Z}.$$

As $d \not\equiv 0 \pmod 4$, we have that $d \equiv 1, 2, 3 \pmod 4$. Additionally,

$$(a')^2 \equiv (b')^2 d \pmod 4,$$

therefore a' and b' have the same parity. This give us the following cases:

- If a' and b' are even, then $\alpha = \widetilde{a} + \widetilde{b}\sqrt{d}$, with $\widetilde{a}$ and $\widetilde{b} \in \mathbb{Z}$.
- If a' and b' are odd, then $(a')^2 \equiv (b')^2 \equiv 1 \pmod 4$, so $d \equiv 1 \pmod 4$.

Finally, we have proved the following proposition:

Proposition 3.1. *If $K = \mathbb{Q}(\sqrt{d})$ with d a square-free integer, then*

$$\mathcal{O}_K = \begin{cases} \mathbb{Z}[\sqrt{d}], & \text{if } d \equiv 2, 3 \ (mod\ 4) \\ \mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right], & \text{if } d \equiv 1 \ (mod\ 4) \end{cases}$$

From the proposition it is clear that an integral basis, depending on d, is the following:

$$\begin{cases} \{1, \sqrt{d}\}, & \text{if } d \equiv 2, 3 \pmod 4 \\ \{1, \frac{1+\sqrt{d}}{2}\}, & \text{if } d \equiv 1 \pmod 4 \end{cases}$$

3.2 Ring of Integers and Discriminant of Cyclotomic Number Fields

Proposition 3.2. *Let $n = p^l$ with p a prime number and ζ a primitive n-th root of unity in $\mathbb{C}$. Then $\{1, \zeta, \ldots, \zeta^{\phi(n)-1}\}$ is a $\mathbb{Q}$- basis of $K = \mathbb{Q}(\zeta)$ and*

$$D_K(1, \zeta, \ldots, \zeta^{\phi(n)-1}) = \pm r^s, \quad \text{where } s = p^{l-1}(lp - l - 1).$$

Proof. The main steps are the following:

- $\Phi_n(x) = \dfrac{x^{p^l} - 1}{x^{p^{l-1}}} = x^{p^{l-1}(l-1)} + \ldots + x^{2p^{l-1}} + 1.$
- From (2.6), $D_K(1, \zeta, \ldots, \zeta^{\phi(n)-1}) = \pm N_K(\phi'(\zeta))$.
- $\Phi_n(x) = \dfrac{p^l \zeta^{p^{l-1}}}{\zeta^{n/p}}$.
- $N_K(\phi'(\zeta)) = \dfrac{N_K(p^l \zeta^{p^{l-1}})}{N_K(\zeta^{n/p})} = \dfrac{p^{l\phi(n)} N_K(\zeta^{p^{l-1}})}{N_K(\zeta^{n/p})}$.

□

Proposition 3.3. *Let $n = p$, with p a prime number, and let ζ be a n-th primitive root of unity. If $K = \mathbb{Q}(\zeta)$, then $\{1, \zeta, \zeta^2, \ldots, \zeta^{p-2}\}$ is and integral basis for $\mathcal{O}_K$.*

Proof. The main steps are the following:

- $\Phi_p(x) = \dfrac{x^p - 1}{x - 1} = x^p + \ldots + x + 1.$
- From (2.6), $D_K(1, \zeta, \ldots, \zeta^{p-2}) = \pm \displaystyle\prod_{i=1}^{p-1} (\phi'(\zeta^i))$.
- $\Phi_(\zeta^i) = \dfrac{p\zeta^{-i}}{\zeta^i - 1}$.
- $D_K(1, \zeta, \ldots, \zeta^{p-2}) = \pm \displaystyle\prod_{i=1}^{p-1} \frac{p\zeta^{-i}}{\zeta^i - 1} = \pm \frac{p^{p-1}}{\Phi_p(1)} = \pm p^{p-2} \neq 0.$
- ζ^i are algebraic integers, so if $\{\alpha_1, \ldots, \alpha_{p-2}\}$ is an integral basis, then from (2.1),

  $$D_K(1, \zeta, \ldots, \zeta^{p-2}) = c^2 D_K(\alpha_1, \ldots, \alpha_{p-2}),$$

  where c is the determinant of the matrix $C = (c_{ij})$ where $\zeta^i = \displaystyle\sum_{j=1}^{p-2} c_{ij}\alpha_j$. it verifies that $c = 1$. Let us consider the following result:

Let $a_1, \ldots, a_n \in \mathcal{O}_K$ linearly independent over $\mathbb{Q}$. Let $N = \mathbb{Z}a_1 + \ldots + \mathbb{Z}a_n$ and $m = [\mathcal{O}_K : N]$. Prove that $D_K(a_1, \ldots, a_n) = m^2 D_K$.

If we fix $N = \mathbb{Z} \cdot 1 + \mathbb{Z}\zeta^2 \ldots + \mathbb{Z}\zeta^{p-1}$, then $[\mathcal{O}_K : N] = 1$, so $1, \zeta, \ldots, \zeta^{p-2}$ is an integral basis.

□

Theorem 3.1. *Let ζ be a n-th primitive root of unity. If $K = \mathbb{Q}(\zeta)$, then $\{1, \zeta, \zeta^2, \ldots, \zeta^{\phi(n)}\}$ is and integral basis for $\mathcal{O}_K$, i.e. $\mathcal{O}_K = \mathbb{Z}[\zeta]$. In particular, the discriminant of K is*

$$D_K = \frac{(-1)^{\phi(n)/2} n^{\phi(n)}}{\prod_{p|n} p^{\phi(n)/p-1}}.$$

4 Dedekind Domains

Definition 4.1. *An integral domain R is a Dedekind domain if,*

(i) Every ideal in R is finitely generated.

(ii) R in integrally closed in its field of fraction $Q(R) = \{\alpha/\beta : \alpha, \beta \in R, \beta \neq 0\}$. It means that if α/β is a root of some monic polynomial over R, then $\alpha/\beta \in R$.

(iii) Every non zero prime ideal in R is a maximal ideal.

Theorem 4.1. *Let K be a number field. $\mathcal{O}_K$ is a Dedekind domain.*

Proof. $\mathcal{O}_K$ is a free abelian group of rank n , so if $\mathfrak{a}$ is an ideal of $\mathcal{O}_K$, $\mathfrak{a}$ is too, which proves (i). It is possible to prove that if $\mathfrak{a} \subset \mathcal{O}_K$ is a prime ideal, then $\mathcal{O}_K/\mathfrak{a}$ is a finite integral domain, so it is a field and then $\mathfrak{a}$ is maximal.

□

Theorem 4.2. *Let R be a Dedekind domain. Then every ideal $\mathfrak{a} \neq 0, R$ has a unique (unless reordering) factorization in prime ideals:*

$$\mathfrak{a} = \mathfrak{p}_1 \mathfrak{p}_2 \cdots \mathfrak{p}_r.$$

5 Factorization in Ring of Integers

Note that there are primes of $\mathbb{Z}$, which are not irreducible. For example,

$$5 = (2+1)(2-i), \text{ in } \mathbb{Z}[i].$$

Problem: Let K be a number field and p a prime in $\mathbb{Z}$. Study the prime decomposition of

$$(p) = p\mathcal{O}_K.$$

Definition 5.1. *We say that an ideal $\mathfrak{b}$ lies over p (or divides p) if $\mathfrak{b}$ appears in the prime factorization of (p).*

Note that if $\mathfrak{b}$ lies over p, then $p = \mathfrak{b} \cap \mathbb{Z}$, and every prime ideal of $\mathcal{O}_K$ lies over a unique prime of $\mathbb{Z}$.

Definition 5.2. *Suppose that*

$$p\mathcal{O}_K = \mathfrak{b}_1^{e_1}\mathfrak{b}_2^{e_2}\dots\mathfrak{b}_r^{e_r},$$

where $\mathfrak{b}_i's$ are primes of $\mathcal{O}_K$. The integers e_i are called the ramification index of over p and

$$f_i = [\mathcal{O}_K/\mathfrak{b}_i : \mathbb{Z}/p\mathbb{Z}]$$

is called the inertial degree of $\mathfrak{b}_i$ over p.

Theorem 5.1. *If K is a number field with $[K:\mathbb{Q}] = n$, then*

$$\sum_{i=1}^{r} e_i f_i = n.$$

If K is a number field, we know that $\mathcal{O}_K$ is a Dedekind domain. Then, each ideal in $\mathcal{O}_K$ may be written as a product of prime ideals.
Problem: Find $\mathfrak{p}_i$ and e_i:

$$\begin{array}{ccc} K & \mathcal{O}_K & p\mathcal{O}_K = \mathfrak{p}_1^{e_1}\mathfrak{p}_2^{e_2}\dots\mathfrak{p}_r^{e_r} \\ | & | & | \\ \mathbb{Q} & \mathbb{Z} & p \end{array}$$

5.1 Factorization in Quadratic Fields

Let $K = \mathbb{Q}(\sqrt{d})$, with d squarefree and $\mathcal{O}_K = \mathbb{Z}[\alpha]$ with

$$\alpha = \begin{cases} \sqrt{d}, & \text{if } d \equiv 2,3 \pmod 4 \\ \frac{1+\sqrt{d}}{2}, & \text{if } d \equiv 1 \pmod 4 \end{cases}$$

If f is the minimal polynomial of α over $\mathbb{Q}$, then

$$f(x) = \begin{cases} x^2 - d, & \text{if } d \equiv 2,3 \pmod 4 \\ x^2 - x + \frac{1-d}{4}, & \text{if } d \equiv 1 \pmod 4 \end{cases}$$

Remark 1. *The following isomorphism holds canonically:*

$$\mathcal{O}_K/p\mathcal{O}_K \cong (\mathbb{Z}[x]/(f(x)))/(p\mathcal{O}_K) \cong \mathbb{Z}[x]/(p, f(x)) \cong \mathbb{Z}_p[x]/(\overline{f}(x))$$

Let us see the possible factors of $\overline{f}(x)$ in $\mathbb{Z}_p[x]$:

- $\overline{f}(x)$ is irreducible.
  This implies $\mathbb{Z}_p[x]/(\overline{f}(x))$ is a field, then $\mathcal{O}_K/p\mathcal{O}_K$ is also a field and so $p\mathcal{O}_K$ is a prime ideal.

  For the remaining cases, observe that:

$$\begin{array}{ccccc} \mathcal{O}_K & \longrightarrow & \mathcal{O}_K/p\mathcal{O}_K & & \\ \downarrow & & \downarrow & & \\ \mathbb{Z}/(f(x)) & \longrightarrow & \mathbb{Z}[x]/(p, f(x)) & \longrightarrow & \mathbb{Z}_p[x]/(\overline{f}(x)) \end{array}$$

- $\overline{f}(x) = \overline{g}(x)\overline{h}(x)$, with $\overline{g}(x)$ and $\overline{h}(x)$ distinct, monic and linear.
From the Chinese remainder theorem

$$\mathbb{Z}_p[x]/(\overline{f}(x)) \cong \mathbb{Z}_p[x]/(\overline{g}(x)) \times \mathbb{Z}_p[x]/(\overline{h}(x)).$$

Restricting to each factor we see that the kernel of the map

$$\mathcal{O}_K \to \mathbb{Z}_p[x]/(\overline{g}(x)) \times \mathbb{Z}_p[x]/(\overline{h}(x)),$$

is in the first factor the ideal $(p, g(\alpha))$ and in the second factor $(p, h(\alpha))$. Then, the kernel is $(p, g(\alpha)) \cap (p, h(\alpha))$.

Remark 2. *The ideals $(p, g(\alpha))$ and $(p, h(\alpha))$ are prime and relatively primes (i.e their sum is the whole ring) and it holds that*

$$(p, g(\alpha) \cap (p, h(\alpha)) = (p, g(\alpha)) \cdot (p, h(\alpha)).$$

(Exercise)

But from the diagram, the kernel of the map is in fact $p\mathcal{O}_K$, so the factorization of this ideal is

$$p\mathcal{O}_K = (p, g(\alpha)) \cdot (p, h(\alpha)).$$

- $\overline{f}(x) = \overline{g}(x)^2$, with $\overline{g}(x)$ monic and irreducible.
First, we assume that $p \neq 2$.

Remark 3. *If $d \equiv 2, 3$ (mod 4), then $\overline{f}(x) = x^2 - d$ is a square in $\mathbb{Z}_p[x]$ if and only if $p|d$.*

In fact,

$$x^2 - d \equiv (x + a)^2 \pmod{p} \Leftrightarrow (d(2x + a + d) \equiv 0 \pmod{} \Leftrightarrow p|d.$$

We take $\overline{g}(x) = x$. Then the kernel of the map

$$\mathcal{O}_K \to \mathbb{Z}_p[x]/(x^2)$$

is for one hand $(p, g(\alpha)) = (p, \alpha^2)$ and for the other hand is $p\mathcal{O}_K$. Then,

$$p\mathcal{O}_K = (p, \alpha^2) = (p, \alpha)^2.$$

It remains to see what happens when $p = 2$, but it will be left as an exercise.

We resume the previous results in the next proposition,

Proposition 5.1. *Let $K = \mathbb{Q}(\sqrt{d})$, with d squarefree and let $f(x)$ be the minimal polynomial of $\sqrt{d}$ over $\mathbb{Q}$. If p is a prime number, then the factorization in irreducible factors in $\mathbb{Z}_p[x]$*

$$\overline{f}(x) = \overline{g}_1(x)^{e_1}\overline{g}_2(x)^{e_2}, \text{ with } e_i = 1 \text{ or } 2$$

implies

$$p\mathcal{O}_K = (p, g_1(\alpha))^{e_1}(p, g_2(\alpha))^{e_2}.$$

A more general result is the following:

Theorem 5.2. *Let $K = \mathbb{Q}(\theta)$ with θ an algebraic integer. Let us suppose that $p \nmid [\mathcal{O}_K : \mathbb{Z}[\theta]]$ and let $g(x)$ be the minimal polynomial of θ. If*

$$f(x) \equiv g_1(x)^{e_1} g_2(x)^{e_2} \dots g_r(x)^{e_r} \ (mod\ p),$$

where g_i are irreducible and distinct, then

$$p\mathcal{O}_K = \mathfrak{p}_1^{e_1} \mathfrak{p}_2^{e_2} \dots \mathfrak{p}_r^{e_r},$$

where $\mathfrak{p}_i = (p, g_i(\theta))$ are prime ideals, $N(\mathfrak{p}_i) = p^{f_i}$ and $f_i = deg(g_i)$.

Remark 4. *If $\mathcal{O}_K = \mathbb{Z}[\theta]$, then the theorem holds for every prime (same if $g(x)$ in Einsenstein in p.)*

Definition 5.3. *Let p be a prime number and K a number field with $[K : \mathbb{Q}] = n$. We say that,*

- *p is totally ramified if $p\mathcal{O}_K = \mathfrak{p}^n$, for some prime $\mathfrak{p}$.*
- *p is inert if $p\mathcal{O}_K$ is prime.*
- *p splits completely if $p\mathcal{O}_K = \mathfrak{p}_1\mathfrak{p}_2 \dots \mathfrak{p}_n$.*

In general, we say that p ramifies in K if in the prime factorization in $\mathcal{O}_K$, some $e_i \geq 2$.

Corollary 5.1. *Let θ be an algebraic integer such that its minimal polynomial is Einsenstein in the prime p. If $K = \mathbb{Q}(\theta)$, then p is totally ramified in $\mathcal{O}_K$.*

Theorem 5.3. *(Dedekind) A prime p ramifies in K if and only if $p|D_K$.*

Is it possible to prove the following special cases:

- If $p \nmid [\mathcal{O}_K : \mathbb{Z}[\theta]]$, then p ramifies in $\mathcal{O}_K$ if and only of $p \nmid D_K$.
- If $K = \mathbb{Q}(\theta)$ and $\mathcal{O}_K = \mathbb{Z}[\theta]$, then if $p|D_K$, then p ramifies in K. (Exercise)

5.2 Action of the Galois Group over primes

Theorem 5.4. *Let K be a Galois extension over $\mathbb{Q}$ and p a prime number. Let $\mathfrak{p}_1, \dots, \mathfrak{p}_r$ be the primes in K over p. Then Gal($K/\mathbb{Q}$) acts transitively in this set, i.e., for all i, j, there exists $\sigma \in$ Gal($K/\mathbb{Q}$) such that $\sigma(\mathfrak{p}_i) = \mathfrak{p}_j$.*

Proof. Note that $\sigma(\mathcal{O}_K) = \mathcal{O}_K$ and if $\mathfrak{p}$ is a prime over p, then $\sigma(\mathfrak{p})$ is also a prime ideal over p. Let $\mathfrak{p}_i$ and $\mathfrak{p}_j$ different primes over p. Suppose that $\sigma(\mathfrak{p}_i) \neq \mathfrak{p}_j$, for all $\sigma \in \mathrm{Gal}(K/\mathbb{Q})$. Both ideals are maximal, so $\mathfrak{p}_j \subsetneq \mathfrak{p}_j$. Let $x \in \mathfrak{p}_j$ but $x \notin \sigma(\mathfrak{p}_i)$. Taking the norm

$$N_K(x) = \prod_{\sigma} \sigma(x) = x \cdot \prod_{\sigma \neq\ id} \sigma(x) \in \mathfrak{p}_j.$$

For the other hand, $N_K(x) \in \mathbb{Z}$, then $N_K(x) \in p\mathbb{Z} = \mathbb{Z} \cap \mathfrak{p}_j = \mathbb{Z} \cap \mathfrak{p}_i \subset \mathfrak{p}_i$. But $N_K(x) \notin \sigma^{-1}$, so we have a contradiction. □

Corollary 5.2. *Let K be a Galois extension over $\mathbb{Q}$ of degree n and let $\mathfrak{p}$ be a prime over p. Then, if $p\mathcal{O}_K = \mathfrak{b}_1^{e_1} \mathfrak{b}_2^{e_2} \dots \mathfrak{b}_r^{e_r}$, then $e_1 = e_2 \dots = e_r$, $f_1 = f_2 \dots = f_r$ and $erf = n$.*

6 Factorization in Cyclotomic Fields

Let $m \geq 1$ and $K = \mathbb{Q}(\zeta_m)$. Then $\mathcal{O}_K = \mathbb{Z}[\zeta_m]$ and p a prime in $\mathbb{Z}$. Then

$$\Phi_m(x) \equiv (g_1(x)g_2(x)\dots g_r(x))^e \pmod{\mathfrak{p}},$$

deg $(g_i(x))$=f for all i and $erf = \phi(m)$. Suppose that $p \nmid m$. So, $x^m - 1 = \prod_{d|m} \phi_d(x)$ has no factors with multiplicity greater than one, in particular $\phi_m(x)$. Then $e = 1$.

- Suppose $f = 1$, then $\phi_m(x)$ has only linear factors in $\mathbb{Z}_p[x]$.

  Lemma 6.1. *Let m be a positive integer and L be a field with $char(L) \nmid m$. If $\alpha \in L$, then $\phi_m(\alpha) = 0$ if and only if α is a primitive m-th root of unity.*

  Following the previous lemma, $\mathbb{Z}_p$ has a primitive m-th root of unity. $\mathbb{Z}_p^*$ is a cyclic group of order $p-1$, then its elements of order m are exactly those $m|p-1$. So, $\mathbb{Z}_p^*$ has elements of order m if and only if $p \equiv 1 \pmod{m}$.

  Proposition 6.1. *p splits completely in $\mathcal{O}_K$ if and only $p \nmid m$ and $p \equiv 1$ (mod m).*

- $f > 1$. Let $g(x)$ be an irreducible factor of $\Phi_m(x)$ in $\mathbb{Z}_p[x]$, with deg$(g(x))$=f. Let α be a root of $g(x)$ and $F = \mathbb{Z}_p[\alpha] \cong \mathbb{Z}_p[x]/(g(x))$. Then $[F : \mathbb{Z}_p] = f$ and F has a primitive m-th root of unity, so $|F| = p^f$ and F^* is cyclic with order $p^f - 1$.

  Proposition 6.2. *f is the order of p in $\mathbb{Z}_p^*$ and there are $\phi(m)/f$ primes over p.*

If $p|m$, then p ramifies.

Example 4. *p in $\mathbb{Q}(\zeta_p)$. From $x^p - 1 \equiv (x-1)^p$ (mod p) and $\Phi_p(x) = \frac{x^p-1}{x-1}$, we have $\Phi_p(x) \equiv (x-1)^{p-1}$ (mod p), then*

$$p\mathcal{O}_K = (p, \zeta_p - 1)^{p-1},$$

that is, p is totally ramified.

6.1 Ideal Class Group

Definition 6.1. *A fractional ideal $\mathfrak{a}$, is an $\mathcal{O}_K$-module contained in K such that there is $m \in \mathbb{Z}$ such that $m\mathfrak{a} \subset \mathcal{O}_K$.*

If $\mathfrak{p}$ is a prime ideal, we define

$$\mathfrak{p}^{-1} = \{x \in K : x\mathfrak{p} \subseteq \mathcal{O}_K\}.$$

Theorem 6.1. *If $\mathfrak{p}$ is a prime ideal, then $\mathfrak{p}^{-1}$ is a fractional ideal and $\mathfrak{p}^{-1}\mathfrak{p} = \mathcal{O}_K$.*

We have that J_K, the set of fractional ideals of K is an abelian group. In fact, the neutral element is the ring of integers. If $\mathfrak{a}$ is a prime ideal, from the previous theorem there exists the inverse element. In the general case, if $\mathfrak{a}$ is an integral ideal, we know that there are unique prime ideals $\mathfrak{p}_i$ such that $\mathfrak{a} = \mathfrak{p}_1 \cdots \mathfrak{p}_r$. If $\mathfrak{b} = \mathfrak{p}_1^{-1} \cdots \mathfrak{p}_r^{-1}$, then $\mathfrak{ab} = (1) = \mathcal{O}_K$. From here, we prove the following:

Theorem 6.2. *Let $\mathfrak{a}$ be a fractional ideal in K. Then $\mathfrak{a}$ may be written uniquely (up order) by*

$$\mathfrak{a} = \prod_{i=1}^{r} \mathfrak{p}_i^{v_i},$$

where $v_i \in \mathbb{Z}$.

In fact, we can write every fractional ideal as $\mathfrak{a} = \frac{\mathfrak{b}}{\mathfrak{c}}$, with $\mathfrak{a}$ and $\mathfrak{b}$ integral ideals. Let P_K be the subgroup of J_K of principal fractional ideals, i.e., ideals of the form $(a) = a\mathcal{O}_K$, for some $a \in K^*$.

Definition 6.2. *The ideal class group of a number field K, as the quotient group*

$$Cl_K = J_K/P_K.$$

Another way to see the ideal class group is considering the following equivalence relation: two fractional ideal $\mathfrak{a}$ and $\mathfrak{b}$ are equivalent if there is $a \in K^*$ such that $\mathfrak{a} = (a)\mathfrak{b}$.

Theorem 6.3. *Cl_K is a finite abelian group. The order is denoted by h_K and is called the class number of K.*

The main steps to prove the theorem are the following:

- Every ideal class contains an integral ideal $\mathfrak{a}$ such that

$$N(\mathfrak{a}) \leq \frac{n!}{n^n}\left(\frac{4}{\pi}\right)^{r_2}\sqrt{|D_K|} \quad \text{(Minkowski bound)},$$

  where $n = r_1 + 2r_2$

- There are finitely many ideals $\mathfrak{a}$ with $N(\mathfrak{a})$ bounded.

For more details, see [2].

In general, $\mathcal{O}_K$ is not a UFD. However, Cl_K is trivial if and only if $\mathcal{O}_K$ is a PID, which is equivalent to be an UFD.

Example 5. *Find h_k if $K = \mathbb{Q}(\sqrt{-14})$.*
Minkowski bound: $\frac{2!}{2^2}\left(\frac{4}{\pi}\right)^0\sqrt{4\cdot 14} = \sqrt{14} < 4$. Then, every class ideal has an integral representative $\mathfrak{a}$ with $N(\mathfrak{a}) < 4$. Note that if $\mathfrak{a} = \mathfrak{p}_1\mathfrak{p}_2\ldots\mathfrak{p}_r$, then $N(\mathfrak{p}) = p^f$, so $p = 2$ or 3. Let us see the factorization of $2\mathcal{O}_K$ and $3\mathcal{O}_K$.

- $x^2 - 14 \equiv x^2$ *(mod 2), then* $2\mathcal{O}_K = (2, \sqrt{14})^2$.
- $x^2 - 14 \equiv x^2 + 1$ *(mod 3) which is irreducible, then* $2\mathcal{O}_K$ *is prime.*

Therefore, $\mathfrak{p} = (2, \sqrt{14})$ or $(3).(2, \sqrt{14})$ is a principal ideal if and only if there is an element $a + b\sqrt{14}$ with $N(a + b\sqrt{14}) = \pm 2$ and $(2, \sqrt{14}) = (a + b\sqrt{14})$. It is no difficult to prove that $(2, \sqrt{14}) = (4 + \sqrt{14})$ so $h_K = 1$.

7 Dirichlet's Unit Theorem

An element $\alpha \in \mathcal{O}_K$ is a unit, if there is an element $\beta \in \mathcal{O}_K$ such that $\alpha\beta = 1$. The following theorem, describe the structure of the group of units of $\mathcal{O}_K$, denoted by U_K.

Theorem 7.1. *Let K be a number field of degree n over $\mathbb{Q}$ with r_1 and r_2 the number of real and nonreal embedding over $\mathbb{C}$. Then there exist fundamental units $\varepsilon_1, \dots \varepsilon_r$, with $r = r_1 + r_2 - 1$, such that every $\varepsilon \in \mathcal{O}_K^*$ can be written in a unique way by*

$$\varepsilon = \zeta \varepsilon_1^{n_1} \cdot \varepsilon_r^{n_r},\ n_i \in \mathbb{Z},$$

where ζ is a root of unity in $\mathcal{O}_K$. More precisely, if W_K is the group of root of unity in $\mathcal{O}_K^*$, then W_K is finite, cyclic and $\mathcal{O}_K^* \cong W_K \times \mathbb{Z}^r$.

Imaginary Quadratic Fields

- $d \equiv 2, 3 \pmod 4$.
  In this case, $\mathcal{O}_K = \mathbb{Z}[\sqrt{d}]$ and $a + b\sqrt{d} \in \mathcal{O}_K^*$ if and only if $a^2 - b^2 d = 1$.
  If $b = 0$, then $a = \pm 1$ and $\mathcal{O}_K^* \cong \{\pm 1\} \cong \mathbb{Z}_2$.
  If $b \neq 0$, then $a^2 - b^2 d \geq -d$ and $-d \leq -1$. If $d = -1$, $a^2 - b^2 d = a^2 + b^2 = 1$, then $a = \pm 1, b = 0$ or $a = 0, b = \pm 1$. Therefore, $\mathcal{O}_K^* \cong \{\pm 1, \pm i\} \cong \mathbb{Z}_4$.
- $d \equiv 1 \pmod 4$.
  In this case, $\mathcal{O}_K = \mathbb{Z}[\frac{1+\sqrt{d}}{2}]$ and $\frac{a+b\sqrt{d}}{2} \in \mathcal{O}_K^*$ if and only if $a^2 - b^2 d = 4$.
  If $-d \geq 4$, then $b = 0$ and $a = \pm 2$, so $\mathcal{O}_K^* \cong \mathbb{Z}_2$.
  If $d = -3$, $a^2 - b^2 d = a^2 + 3b^2 = 4$, then $a = \pm 2$ and $b = 0$ or $a = \pm 1$ and $b = \pm 1$, so $\mathcal{O}_K^* \cong \{\pm \zeta_3, \pm \zeta_3^2, \pm 1\} \cong \mathbb{Z}_6$.

Remark 5. *$\mathcal{O}_K^*$ is finite if and only if $K = \mathbb{Q}$ or K is an imaginary quadratic field.*

Real Quadratic Fields $K \subset \mathbb{R}$ and $r_1 = 2$, so $W_K = \{\pm 1\}$ and $\mathcal{O}_K^* \cong \{\pm 1\} \times \mathbb{Z}$.
Characterization of the fundamental unit:

- $d \equiv 2, 3 \pmod 4$.
  If $b = min\{\widetilde{b} : d\widetilde{b}^2 \pm 1 = a^2 : \text{ for some } a > 0\}$, then $a + b\sqrt{d}$ is a fundamental unit. (Exercise)
- $d \equiv 1 \pmod 4$.
  If $b = min\{\widetilde{b} : d\widetilde{b}^2 \pm 4 = a^2 : \text{ for some } a > 0\}$, then $a + b\sqrt{d}$ is a fundamental unit. (Exercise)

Example 6. *$\mathbb{Q}(\sqrt{3})$: $min\{\widetilde{b} : d\widetilde{b}^2 \pm 1 = a^2 :$ for some $a > 0\} = 1$ and $a = 2$, then $2 + \sqrt{2}$ is a fundamental unit.*

Definition 7.1. *The regulator of a number field K is given by*

$$R_K := |det(\log |\varepsilon_j^{(i)}|_{ij}),$$

where $\varepsilon_j^{(i)}$ is the real or complex embedding of the fundamental unit ε.

The regulator R_K gives us a measure of the size of U_K.
A different way to find fundamental units is by continued fractions.

Theorem 7.2. *Let n be the period of the continued fraction of $\sqrt{d}$ with d square free and let $C_k = p_k/q_k$ be the k-th convergent. If $d \equiv 2, 3 \pmod 4$, then $p_{n-1} + q_{n-1}\sqrt{d}$ is the fundamental unit of $\mathbb{Q}(\sqrt{d})$.*

Example 7. *In $\mathbb{Q}(\sqrt{6})$, we have that $\sqrt{6} = [2; \overline{2, 4}]$ (exercise). Then, $C_1 = \frac{p_1}{q_1} = a_0 + \frac{1}{a_1} = 2 + \frac{1}{2} = \frac{5}{2}$ and $5 + 2\sqrt{6}$ is a fundamental unit.*

8 Analytic Class Number Formula

If K is a number field, we define the Dedekind zeta function associated with K by

$$\zeta_K(s) = \sum_{\mathfrak{a} \neq 0 \text{ ideal}} \frac{1}{N(\mathfrak{a})^s}, \ s \in \mathbb{C}.$$

This function encodes a lot of information about the number field K. Properties:

- $\zeta_K(s) = \prod_{\mathfrak{p} \text{ prime}} (1 - N(\mathfrak{p})^{-s})^{-1}$, is an holomorphic function if Re(s)>1.
- In $s = 1$, $\zeta_K(s)$ is a divergent series.
- It has a meromorphic continuation to the left side of Re(s)>1.

Theorem 8.1. *Let K be a number field of degree n over $\mathbb{Q}$ with r_1 and r_2 the number of real and complex embedding over $\mathbb{C}$. Then $\zeta_K(s)$ extends to a meromorphic function defined for all $s \in \mathbb{C}$ with a simple pole in $s = 1$ and*

$$\lim_{s \to \infty} \zeta_K(s) = \frac{2^{r_1}(2\pi)^{r_2} h_K R_K}{|W_K| \sqrt{|D_K|}},$$

where W_K is the group of unity in $\mathcal{O}_K$ and R_K is the regulator of K.

8.1 Class Number of Quadratic Number Fields

If K is a quadratic number field, let us consider the Dirichlet function associated with the quadratic character given by the extended Jacobi symbol $\chi_K(m) = \left(\frac{D_K}{m}\right)$,

$$L(\chi_K, s) = \sum_{n=1}^{\infty} \frac{\chi_K(m)}{n^s}.$$

This function is related to the class number by the following identity:

$$\lim_{s \to \infty} \zeta_K(s) = L(\chi_K, 1).$$

9 Exercises

1. Let d_1 and d_2 square-free integers different from 0 and 1. Prove that $\mathbb{Q}(\sqrt{d_1})$ and $\mathbb{Q}(\sqrt{d_2})$ are equal if and only if $d_1 = d_2$.

2. Let θ be an algebraic integer such that its minimal polynomial is Einsenstein in the prime p. Prove that if $K = \mathbb{Q}(\theta)$, then p is totally ramified in $\mathcal{O}_K$.

3. Prove that if $p \nmid [\mathcal{O}_K : \mathbb{Z}[\theta]]$, then p ramifies in $\mathcal{O}_K$ if and only of $p \mid D_K$.

4. If $K = \mathbb{Q}(\theta)$ and $\mathcal{O}_K = \mathbb{Z}[\theta]$, prove that if $p|D_K$, then p ramifies in K.

5. (i) Let K be a number field with $[K : \mathbb{Q}] = n$ and $\beta \in \mathcal{O}_K$. Prove that $\beta \in \mathcal{O}_K^*$ if and only if $N_K(\beta) = 1$.

   (ii) Prove that $\mathbb{Z}[\sqrt{2}]^* = \{\pm(1+\sqrt{2})^k : k \in \mathbb{Z}\}$ and $\mathbb{Z}[\sqrt{2}]^* = \{\pm 1\}$

6. If K is a number field, prove that its discriminant D_K is an integer.

7. Let $a_1, \ldots, a_n \in \mathcal{O}_K$ linearly independent over $\mathbb{Q}$. Let $N = \mathbb{Z}a_1 + \ldots + \mathbb{Z}a_n$ and $m = [\mathcal{O}_K : N]$. Prove that $D_K(a_1, \ldots, a_n) = m^2 D_K$. *(Hint: Use the following result: Let $M = \mathbb{Z}\alpha_1 + \ldots + \mathbb{Z}\alpha_n$ and N be a sub-module. Then there exists $\beta_1, \ldots, \beta_m \in N$ with $m \geq n$ such that $N = \mathbb{Z}\beta_1 + \ldots + \beta_m\mathbb{Z}$ and $\beta_i = \sum_{j \geq i} p_{ij}\alpha_j$ with $1 \leq i \leq m$ and $p_{ij} \in \mathbb{Z}$)*

8. Let $f(x) = x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0 \in \mathbb{Z}[x]$ the minimal polynomial of θ. Let $K = \mathbb{Q}(\theta)$. If for each prime p such that $p^2|D_K(\theta)$ we have $f(x)$ Eisensteinian (that is, $f(x)$ satisfies the irreducibly Eisenstein's criterion for p) with respect to p. Show that $\mathcal{O}_K = \mathbb{Z}[\theta]$. *(Hint: Use the previous problem)*

9. If the minimal polynomial of α over $\mathbb{Q}$ is $f(x) = x^n + ax + b$ and $K = \mathbb{Q}(\alpha)$, show that

$$D_K(\alpha) = (-1)^{\binom{n}{2}}(n^n b^{n-1} + a^n(1-n)^{n-1}).$$

10. (a) Determine the ring of integers of $\mathbb{Q}(\sqrt[3]{2})$.

    (b) Determine the factorization of $7, 29$ and 31 in $\mathbb{Q}(\sqrt[3]{2})$.

11. Compute the discriminant of a quadratic number field.

12. Let $\mathcal{O}_K = \mathbb{Z}[\alpha]$, where $K = \mathbb{Q}(\sqrt{d})$, d is a square-free integer. If f is the minimal polynomial of α over $\mathbb{Q}$, show that

$$f(x) = \begin{cases} x^2 - d, & \text{if } d \equiv 2, 3 \pmod 4 \\ x^2 - x + \frac{1-d}{4}, & \text{if } d \equiv 1 \pmod 4 \end{cases}$$

References

[1] Harold M. Edwards. "The Genesis of Ideal Theory". *Archive for History of Exact Sciences* 23, pp. 321–378, 1980.

[2] Daniel A. Marcus. *Number Fields*. Springer-Verlag New York, 2018.