

NUMBER THEORY

Lectures by Amaury Thuillier
Notes by Alexis Marchand

ENS de Lyon
S2 2018-2019
M1 course

Contents

1	Number fields and rings of integers	1
1.1	Algebraic and integral numbers	1
1.2	Number fields	2
1.3	Traces, norms and discriminants	3
1.4	Rings of integers	4
1.5	Cyclotomic number fields	6
2	Ideal factorisation of algebraic numbers	8
2.1	Dedekind rings	8
2.2	Factorisation of ideals in Dedekind rings	9
2.3	Class group	11
2.4	Factorisation and ramification	11
2.5	Factorisation in Galois extensions	14
2.6	Quadratic Reciprocity Law	16
3	Class group and unit group	18
3.1	Lattices	18
3.2	Finiteness of the class group	20
3.3	Binary quadratic forms and class groups	22
3.4	Reduced forms	24
3.5	Unit group	24
3.6	Application to the Pell-Fermat Equation	25
4	Introduction to analytic methods	26
4.1	Dirichlet series	26
4.2	Dedekind ζ -function of a number field	27
4.3	Class Number Formula	28
4.4	Dirichlet characters and Dirichlet L -functions	30
	References	31

1 Number fields and rings of integers

1.1 Algebraic and integral numbers

Definition 1.1.1 (Algebraic and integral numbers). *Let K/\mathbb{Q} be a field extension and $\alpha \in K$.*

- (i) We say that α is algebraic (over \mathbb{Q}) if there exists $f \in \mathbb{Q}[T] \setminus \{0\}$ s.t. $f(\alpha) = 0$. In this case, there exists a unique monic polynomial $f_{\alpha, \min} \in \mathbb{Q}[T]$, called the minimal polynomial of α , s.t. $\text{Ker ev}_\alpha = (f_{\alpha, \min})$, where $\text{ev}_\alpha : P \in \mathbb{Q}[T] \mapsto P(\alpha) \in K$.
- (ii) We say that α is integral (over \mathbb{Z}), or that α is an algebraic integer, if there exists a monic polynomial $f \in \mathbb{Z}[T]$ s.t. $f(\alpha) = 0$.

Proposition 1.1.2. Let K/\mathbb{Q} be a field extension and let $\alpha \in K$ be an algebraic number. Then α is integral iff $f_{\alpha, \min} \in \mathbb{Z}[T]$.

Proposition 1.1.3. Let K/\mathbb{Q} be a field extension and $\alpha \in K$.

- (i) The following assertions are equivalent:
 - (a) α is algebraic.
 - (b) $\mathbb{Q}[\alpha]$ is a finite-dimensional \mathbb{Q} -vector space.
 - (c) There exists a nonzero finite-dimensional \mathbb{Q} -vector space $V \subseteq K$ s.t. $\alpha V \subseteq V$.
- (ii) The following assertions are equivalent:
 - (a) α is integral.
 - (b) $\mathbb{Z}[\alpha]$ is a finitely generated \mathbb{Z} -module.
 - (c) There exists a nonzero finitely generated \mathbb{Z} -module $M \subseteq K$ s.t. $\alpha M \subseteq M$.

Proof. In both cases, (c) \Rightarrow (a) is a consequence of the Cayley-Hamilton Theorem (and the other implications are easy). \square

Corollary 1.1.4. Let K/\mathbb{Q} be a field extension. If $\alpha, \beta \in K$ are algebraic (resp. integral), then $(\alpha + \beta)$ and $(\alpha\beta)$ are algebraic (resp. integral).

Remark 1.1.5. If K/\mathbb{Q} is a field extension and $\alpha \in K$ is algebraic, then there exists $\beta \in K$ integral and $m \in \mathbb{N}^*$ s.t. $\alpha = \frac{\beta}{m}$.

Proposition 1.1.6. Let K/\mathbb{Q} be a field extension.

- (i) $K_0 = \{\alpha \in K, \alpha \text{ is algebraic}\}$ is a subfield of K containing \mathbb{Q} .
- (ii) $A_0 = \{\alpha \in K, \alpha \text{ is integral}\}$ is a subring of K containing \mathbb{Z} .

Moreover, $K_0 = \text{Frac}(A_0)$.

Notation 1.1.7. If $K = \mathbb{C}$, we write $\overline{\mathbb{Q}}$ (resp. $\overline{\mathbb{Z}}$) for the set of algebraic (resp. integral) numbers.

1.2 Number fields

Definition 1.2.1 (Number field). A number field K is a finite extension of \mathbb{Q} . Its degree, denoted by $[K : \mathbb{Q}]$, is its dimension as a \mathbb{Q} -vector space.

Remark 1.2.2. If K is a number field and $\alpha \in K$, then the degree of α (i.e. the degree of $f_{\alpha, \min}$) divides the degree of K .

Theorem 1.2.3 (Primitive Element Theorem). If K is a number field, then there exists $\vartheta \in K$ s.t. $K = \mathbb{Q}(\vartheta)$.

Corollary 1.2.4. Let $K = \mathbb{Q}(\vartheta)$ be a number field. Then the set $\text{Hom}_{\text{fields}}(K, \mathbb{C})$ of embeddings of K in \mathbb{C} is in bijection with the set of complex roots of $f_{\vartheta, \min}$. In particular:

$$|\text{Hom}_{\text{fields}}(K, \mathbb{C})| = [K : \mathbb{Q}].$$

Definition 1.2.5. Let K be a number field and let $\sigma \in \text{Hom}_{\text{fields}}(K, \mathbb{C})$.

- If $\sigma(K) \subseteq \mathbb{R}$, we say that σ is a real embedding.
- Otherwise, we say that σ is a complex (nonreal) embedding.

We write Σ_r (resp. Σ_c) for the set of real (resp. complex) embeddings $K \hookrightarrow \mathbb{C}$. We note that Σ_c is stable under complex conjugation, and we fix Σ'_c a set of representatives of the quotient of Σ_c by complex conjugation.

Notation 1.2.6. If K is a number field, we have $\text{Hom}_{\text{fields}}(K, \mathbb{C}) = \Sigma_r \cup \Sigma_c$. We write $r_1 = |\Sigma_r|$ and $2r_2 = |\Sigma_c|$. Hence $[K : \mathbb{Q}] = r_1 + 2r_2$.

Corollary 1.2.7. If K is a number field, consider the map:

$$\Phi : x \in K \mapsto (\sigma(x))_{\sigma \in \Sigma_r \cup \Sigma'_c} \in \mathbb{R}^{\Sigma_r} \oplus \mathbb{C}^{\Sigma'_c}.$$

Then Φ is a homomorphism of \mathbb{Q} -algebras, which induces a homomorphism of \mathbb{R} -algebras:

$$\Phi_{\mathbb{R}} : K \otimes_{\mathbb{Q}} \mathbb{R} \longrightarrow \mathbb{R}^{\Sigma_r} \oplus \mathbb{C}^{\Sigma'_c}.$$

This homomorphism $\Phi_{\mathbb{R}}$ is actually an isomorphism.

Proof. Write $K = \mathbb{Q}(\vartheta) = \mathbb{Q}[T]/(f)$, where $f = f_{\vartheta, \min}$. Hence, $K \otimes_{\mathbb{Q}} \mathbb{R} = \mathbb{R}[T]/(f)$. Now, if g_1, \dots, g_{r_1} (resp. h_1, \dots, h_{r_2}) are the irreducible factors in $\mathbb{R}[T]$ of f of degree 1 (resp. of degree 2), then:

$$K \otimes_{\mathbb{Q}} \mathbb{R} = \mathbb{R}[T]/(f) = (\mathbb{R}[T]/(g_1) \oplus \dots \oplus \mathbb{R}[T]/(g_{r_1})) \oplus (\mathbb{R}[T]/(h_1) \oplus \dots \oplus \mathbb{R}[T]/(h_{r_2})) = \mathbb{R}^{\Sigma_r} \oplus \mathbb{C}^{\Sigma'_c}.$$

Moreover, the implicit isomorphism is $\Phi_{\mathbb{R}}$. □

1.3 Traces, norms and discriminants

Definition 1.3.1 (Traces, norms and discriminants). Let K/K_0 be a finite field extension. If $\alpha \in K$, then the map $m_{\alpha, K/K_0} : x \in K \mapsto \alpha x \in K$ is K_0 -linear. We define:

- (i) The trace of α : $\text{tr}_{K/K_0}(\alpha) = \text{tr}(m_{\alpha, K/K_0}) \in K_0$.
- (ii) The norm of α : $N_{K/K_0}(\alpha) = \det(m_{\alpha, K/K_0}) \in K_0$.
- (iii) The characteristic polynomial of α : $f_{\alpha, K/K_0} = \det(T \text{id}_K - m_{\alpha, K/K_0}) \in K_0[T]$.

We have:

$$f_{\alpha, K/K_0} = T^{[K:K_0]} - \text{tr}_{K/K_0}(\alpha)T^{[K:K_0]-1} + \dots + (-1)^{[K:K_0]}N_{K/K_0}(\alpha).$$

Proposition 1.3.2. Let K be a number field and $\alpha \in K$.

- (i) We have:

$$f_{\alpha, K/\mathbb{Q}} = \prod_{\sigma \in \text{Hom}_{\text{fields}}(K, \mathbb{C})} (T - \sigma(\alpha)).$$

Therefore, $\text{tr}_{K/\mathbb{Q}}(\alpha) = \sum_{\sigma \in \text{Hom}_{\text{fields}}(K, \mathbb{C})} \sigma(\alpha)$ and $N_{K/\mathbb{Q}}(\alpha) = \prod_{\sigma \in \text{Hom}_{\text{fields}}(K, \mathbb{C})} \sigma(\alpha)$.

- (ii) If L is a finite extension of K , then:

$$f_{\alpha, L/\mathbb{Q}} = (f_{\alpha, K/\mathbb{Q}})^{[L:K]}.$$

Therefore, $\text{tr}_{L/\mathbb{Q}}(\alpha) = [L : K] \text{tr}_{K/\mathbb{Q}}(\alpha)$ and $N_{L/\mathbb{Q}}(\alpha) = (N_{K/\mathbb{Q}}(\alpha))^{[L:K]}$.

Proof. Note that $m_{\alpha, K/\mathbb{Q}} : K \rightarrow K$ induces a \mathbb{R} -linear map $K \otimes_{\mathbb{Q}} \mathbb{R} \rightarrow K \otimes_{\mathbb{Q}} \mathbb{R}$. By the isomorphism $K \otimes_{\mathbb{Q}} \mathbb{R} \simeq \mathbb{R}^{\Sigma_r} \oplus \mathbb{C}^{\Sigma'_c}$, it induces a \mathbb{R} -linear map $\Lambda_{\alpha} : \mathbb{R}^{\Sigma_r} \oplus \mathbb{C}^{\Sigma'_c} \rightarrow \mathbb{R}^{\Sigma_r} \oplus \mathbb{C}^{\Sigma'_c}$. Now, compute the matrix of Λ_{α} in the canonical basis and deduce the result. \square

Proposition 1.3.3. *Let K be a number field. Then the map $b_K : (x, y) \in K \times K \mapsto \text{tr}_{K/\mathbb{Q}}(xy) \in \mathbb{Q}$ is a nondegenerate \mathbb{Q} -bilinear form. Moreover, after extending the scalars to \mathbb{R} , the signature of the induced \mathbb{R} -bilinear form $b_{\mathbb{R}} : (K \otimes_{\mathbb{Q}} \mathbb{R}) \times (K \otimes_{\mathbb{Q}} \mathbb{R}) \rightarrow \mathbb{R}$ is $(r_1 + r_2, r_2)$.*

Proof. The \mathbb{Q} -bilinear form $b_K : K \times K \rightarrow \mathbb{Q}$ induces a \mathbb{R} -bilinear form $b_{\mathbb{R}} : (K \otimes_{\mathbb{Q}} \mathbb{R}) \times (K \otimes_{\mathbb{Q}} \mathbb{R}) \rightarrow \mathbb{R}$, which induces a \mathbb{R} -bilinear form $b'_{\mathbb{R}} : (\mathbb{R}^{\Sigma_r} \oplus \mathbb{C}^{\Sigma'_c}) \times (\mathbb{R}^{\Sigma_r} \oplus \mathbb{C}^{\Sigma'_c}) \rightarrow \mathbb{R}$. Now, $b'_{\mathbb{R}}$ is the orthogonal sum of the bilinear forms $\text{tr}_{\mathbb{R}/\mathbb{R}}$ and $\text{tr}_{\mathbb{C}/\mathbb{R}}$. Using this, we show that $b'_{\mathbb{R}}$ is nondegenerate of signature $(r_1 + r_2, r_2)$. \square

Remark 1.3.4. *Proposition 1.3.3 gives an effective way to compute r_1 and r_2 .*

Definition 1.3.5 (Discriminant). *Let K be a number field of degree n . The discriminant of a n -uple $(\omega_1, \dots, \omega_n) \in K^n$ is defined by:*

$$\Delta(\omega_1, \dots, \omega_n) = \det \left(\left(\text{tr}_{K/\mathbb{Q}}(\omega_i \omega_j) \right)_{1 \leq i, j \leq n} \right).$$

Proposition 1.3.6. *Let K be a number field of degree n and $(\omega_1, \dots, \omega_n) \in K^n$.*

(i) *If $\text{Hom}_{\text{fields}}(K, \mathbb{C}) = \{\sigma_1, \dots, \sigma_n\}$, then:*

$$\Delta(\omega_1, \dots, \omega_n) = \det \left((\sigma_j(\omega_i))_{1 \leq i, j \leq n} \right)^2.$$

(ii) *If $A = (a_{ij})_{1 \leq i, j \leq n} \in M_n(\mathbb{Q})$ and $\omega'_i = \sum_{j=1}^n a_{ij} \omega_j$ for $i \in \{1, \dots, n\}$, then:*

$$\Delta(\omega'_1, \dots, \omega'_n) = (\det A)^2 \Delta(\omega_1, \dots, \omega_n).$$

(iii) $\Delta(\omega_1, \dots, \omega_n) \neq 0$ *if and only if* $(\omega_1, \dots, \omega_n)$ *is a \mathbb{Q} -basis of K .*

Example 1.3.7. *Assume that $K = \mathbb{Q}(\alpha)$, and $[K : \mathbb{Q}] = n$. Then $\Delta(1, \alpha, \dots, \alpha^{n-1})$ can be expressed as a Vandermonde determinant, which gives:*

$$\begin{aligned} \Delta(1, \alpha, \dots, \alpha^{n-1}) &= (-1)^{\frac{n(n-1)}{2}} \prod_{\sigma \neq \tau} (\sigma(\alpha) - \tau(\alpha)) \\ &= \text{disc}(f_{\alpha, \min}) \\ &= (-1)^{\frac{n(n-1)}{2}} \text{Res}(f_{\alpha, \min}, f'_{\alpha, \min}) \\ &= (-1)^{\frac{n(n-1)}{2}} N_{K/\mathbb{Q}}(f'_{\alpha, \min}(\alpha)). \end{aligned}$$

Example 1.3.8. *If $d \in \mathbb{Z}$ is not a square, and $K = \mathbb{Q}(\sqrt{d})$, then $\Delta(1, \sqrt{d}) = 4d$.*

1.4 Rings of integers

Definition 1.4.1 (Ring of integer). *If K is a number field, then the ring of integer of K is defined by:*

$$\mathcal{O}_K = \{\alpha \in K, \alpha \text{ is integral over } \mathbb{Z}\} = \{\alpha \in K, f_{\alpha, \min} \in \mathbb{Z}[T]\}.$$

\mathcal{O}_K is a subring of K , and $K = \text{Frac}(\mathcal{O}_K)$.

Example 1.4.2. *Let d be a square-free integer. If $K = \mathbb{Q}(\sqrt{d})$, then:*

$$\mathcal{O}_K = \begin{cases} \mathbb{Z}[\sqrt{d}] & \text{if } d \not\equiv 1 \pmod{4} \\ \mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right] & \text{if } d \equiv 1 \pmod{4} \end{cases}.$$

Proposition 1.4.3. *Let K be a number field. Then \mathcal{O}_K is a free \mathbb{Z} -module of rank $[K : \mathbb{Q}]$.*

Proof. Let $\omega_1, \dots, \omega_n \in \mathcal{O}_K$ s.t. $(\omega_1, \dots, \omega_n)$ is a \mathbb{Q} -basis of K . Consider the bilinear form $b_K : K \times K \rightarrow \mathbb{Q}$ given by the trace and let $(\omega_1^*, \dots, \omega_n^*)$ be the dual basis of $(\omega_1, \dots, \omega_n)$ w.r.t. b_K , i.e. $b_K(\omega_i, \omega_j^*) = \delta_{ij}$ for all i, j . For $\alpha \in \mathcal{O}_K$, one can write:

$$\alpha = \sum_{i=1}^n b_K(\alpha, \omega_i) \omega_i^* = \sum_{i=1}^n \underbrace{\text{tr}_{K/\mathbb{Q}}(\alpha \omega_i)}_{\in \mathbb{Z}} \omega_i^*.$$

Therefore:

$$\bigoplus_{i=1}^n \mathbb{Z} \omega_i \subseteq \mathcal{O}_K \subseteq \bigoplus_{i=1}^n \mathbb{Z} \omega_i^*.$$

This shows that \mathcal{O}_K is a free \mathbb{Z} -module of rank n . □

Proof (Alternative method). Choose $\omega_1, \dots, \omega_n \in \mathcal{O}_K$ s.t. $(\omega_1, \dots, \omega_n)$ is a \mathbb{Q} -basis of K and $\Delta(\omega_1, \dots, \omega_n)$ is minimal. Then we claim that $(\omega_1, \dots, \omega_n)$ is a \mathbb{Z} -basis of \mathcal{O}_K . By contradiction, if there exists $\alpha \in \mathcal{O}_K \setminus \bigoplus_{i=1}^n \mathbb{Z} \omega_i$, write $\alpha = \sum_{i=1}^n a_i \omega_i$, with $a_1, \dots, a_n \in \mathbb{Q}$. We may assume that $a_1 \in \mathbb{Q} \setminus \mathbb{Z}$ and that $0 < a_1 < 1$. Now, we obtain:

$$|\Delta(\alpha, \omega_2, \dots, \omega_n)| = a_1^2 |\Delta(\omega_1, \dots, \omega_n)| < |\Delta(\omega_1, \dots, \omega_n)|,$$

which contradicts the minimality of $\Delta(\omega_1, \dots, \omega_n)$. □

Definition 1.4.4 (Discriminant of a number field). *If K is a number field, then all the \mathbb{Z} -bases of \mathcal{O}_K have the same discriminant. This discriminant is called the discriminant of K and denoted by D_K .*

Proof. If $(\omega_1, \dots, \omega_n)$ and $(\omega'_1, \dots, \omega'_n)$ are two \mathbb{Z} -bases of \mathcal{O}_K , then the matrix of change of basis is $A \in GL_n(\mathbb{Z})$. Hence, $\det A \in \{\pm 1\}$, and so:

$$\Delta(\omega'_1, \dots, \omega'_n) = (\det A)^2 \Delta(\omega_1, \dots, \omega_n) = \Delta(\omega_1, \dots, \omega_n).$$

□

Example 1.4.5. *Let d be a square-free integer. If $K = \mathbb{Q}(\sqrt{d})$, then:*

$$D_K = \begin{cases} 4d & \text{if } d \not\equiv 1 \pmod{4} \\ d & \text{if } d \equiv 1 \pmod{4} \end{cases}.$$

Example 1.4.6. *For any number field K , the sign of D_K is $(-1)^{r_2}$.*

Proposition 1.4.7. *Let K be a number field. Let $\omega_1, \dots, \omega_n \in \mathcal{O}_K$ s.t. $(\omega_1, \dots, \omega_n)$ is a \mathbb{Q} -basis of K . Then:*

$$\Delta(\omega_1, \dots, \omega_n) = \left(\mathcal{O}_K : \bigoplus_{i=1}^n \mathbb{Z} \omega_i \right)^2 D_K.$$

Proof. Let (e_1, \dots, e_n) be a \mathbb{Z} -basis of \mathcal{O}_K . Write $\omega_i = \sum_{j=1}^n a_{ij} e_j$ for $i \in \{1, \dots, n\}$, with $A = (a_{ij})_{1 \leq i, j \leq n} \in M_n(\mathbb{Z})$. Then $\Delta(\omega_1, \dots, \omega_n) = (\det A)^2 D_K$. Now, we have the following commutative diagram:

$$\begin{array}{ccc} \mathbb{Z}^n & \xrightarrow{\times A} & \mathbb{Z}^n \\ \simeq \downarrow & & \simeq \downarrow \\ \bigoplus_{i=1}^n \mathbb{Z} \omega_i & \xrightarrow{\subseteq} & \mathcal{O}_K \end{array}$$

By the Elementary Divisor Theorem, there exist $P, Q \in GL_n(\mathbb{Z})$, $d_1, \dots, d_n \in \mathbb{N}^*$ s.t. $d_i \mid d_{i+1}$ for all i and $A = P \operatorname{diag}(d_1, \dots, d_n) Q$. Hence:

$$\left(\mathcal{O}_K : \bigoplus_{i=1}^n \mathbb{Z}\omega_i \right) = |\mathbb{Z}^n / \operatorname{Im} A| = \left| \prod_{i=1}^n \mathbb{Z}/d_i\mathbb{Z} \right| = d_1 \cdots d_n = |\det A|.$$

□

Corollary 1.4.8. *Let K be a number field. Let $\omega_1, \dots, \omega_n \in \mathcal{O}_K$ s.t. $(\omega_1, \dots, \omega_n)$ is a \mathbb{Q} -basis of K . If $\Delta(\omega_1, \dots, \omega_n)$ is square-free, then $D_K = \Delta(\omega_1, \dots, \omega_n)$ and $\mathcal{O}_K = \bigoplus_{i=1}^n \mathbb{Z}\omega_i$.*

Remark 1.4.9. *We now have an algorithm to compute \mathcal{O}_K , given a number field K :*

- Choose a \mathbb{Q} -basis $(\omega_1, \dots, \omega_n)$ of K in \mathcal{O}_K .
- Compute $\Delta(\omega_1, \dots, \omega_n)$.
- Find a square factor d of $\Delta(\omega_1, \dots, \omega_n)$ (if this is impossible, then $\mathcal{O}_K = \bigoplus_{i=1}^n \mathbb{Z}\omega_i$).
- Try to find a n -uple $(a_1, \dots, a_n) \in \{0, \dots, d-1\}^n$ s.t. $\frac{a_1}{d}\omega_1 + \dots + \frac{a_n}{d}\omega_n \in \mathcal{O}_K$. If this is possible, modify $(\omega_1, \dots, \omega_n)$. Otherwise, try another square factor.

1.5 Cyclotomic number fields

Notation 1.5.1. *If K is a field and $n \in \mathbb{N}^*$, we define:*

- $\mu_n(K) = \{x \in K, x^n = 1\} \leq K^\times$.
- $\mu'_n(K) = \{x \in K, x \text{ is of order } n \text{ in } K^\times\} \leq \mu_n(K)$.

We have $\mu'_n(K) \neq \emptyset \iff |\mu_n(K)| = n$. If this is the case, then $\mu_n(K)$ is a cyclic group and $\mu'_n(K)$ is its set of generators. Elements of $\mu'_n(K)$ are called primitive n -th roots of unity.

Proposition 1.5.2.

(i) *There exists a unique sequence $(\Phi_n)_{n \in \mathbb{N}^*}$ in $\mathbb{Z}[T]$ s.t.*

$$\forall n \in \mathbb{N}^*, T^n - 1 = \prod_{d|n} \Phi_d.$$

Moreover, Φ_n is monic for all $n \in \mathbb{N}^$.*

(ii) *If K is a field of characteristic prime to n , then:*

$$\mu'_n(K) = \{x \in K, \Phi_n(x) = 0\}.$$

The polynomial Φ_n is called the n -th cyclotomic polynomial.

Remark 1.5.3. *In $\mathbb{C}[T]$, one can write $\Phi_n = \prod_{\zeta \in \mu'_n(\mathbb{C})} (T - \zeta)$.*

Definition 1.5.4 (Cyclotomic number field). *The n -th cyclotomic number field is by definition $\mathbb{Q}(\mu_n(\mathbb{C})) = \mathbb{Q}(\mu'_n(\mathbb{C}))$.*

Proposition 1.5.5. *For $n \in \mathbb{N}^*$, Φ_n is irreducible over \mathbb{Q} . Therefore, if $\zeta_n \in \mu'_n(\mathbb{C})$, then:*

$$\mathbb{Q}(\mu_n(\mathbb{C})) = \mathbb{Q}(\zeta_n) = \mathbb{Q}[T]/(\Phi_n).$$

Hence $[\mathbb{Q}(\mu_n(\mathbb{C})) : \mathbb{Q}] = \deg \Phi_n = |\mu'_n(\mathbb{C})| = \varphi(n)$, where φ is the Euler function.

Lemma 1.5.6. *Let p be a prime number and $\nu \in \mathbb{N}^*$. Then $\operatorname{disc}(\Phi_{p^\nu})$ is a power of p .*

Proof. Write $n = p^\nu$. By Example 1.3.7, we have $\text{disc}(\Phi_n) = \pm N_{\mathbb{Q}(\zeta_n)/\mathbb{Q}}(\Phi'_n(\zeta_n))$. Now, write:

$$T^{p^\nu} - 1 = \Phi_{p^\nu}(T) (T^{p^{\nu-1}} - 1).$$

After derivating and evaluating at ζ_n , we obtain:

$$n\zeta_n^{n-1} = \Phi'_n(\zeta_n) (\zeta_n^{p^{\nu-1}} - 1).$$

But $N_{\mathbb{Q}(\zeta_n)/\mathbb{Q}}(\zeta_n) = \pm \Phi_n(0)$ because $f_{\zeta_n, \min} = \Phi_n$, which leads to $N_{\mathbb{Q}(\zeta_n)/\mathbb{Q}}(\zeta_n^{n-1}) = \pm 1$. To compute $N_{\mathbb{Q}(\zeta_n)/\mathbb{Q}}(\zeta_n^{p^{\nu-1}} - 1)$, note that $\xi = \zeta_n^{p^{\nu-1}} \in \mu'_p(\mathbb{C})$, so $f_{\xi, \min} = \Phi_p$ and $f_{\xi-1, \min} = \Phi_p(T+1)$. Thus, $N_{\mathbb{Q}(\xi)/\mathbb{Q}}(\xi - 1) = \pm \Phi_p(1) = \pm p$ because $\Phi_p = T^{p-1} + T^{p-2} + \dots + T + 1$. Now, we easily obtain that $\text{disc}(\Phi_{p^\nu})$ is a power of p . \square

Remark 1.5.7. For $n \geq 3$, if $\zeta_n \in \mu'_n(\mathbb{C})$, we can show that:

$$\text{disc} \Phi_n = \Delta(1, \zeta_n, \dots, \zeta_n^{\varphi(n)-1}) = (-1)^{\frac{\varphi(n)}{2}} \frac{n^{\varphi(n)}}{\prod_{p \text{ prime}} p^{\frac{\varphi(n)}{p-1}}}$$

In particular, the prime factors of $\text{disc} \Phi_n$ are exactly the prime factors of n .

Lemma 1.5.8. Let p be a prime number. Consider a monic polynomial $f \in \mathbb{Z}[T]$. We say that f is p -Eisenstein if $f \equiv T^n \pmod{p}$ and $f(0) \not\equiv 0 \pmod{p}$. In this case:

- (i) f is irreducible over \mathbb{Q} .
- (ii) $p \nmid (\mathcal{O}_K : \mathbb{Z}[\alpha])$ where $K = \mathbb{Q}[T]/(f)$ and α is a root of f in K .

Proof. (ii) By contradiction, let $x \in \mathcal{O}_K \setminus \mathbb{Z}[\alpha]$ s.t. $px \in \mathbb{Z}[\alpha]$. Write $x = \frac{1}{p} \sum_{i=0}^{n-1} u_i \alpha^i$, with $u_0, \dots, u_{n-1} \in \mathbb{Z}$. Since $x \notin \mathbb{Z}[\alpha]$, there exists a minimal index i_0 s.t. $u_{i_0} \notin p\mathbb{Z}$. Hence:

$$\alpha^{n-1-i_0} x = \alpha^{n-1-i_0} \underbrace{\sum_{i=0}^{i_0-1} \frac{u_i}{p} \alpha^i}_{x_1} + \frac{u_{i_0}}{p} \alpha^{n-1} + \underbrace{\frac{\alpha^n}{p} \sum_{i=i_0+1}^{n-1} u_i \alpha^{i-(i_0+1)}}_{x_3}.$$

But α is a root of the Eisenstein polynomial f , so $\alpha^n \in p\mathbb{Z}[\alpha]$, which shows that $x_3 \in \mathbb{Z}[\alpha] \subseteq \mathcal{O}_K$. Moreover, $\alpha^{n-1-i_0} x \in \mathcal{O}_K$ and $x_1 \in \mathbb{Z}[\alpha] \subseteq \mathcal{O}_K$. As a consequence:

$$\frac{u_{i_0}}{p} \alpha^{n-1} \in \mathcal{O}_K.$$

Thus:

$$\mathbb{Z} \ni N_{K/\mathbb{Q}} \left(\frac{u_{i_0}}{p} \alpha^{n-1} \right) = \frac{u_{i_0}^n f(0)^{n-1}}{p^n}.$$

As $p \nmid u_{i_0}$, we obtain $p^n \mid f(0)^{n-1}$, so $p^2 \mid f(0)$, which is a contradiction. \square

Corollary 1.5.9. Let $f \in \mathbb{Z}[T]$ be a p -Eisenstein polynomial. If $K = \mathbb{Q}[T]/(f)$, then:

$$v_p(D_K) = v_p(\text{disc } f).$$

Theorem 1.5.10. If $\zeta_n \in \mu'_n(\mathbb{C})$, then:

$$\mathcal{O}_{\mathbb{Q}(\mu_n(\mathbb{C}))} = \mathbb{Z}[\zeta_n].$$

Equivalently, $D_{\mathbb{Q}(\mu_n(\mathbb{C}))} = \text{disc}(\Phi_n)$.

Proof. *First step:* assume that $n = p^\nu$ is a power of a prime number p . By Lemma 1.5.6, $\text{disc}(\Phi_n)$ is also a power of p , and so is $D_{\mathbb{Q}(\mu_n(\mathbb{C}))}$ because $D_{\mathbb{Q}(\mu_n(\mathbb{C}))} \mid \text{disc}(\Phi_n)$. Therefore, it suffices to show that $v_p(D_{\mu_n(\mathbb{C})}) = v_p(\text{disc}(\Phi_n))$. But we see that $\Phi_n(T+1)$ is p -Eisenstein (because $n = p^\nu$). By Corollary 1.5.9, $v_p(D_{\mu_n(\mathbb{C})}) = v_p(\text{disc}(\Phi_n(T+1))) = v_p(\text{disc}(\Phi_n))$. *Second step:* write $n = p_1^{\nu_1} \cdots p_r^{\nu_r}$, with p_1, \dots, p_r distinct primes. Let $\xi_i = \zeta_n^{np_i^{-\nu_i}} \in \mu_{p_i^{\nu_i}}(\mathbb{C})$ for $i \in \{1, \dots, r\}$. Then we have an algebra homomorphism $\lambda : \mathbb{Q}(\xi_1) \otimes_{\mathbb{Q}} \cdots \otimes_{\mathbb{Q}} \mathbb{Q}(\xi_r) \rightarrow \mathbb{Q}(\zeta_n)$, which is surjective. As the two \mathbb{Q} -algebras have the same dimension, we conclude that λ is an isomorphism, so $\mathbb{Q}(\xi_1) \otimes_{\mathbb{Q}} \cdots \otimes_{\mathbb{Q}} \mathbb{Q}(\xi_r)$ is a field: we say that $\mathbb{Q}(\xi_1), \dots, \mathbb{Q}(\xi_r)$ are *linearly disjoint*. Moreover, $D_{\mathbb{Q}(\xi_1)}, \dots, D_{\mathbb{Q}(\xi_r)}$ are coprime because $D_{\mathbb{Q}(\xi_i)}$ is a power of p_i . These two facts imply that:

$$\mathcal{O}_{\mathbb{Q}(\zeta_n)} = \lambda \left(\mathcal{O}_{\mathbb{Q}(\xi_1)} \otimes_{\mathbb{Z}} \cdots \otimes_{\mathbb{Z}} \mathcal{O}_{\mathbb{Q}(\xi_r)} \right) = \mathbb{Z}[\xi_1, \dots, \xi_r] = \mathbb{Z}[\zeta_n],$$

and $D_{\mathbb{Q}(\zeta_n)} = D_{\mathbb{Q}(\xi_1)} \cdots D_{\mathbb{Q}(\xi_r)}$. □

Corollary 1.5.11. *The prime factors of $D_{\mathbb{Q}(\mu_n(\mathbb{C}))}$ are exactly the prime factors of n .*

2 Ideal factorisation of algebraic numbers

Remark 2.0.1. *Let $K = \mathbb{Q}(\sqrt{-5})$. We know that $\mathcal{O}_K = \mathbb{Z}[\sqrt{-5}]$. In \mathcal{O}_K , we have $6 = 2 \times 3 = (1 + \sqrt{-5})(1 - \sqrt{-5})$: these are two distinct factorisations of 6 in \mathcal{O}_K as products of irreducible elements. Therefore, \mathcal{O}_K is not a factorial domain. The aim of what follows will be to restore factorisation in \mathcal{O}_K .*

2.1 Dedekind rings

Definition 2.1.1 (Dedekind ring). *A ring A is said to be Dedekind if the three following conditions are satisfied:*

- (i) *A is integrally closed, i.e. integrally closed in its fraction field.*
- (ii) *A is noetherian.*
- (iii) *Every nonzero prime ideal of A is maximal.*

Remark 2.1.2. *Condition (iii) in the definition of Dedekind rings can be rewritten as $\dim A \leq 1$, where $\dim A$ is the Krull dimension of A .*

Example 2.1.3. *Fields and principal ideal domains are Dedekind.*

Proposition 2.1.4. *Let K be a number field. Then \mathcal{O}_K is Dedekind.*

Proof. As \mathcal{O}_K is a free \mathbb{Z} -module of finite rank (by Proposition 1.4.3), \mathcal{O}_K is noetherian. Now, let $x \in \text{Frac}(\mathcal{O}_K) = K$ be integral over \mathcal{O}_K . Then there exists a sub \mathcal{O}_K -module $0 \subsetneq M \subseteq K$ of finite type s.t. $xM \subseteq M$. But as \mathcal{O}_K is itself a \mathbb{Z} -module of finite type, so is M . Therefore, x is integral over \mathbb{Z} and $x \in \mathcal{O}_K$; this proves that \mathcal{O}_K is integrally closed. Finally, let \mathfrak{p} be a nonzero prime ideal in \mathcal{O}_K and let $x \in \mathfrak{p} \setminus \{0\}$. Then we have $x\mathcal{O}_K \subseteq \mathfrak{p} \subseteq \mathcal{O}_K$. As $x\mathcal{O}_K$ and \mathcal{O}_K are free \mathbb{Z} -modules of rank $[K : \mathbb{Q}]$, so is \mathfrak{p} . Therefore, $\mathcal{O}_K/\mathfrak{p}$ is a finite integral domain, so it is a field and \mathfrak{p} is maximal. □

2.2 Factorisation of ideals in Dedekind rings

Proposition 2.2.1. *Let A be a Dedekind ring. Let $I^+(A)$ be the set of nonzero ideals of A and let P be the set of nonzero prime ideals of A . Then there is a natural monoid structure on $I^+(A)$ (given by multiplication of ideals), and this structure is compatible with the inclusion: if $\mathfrak{a} \subseteq \mathfrak{b}$, then $\mathfrak{a}\mathfrak{c} \subseteq \mathfrak{b}\mathfrak{c}$. Moreover, we have a monoid homomorphism:*

$$\varphi : \begin{cases} \mathbb{N}^{(P)} & \longrightarrow I^+(A) \\ (m_{\mathfrak{p}})_{\mathfrak{p} \in P} & \longmapsto \prod_{\mathfrak{p} \in P} \mathfrak{p}^{m_{\mathfrak{p}}} \end{cases},$$

where $\mathbb{N}^{(P)}$ is the set of sequences indexed by P with a finite number of nonzero terms.

Definition 2.2.2 (Fractional ideals). *Let A be a Dedekind ring. A fractional ideal of A is a nonzero A -submodule \mathfrak{a} of $K = \text{Frac}(A)$ s.t. $\exists d \in A \setminus \{0\}$, $d\mathfrak{a} \subseteq A$. The set of fractional ideals of A will be denoted by $I(A)$; it is a monoid.*

Lemma 2.2.3. *Let A be a noetherian ring. Then every nonzero ideal of A contains a finite product of nonzero prime ideals.*

Proof. If there exists a nonzero ideal \mathfrak{a} of A s.t. \mathfrak{a} does not contain any finite product of nonzero prime ideals, then, since A is noetherian, we may assume \mathfrak{a} to be maximal among the ideals satisfying this property. Now, \mathfrak{a} is not a prime ideal so there exist $a, b \in A \setminus \mathfrak{a}$ s.t. $ab \in \mathfrak{a}$. Hence, $\mathfrak{a} \subsetneq \mathfrak{a} + Aa$, so there exist prime ideals $\mathfrak{p}_1, \dots, \mathfrak{p}_r$ s.t. $\mathfrak{a} + Aa \supseteq \mathfrak{p}_1 \cdots \mathfrak{p}_r$. Likewise, there exist prime ideals $\mathfrak{q}_1, \dots, \mathfrak{q}_s$ s.t. $\mathfrak{a} + Ab \supseteq \mathfrak{q}_1 \cdots \mathfrak{q}_s$. Now, $\mathfrak{a} = \mathfrak{a} + Aab \supseteq (\mathfrak{a} + Aa)(\mathfrak{a} + Ab) \supseteq \mathfrak{p}_1 \cdots \mathfrak{p}_r \mathfrak{q}_1 \cdots \mathfrak{q}_s$, a contradiction. \square

Notation 2.2.4. *Let A be a Dedekind ring. For $\mathfrak{a} \in I^+(A)$, we set:*

$$\tilde{\mathfrak{a}} = \{x \in K, x\mathfrak{a} \subseteq A\} \in I(A).$$

Lemma 2.2.5. *Let A be a Dedekind ring and let \mathfrak{p} be a nonzero prime ideal of A .*

- (i) $A \subsetneq \tilde{\mathfrak{p}}$.
- (ii) $\mathfrak{p} \cdot \tilde{\mathfrak{p}} = A$.

Proof. (i) Let $x \in \mathfrak{p} \setminus \{0\}$. By Lemma 2.2.3, there exist prime ideals $\mathfrak{p}_1, \dots, \mathfrak{p}_r$ s.t. $\mathfrak{p}_1 \cdots \mathfrak{p}_r \subseteq Ax$, with r minimal. Since $\mathfrak{p}_1 \cdots \mathfrak{p}_r \subseteq \mathfrak{p}$, there exists i s.t. $\mathfrak{p}_i \subseteq \mathfrak{p}$ and therefore $\mathfrak{p}_i = \mathfrak{p}$ (because \mathfrak{p}_i is maximal since A is Dedekind). We may assume that $i = 1$, thus $\mathfrak{p}\mathfrak{p}_2 \cdots \mathfrak{p}_r \subsetneq Ax \subseteq \mathfrak{p}$, and $\mathfrak{p}_2 \cdots \mathfrak{p}_r \not\subseteq Ax$ by minimality of r . Choose $y \in \mathfrak{p}_2 \cdots \mathfrak{p}_r \setminus Ax$. Hence, $\frac{y}{x} \in \tilde{\mathfrak{p}} \setminus A$, which proves the result. (ii) We have $A \subseteq \tilde{\mathfrak{p}}$, so $\mathfrak{p} \subseteq \mathfrak{p}\tilde{\mathfrak{p}} \subseteq A$. Therefore, $\mathfrak{p}\tilde{\mathfrak{p}} = \mathfrak{p}$ or $\mathfrak{p}\tilde{\mathfrak{p}} = A$ (because \mathfrak{p} is maximal because A is Dedekind). The first case cannot happen: if $\mathfrak{p}\tilde{\mathfrak{p}} = \mathfrak{p}$, then elements of $\tilde{\mathfrak{p}}$ stabilise the A -module \mathfrak{p} , so by the Cayley-Hamilton Theorem, they are integral over A , so they are in A because A is integrally closed. Therefore, $\mathfrak{p}\tilde{\mathfrak{p}} = A$. \square

Theorem 2.2.6. *Let A be a Dedekind ring. Then the homomorphism $\varphi : \mathbb{N}^{(P)} \rightarrow I^+(A)$ of Proposition 2.2.1 is an isomorphism.*

Proof. We extend φ to a map $\varphi : \mathbb{Z}^{(P)} \rightarrow I(A)$. We shall prove that $I(A)$ is a group, that φ is a group isomorphism and that $\varphi(\mathbb{N}^{(P)}) = I^+(A)$. *Surjectivity of φ .* By contradiction, consider an ideal $\mathfrak{a} \in I^+(A) \setminus \text{Im } \varphi$ and assume that \mathfrak{a} is maximal among the ideals of $I^+(A) \setminus \text{Im } \varphi$ (because A is noetherian). Then \mathfrak{a} is a strict ideal of A that is not prime, so there exists a prime ideal \mathfrak{p} s.t. $\mathfrak{a} \subsetneq \mathfrak{p}$. Therefore, $\mathfrak{a} \subsetneq \tilde{\mathfrak{p}}\mathfrak{a} \subseteq A$ (using Lemma 2.2.5). By maximality of \mathfrak{a} , we have $\tilde{\mathfrak{p}}\mathfrak{a} \in \text{Im } \varphi$, so $\mathfrak{a} = \tilde{\mathfrak{p}}\mathfrak{a} \in \mathfrak{p}\text{Im } \varphi \subseteq \text{Im } \varphi$, a contradiction. Now, if $\mathfrak{a} \in I(A)$, let $d \in A \setminus \{0\}$ s.t. $d\mathfrak{a} \subseteq A$. Write $d\mathfrak{a} = \varphi((m_{\mathfrak{p}})_{\mathfrak{p} \in P})$, $dA = \varphi((n_{\mathfrak{p}})_{\mathfrak{p} \in P})$, so that $\mathfrak{a} = \varphi((m_{\mathfrak{p}})_{\mathfrak{p} \in P} - (n_{\mathfrak{p}})_{\mathfrak{p} \in P}) \in \text{Im } \varphi$. *Injectivity of φ .* Let $(m_{\mathfrak{p}})_{\mathfrak{p} \in P} \in \mathbb{Z}^{(P)}$, $(n_{\mathfrak{p}})_{\mathfrak{p} \in P} \in \mathbb{Z}^{(P)}$ s.t. $\varphi((m_{\mathfrak{p}})_{\mathfrak{p} \in P}) = \varphi((n_{\mathfrak{p}})_{\mathfrak{p} \in P})$. We may assume that

$\forall \mathfrak{p} \in P, \min \{m_{\mathfrak{p}}, n_{\mathfrak{p}}\} = 0$. Now, if there exists $\mathfrak{p} \in P$ with $m_{\mathfrak{p}} > 0$, then $\mathfrak{p} \supseteq \prod_{\mathfrak{q} \in P} \mathfrak{q}^{n_{\mathfrak{q}}}$, so there exists $\mathfrak{q} \in P$ s.t. $\mathfrak{q} \subseteq \mathfrak{p}$ and $n_{\mathfrak{q}} > 0$. Thus $\mathfrak{q} = \mathfrak{p}$, which contradicts the assumption that $\min \{m_{\mathfrak{p}}, n_{\mathfrak{p}}\} = 0$. *Existence of inverses in $I(A)$.* If $\mathfrak{a} \in I(A)$, we can write $\mathfrak{a} = \prod_{\mathfrak{p} \in P} \mathfrak{p}^{m_{\mathfrak{p}}}$, so that $\mathfrak{a}^{-1} = \prod_{\mathfrak{p} \in P} \mathfrak{p}^{-m_{\mathfrak{p}}}$, and we may check that $\mathfrak{a}^{-1} = \tilde{\mathfrak{a}}$. *Image of $\mathbb{N}^{(P)}$.* It is clear that $\varphi(\mathbb{N}^{(P)}) \subseteq I^+(A)$. Conversely, if $\mathfrak{a} \in I^+(A)$, write $\mathfrak{a} = \prod_{\mathfrak{p} \in P} \mathfrak{p}^{m_{\mathfrak{p}}} \subseteq A$. Thus:

$$\prod_{m_{\mathfrak{p}} \geq 0} \mathfrak{p}^{m_{\mathfrak{p}}} \subseteq \prod_{m_{\mathfrak{p}} < 0} \mathfrak{p}^{-m_{\mathfrak{p}}}.$$

If there exists \mathfrak{q} s.t. $m_{\mathfrak{q}} < 0$, then $\prod_{m_{\mathfrak{p}} \geq 0} \mathfrak{p}^{m_{\mathfrak{p}}} \subseteq \mathfrak{q}$ and there exists \mathfrak{p} with $\mathfrak{p} = \mathfrak{q}$ and $m_{\mathfrak{p}} \geq 0$, a contradiction. Thus, $\mathfrak{a} \in \varphi(\mathbb{N}^{(P)})$. \square

Definition 2.2.7 (\mathfrak{p} -adic valuation). *Let A be a Dedekind ring. For $\mathfrak{a} \in I^+(A)$, we can write uniquely $\mathfrak{a} = \prod_{\mathfrak{p} \in P} \mathfrak{p}^{v_{\mathfrak{p}}(\mathfrak{a})}$. For $\mathfrak{p} \in P$, the function $v_{\mathfrak{p}} : I^+(A) \rightarrow \mathbb{N}$ thus defined is called the \mathfrak{p} -adic valuation.*

Proposition 2.2.8. *Let A be a Dedekind ring and let $\mathfrak{a}, \mathfrak{b} \in I^+(A)$. Then:*

- (i) $\forall \mathfrak{p} \in P, v_{\mathfrak{p}}(\mathfrak{a}\mathfrak{b}) = v_{\mathfrak{p}}(\mathfrak{a}) + v_{\mathfrak{p}}(\mathfrak{b})$.
- (ii) $\mathfrak{a} \subseteq \mathfrak{b} \iff \forall \mathfrak{p} \in P, v_{\mathfrak{p}}(\mathfrak{b}) \leq v_{\mathfrak{p}}(\mathfrak{a})$.
- (iii) $\forall \mathfrak{p} \in P, v_{\mathfrak{p}}(\mathfrak{a} + \mathfrak{b}) = \min \{v_{\mathfrak{p}}(\mathfrak{a}), v_{\mathfrak{p}}(\mathfrak{b})\}$.
- (iv) $\forall \mathfrak{p} \in P, v_{\mathfrak{p}}(\mathfrak{a} \cap \mathfrak{b}) = \max \{v_{\mathfrak{p}}(\mathfrak{a}), v_{\mathfrak{p}}(\mathfrak{b})\}$.

Definition 2.2.9 (Divisibility in $I^+(A)$). *Let A be a Dedekind ring. If $\mathfrak{a}, \mathfrak{b} \in I^+(A)$, we say that $\mathfrak{a} \mid \mathfrak{b}$ if one of the following two equivalent conditions is satisfied:*

- (i) $\exists \mathfrak{c} \in I^+(A), \mathfrak{b} = \mathfrak{a}\mathfrak{c}$.
- (ii) $\mathfrak{b} \subseteq \mathfrak{a}$.

Remark 2.2.10. *Let A be a Dedekind ring. For $a, b \in A \setminus \{0\}$, we have $a \mid b$ (in A) if and only if $(a) \mid (b)$ (in $I^+(A)$).*

Proposition 2.2.11. *Let A be a Dedekind ring.*

- (i) *For $\mathfrak{a}, \mathfrak{b} \in I^+(A)$, we have $\mathfrak{a} + \mathfrak{b} = \gcd(\mathfrak{a}, \mathfrak{b})$ and $\mathfrak{a} \cap \mathfrak{b} = \text{lcm}(\mathfrak{a}, \mathfrak{b})$ (where the gcd and lcm are defined by the notion of divisibility in $I^+(A)$). In particular:*

$$\gcd(\mathfrak{a}, \mathfrak{b}) \cdot \text{lcm}(\mathfrak{a}, \mathfrak{b}) = \mathfrak{a}\mathfrak{b}.$$

- (ii) *Every $\mathfrak{a} \in I^+(A)$ has a multiple which is a principal ideal. Moreover, we have:*

$$\mathfrak{a} = \gcd((x), x \in \mathfrak{a} \setminus \{0\}).$$

- (iii) *Let $\mathfrak{a}, \mathfrak{b} \in I^+(A)$ and assume that \mathfrak{a} and \mathfrak{b} are coprime (i.e. $\mathfrak{a} + \mathfrak{b} = A$). Then:*

$$A/\mathfrak{a}\mathfrak{b} \simeq A/\mathfrak{a} \oplus A/\mathfrak{b}.$$

Example 2.2.12. *Let $K = \mathbb{Q}(\sqrt{-5})$. We know that $\mathcal{O}_K = \mathbb{Z}[\sqrt{-5}]$. We have $6 = 2 \times 3 = (1 + \sqrt{-5})(1 - \sqrt{-5})$. Now, if we set $\mathfrak{p}_2 = (2, 1 + \sqrt{-5}) = (2, 1 - \sqrt{-5})$, $\mathfrak{p}_3 = (3, 1 + \sqrt{-5})$ and $\mathfrak{p}'_3 = (3, 1 - \sqrt{-5})$, then $\mathfrak{p}_2, \mathfrak{p}_3, \mathfrak{p}'_3$ are prime in \mathcal{O}_K (which we show by computing $\mathcal{O}_K/\mathfrak{p}_2$, etc.). And we have:*

$$\mathfrak{p}_2^2 = (2), \quad \mathfrak{p}_2\mathfrak{p}_3 = (1 + \sqrt{-5}), \quad \mathfrak{p}_2\mathfrak{p}'_3 = (1 - \sqrt{-5}), \quad \mathfrak{p}_3\mathfrak{p}'_3 = (3).$$

Thus, the unique factorisation of (6) is $(6) = \mathfrak{p}_2^2\mathfrak{p}_3\mathfrak{p}'_3$.

2.3 Class group

Definition 2.3.1 (Class group of a Dedekind ring). *Let A be a Dedekind ring. Then we have an exact sequence:*

$$1 \longrightarrow A^\times \longrightarrow K^\times \longrightarrow I(A) \longrightarrow \text{Cl}(A) \longrightarrow 1,$$

where $\text{Cl}(A) = I(A)/K^\times$ and where the map $K^\times \rightarrow I(A)$ is given by $x \mapsto Ax$. The group $\text{Cl}(A)$ is called the class group of A .

Proposition 2.3.2. *Let A be a Dedekind ring. Then the following three assertions are equivalent:*

- (i) A is principal.
- (ii) A is factorial.
- (iii) $\text{Cl}(A) = \{1\}$.

Remark 2.3.3. *If K is a number field, then the group $\text{Cl}(\mathcal{O}_K)$ is finite.*

2.4 Factorisation and ramification

Definition 2.4.1 (Norm of an ideal). *Let K be a number field. If \mathfrak{a} is a nonzero ideal of \mathcal{O}_K , we define the norm of \mathfrak{a} by:*

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

$N(\mathfrak{a})$ is finite because \mathfrak{a} is a free \mathbb{Z} -module of rank $[K : \mathbb{Q}]$, as we have seen in the proof of Proposition 2.1.4.

Proposition 2.4.2. *Let K be a number field.*

- (i) *If $\alpha \in \mathcal{O}_K \setminus \{0\}$, then:*

$$N(\alpha\mathcal{O}_K) = |N_{K/\mathbb{Q}}(\alpha)|.$$

- (ii) *N is multiplicative: $N(\mathfrak{a}\mathfrak{b}) = N(\mathfrak{a})N(\mathfrak{b})$ for every nonzero ideals \mathfrak{a} and \mathfrak{b} of \mathcal{O}_K .*

Proof. (i) Note that $N_{K/\mathbb{Q}}(\alpha) = \det(m_\alpha)$, where $m_\alpha : \mathcal{O}_K \rightarrow \mathcal{O}_K$ is the multiplication by α . Now, consider the following commutative diagram:

$$\begin{array}{ccc} \mathbb{Z}^n & \xrightarrow{\times A} & \mathbb{Z}^n \\ \simeq \downarrow & & \simeq \downarrow \\ \mathcal{O}_K & \xrightarrow{m_\alpha} & \mathcal{O}_K \end{array}$$

Thus, $N(\alpha\mathcal{O}_K) = |\mathcal{O}_K/\alpha\mathcal{O}_K| = |\mathbb{Z}^n/\text{Im } A|$. But using the Elementary Divisor Theorem, we see that $|\mathbb{Z}^n/\text{Im } A| = |\det A| = |N_{K/\mathbb{Q}}(\alpha)|$, as in the proof of Proposition 1.4.7. (ii) It suffices to prove the result for prime ideals. Thus, let \mathfrak{p} and \mathfrak{q} be two nonzero prime ideals of A . If $\mathfrak{p} \neq \mathfrak{q}$, then $\mathcal{O}_K/\mathfrak{p}\mathfrak{q} \simeq (\mathcal{O}_K/\mathfrak{p}) \times (\mathcal{O}_K/\mathfrak{q})$, and the result is clear. If $\mathfrak{p} = \mathfrak{q}$, then we have an exact sequence:

$$0 \longrightarrow \mathfrak{p}/\mathfrak{p}^2 \longrightarrow \mathcal{O}_K/\mathfrak{p}^2 \longrightarrow \mathcal{O}_K/\mathfrak{p} \longrightarrow 0,$$

so it suffices to prove that $|\mathfrak{p}/\mathfrak{p}^2| = |\mathcal{O}_K/\mathfrak{p}|$. But $\mathfrak{p}/\mathfrak{p}^2$ is an $(\mathcal{O}_K/\mathfrak{p})$ -vector space, so it suffices to prove that $\dim_{\mathcal{O}_K/\mathfrak{p}}(\mathfrak{p}/\mathfrak{p}^2) = 1$. To do this, choose $a \in \mathfrak{p} \setminus \mathfrak{p}^2$. We can write $(a) = \mathfrak{p}^m \mathfrak{b}$, with \mathfrak{b} prime to \mathfrak{p} , $m \in \mathbb{N}$. Since $a \in \mathfrak{p}$, we have $m \geq 1$; since $a \notin \mathfrak{p}^2$, we have $m < 2$, so $m = 1$ and $(a) = \mathfrak{p}\mathfrak{b}$. As $A = \mathfrak{p} + \mathfrak{b}$, we obtain $\mathfrak{p} = \mathfrak{p}^2 + \mathfrak{p}\mathfrak{b} = \mathfrak{p}^2 + (a)$, so $\mathfrak{p}/\mathfrak{p}^2 = \text{Vect}_{\mathcal{O}_K/\mathfrak{p}}(\bar{a})$. \square

Definition 2.4.3 (Norm of a fractional ideal). *Let K be a number field. If \mathfrak{a} is a fractional ideal of \mathcal{O}_K and $d \in \mathcal{O}_K \setminus \{0\}$ is s.t. $d\mathfrak{a} \subseteq \mathcal{O}_K$, then we define:*

$$N(\mathfrak{a}) = N(d\mathfrak{a}) \left| N_{K/\mathbb{Q}}(d) \right|^{-1}.$$

This definition does not depend on the choice of d .

Remark 2.4.4. *Let K be a number field. If \mathfrak{p} is a prime ideal of \mathcal{O}_K , then there exists a unique prime number p s.t. $\mathfrak{p} \cap \mathbb{Z} = p\mathbb{Z}$, i.e. $p \in \mathfrak{p}$, i.e. $\mathfrak{p} \mid p$.*

Definition 2.4.5 (Residual degree and ramification index). *Let K be a number field. If \mathfrak{p} is a prime ideal of \mathcal{O}_K , let p be the unique prime number s.t. $\mathfrak{p} \mid p$. Then the natural map $\mathbb{Z} \rightarrow \mathcal{O}_K/\mathfrak{p}$ induces a field extension $\mathbb{F}_p \rightarrow \mathcal{O}_K/\mathfrak{p}$.*

(i) *We define the residual degree of \mathfrak{p} by:*

$$f(\mathfrak{p}/p) = \dim_{\mathbb{F}_p}(\mathcal{O}_K/\mathfrak{p}).$$

(ii) *We define the ramification index of \mathfrak{p} by:*

$$e(\mathfrak{p}/p) = v_{\mathfrak{p}}(p\mathcal{O}_K).$$

We say that p is ramified in K if there exists a prime ideal $\mathfrak{p} \mid p$ s.t. $e(\mathfrak{p}/p) \geq 2$.

Proposition 2.4.6. *Let K be a number field and let p be a prime number.*

(i) $\sum_{\mathfrak{p}|p} e(\mathfrak{p}/p) f(\mathfrak{p}/p) = [K : \mathbb{Q}]$.

(ii) *For all $c \in \mathbb{R}$, the set of ideals in \mathcal{O}_K whose norm is bounded by c is finite.*

Proof. (i) Write:

$$p\mathcal{O}_K = \prod_{\mathfrak{p}|p} \mathfrak{p}^{e(\mathfrak{p}/p)}.$$

Computing the norms of both sides gives the result. (ii) Let $c \in \mathbb{R}$ and let \mathfrak{a} be a nonzero ideal of \mathcal{O}_K s.t. $N(\mathfrak{a}) \leq c$. Write $\mathfrak{a} = \mathfrak{p}_1^{m_1} \cdots \mathfrak{p}_r^{m_r}$, and let p_i be a prime number s.t. $\mathfrak{p}_i \mid p_i$ for all i . Then:

$$c \geq N(\mathfrak{a}) = N(\mathfrak{p}_1)^{m_1} \cdots N(\mathfrak{p}_r)^{m_r} = p_1^{m_1 f(\mathfrak{p}_1/p_1)} \cdots p_r^{m_r f(\mathfrak{p}_r/p_r)}.$$

Now, there is only a finite number of possibilities for p_1, \dots, p_r , so there is only a finite number of possibilities for $\mathfrak{p}_1, \dots, \mathfrak{p}_r$ (because each prime number has a finite number of divisors in \mathcal{O}_K). There is also a finite number of possibilities for m_1, \dots, m_r , so there is only a finite number of possibilities for \mathfrak{a} . \square

Proposition 2.4.7. *Let $K = \mathbb{Q}(\alpha)$ be a number field, with $\alpha \in \mathcal{O}_K$ and $f = f_{\alpha, \min} \in \mathbb{Z}[T]$. Let p be a prime number s.t. $p \nmid (\mathcal{O}_K : \mathbb{Z}[\alpha])$. Consider a factorisation $f = h_1^{e_1} \cdots h_r^{e_r}$ of f in $\mathbb{F}_p[T]$, with h_1, \dots, h_r distinct irreducible polynomials in $\mathbb{F}_p[T]$ and $e_1, \dots, e_r \geq 1$. For $1 \leq i \leq r$, let g_i be a representative of h_i in $\mathbb{Z}[T]$. Then:*

(i) *The ideals $\mathfrak{p}_i = (p, g_i(\alpha))$, for $1 \leq i \leq r$, are prime and distinct.*

(ii) *For $1 \leq i \leq r$, $e(\mathfrak{p}_i/p) = e_i$ and $f(\mathfrak{p}_i/p) = \deg h_i$.*

(iii) $p\mathcal{O}_K = \prod_{i=1}^r \mathfrak{p}_i^{e_i}$.

Proof. We have the following commutatives diagram with exact rows and columns:

$$\begin{array}{ccccccc}
& & 0 & & 0 & & 0 \\
& & \downarrow & & \downarrow & & \downarrow \\
0 & \longrightarrow & \mathbb{Z}[\alpha] & \longrightarrow & \mathcal{O}_K & \longrightarrow & \mathcal{O}_K/\mathbb{Z}[\alpha] \longrightarrow 0 \\
& & \times p \downarrow & & \times p \downarrow & & \times p \downarrow \\
0 & \longrightarrow & \mathbb{Z}[\alpha] & \longrightarrow & \mathcal{O}_K & \longrightarrow & \mathcal{O}_K/\mathbb{Z}[\alpha] \longrightarrow 0 \\
& & \downarrow & & \downarrow & & \downarrow \\
& & \mathbb{Z}[\alpha]/p\mathbb{Z}[\alpha] & & \mathcal{O}_K/p\mathcal{O}_K & & 0
\end{array}$$

The Snake Lemma gives an exact sequence $0 \longrightarrow \mathbb{Z}[\alpha]/p\mathbb{Z}[\alpha] \longrightarrow \mathcal{O}_K/p\mathcal{O}_K \longrightarrow 0$, which shows that:

$$\mathbb{Z}[\alpha]/p\mathbb{Z}[\alpha] \simeq \mathcal{O}_K/p\mathcal{O}_K.$$

Now, for $1 \leq i \leq r$, we have:

$$\mathcal{O}_K/\mathfrak{p}_i = \mathcal{O}_K/(p, g_i(\alpha)) \simeq \mathbb{Z}[\alpha]/(p, g_i(\alpha)) \simeq \mathbb{Z}[T]/(f, p, g_i) \simeq \mathbb{F}_p[T]/(h_i),$$

so $\mathcal{O}_K/\mathfrak{p}_i$ is a field and \mathfrak{p}_i is prime. Moreover, we have a map $\varphi_i : \mathbb{F}_p[T] \rightarrow \mathcal{O}_K/\mathfrak{p}_i \simeq \mathbb{F}_p[T]/(h_i)$ given by the canonical projection. Since $\text{Ker } \varphi_i = (h_i)$, it is clear that $\mathfrak{p}_i \neq \mathfrak{p}_j$ for $i \neq j$ (because $(h_i) \neq (h_j)$ for $i \neq j$). Furthermore:

$$f(\mathfrak{p}_i/p) = \dim_{\mathbb{F}_p}(\mathcal{O}_K/\mathfrak{p}_i) = \dim_{\mathbb{F}_p}(\mathbb{F}_p[T]/(h_i)) = \deg h_i.$$

Finally, note that:

$$\prod_{i=1}^r \mathfrak{p}_i^{e_i} = \prod_{i=1}^r (p, g_i(\alpha))^{e_i} \subseteq \prod_{i=1}^r (p, g_i(\alpha)^{e_i}) \subseteq \left(p, \prod_{i=1}^r g_i(\alpha)^{e_i} \right) \subseteq p\mathcal{O}_K.$$

Computing the norms of both sides, we obtain $N(\prod_{i=1}^r \mathfrak{p}_i^{e_i}) = N(p\mathcal{O}_K)$, so $\prod_{i=1}^r \mathfrak{p}_i^{e_i} = p\mathcal{O}_K$. \square

Remark 2.4.8. Factorisation of polynomials in $\mathbb{F}_p[T]$ is effective, so Proposition 2.4.7 gives an algorithm to compute $p\mathcal{O}_K$ for some values of p .

Corollary 2.4.9. Let $K = \mathbb{Q}(\alpha)$ be a number field, with $\alpha \in \mathcal{O}_K$. Assume that $f = f_{\alpha, \min}$ is p -Eisenstein. Then:

$$p\mathcal{O}_K = \mathfrak{p}^{[K:\mathbb{Q}]},$$

with $\mathfrak{p} = (p, \alpha)$.

Example 2.4.10. If $K = \mathbb{Q}(\mu_{p^m}(\mathbb{C}))$ and $\zeta_{p^m} \in \mu'_{p^m}(\mathbb{C})$, then $\Phi_{p^m}(T+1)$ is p -Eisenstein. By Corollary 2.4.9, $p\mathcal{O}_K = \mathfrak{p}^{p^{m-1}(p-1)}$, with $\mathfrak{p} = (p, \zeta_{p^m} - 1)$. Moreover, using the fact that $\Phi_{p^m}(T+1)$ is p -Eisenstein, we see that $p \in (\zeta_{p^m} - 1)$. Therefore $p\mathcal{O}_K = (\zeta_{p^m} - 1)^{p^{m-1}(p-1)}$, and there exists $\varepsilon \in \mathcal{O}_K^\times$ s.t. $p = \varepsilon(\zeta_{p^m} - 1)^{p^{m-1}(p-1)}$.

Lemma 2.4.11. Let L/K be a finite and separable field extension. Then the symmetric bilinear form $b : (x, y) \in L \times L \mapsto \text{tr}_{L/K}(xy)$ is nondegenerate.

Proof. Let $a \in L$. Let K^{alg} be the algebraic closure of K . Thus, for $x, y \in L$

$$\text{tr}_{L/K}(xy) = \sum_{\sigma \in \text{Hom}_{\text{fields}}(L, K^{\text{alg}})} \sigma(x)\sigma(y).$$

If $b(x, \cdot) = 0$, then $\sum_{\sigma \in \text{Hom}_{\text{fields}}(L, K^{\text{alg}})} \sigma(x)\sigma = 0$. By the linear independence of characters, this implies that $\sigma(x) = 0$ for all $\sigma \in \text{Hom}_{\text{fields}}(L, K^{\text{alg}})$, and therefore $x = 0$. This proves that b is nondegenerate. \square

Theorem 2.4.12. *Let K be a number field. Then a prime number p is ramified in K if and only if $p \mid D_K$.*

Proof. Consider the symmetric nondegenerate bilinear form $b : (x, y) \in K \times K \mapsto \text{tr}_{K/\mathbb{Q}}(xy) \in \mathbb{Q}$. Note that b induces a \mathbb{Z} -bilinear form $b : \mathcal{O}_K \times \mathcal{O}_K \rightarrow \mathbb{Z}$. Now, consider the \mathbb{F}_p -algebra $A = \mathcal{O}_K/p\mathcal{O}_K$, and denote by $\bar{\cdot}$ the projection $\mathcal{O}_K \rightarrow A$. We have:

$$\forall x, y \in \mathcal{O}_K, \overline{b(x, y)} = \overline{\text{tr}(\mathcal{O}_K \xrightarrow{\times xy} \mathcal{O}_K)} = \text{tr}(\mathcal{O}_K/p\mathcal{O}_K \xrightarrow{\times \overline{xy}} \mathcal{O}_K/p\mathcal{O}_K) = \text{tr}_{A/\mathbb{F}_p}(\overline{xy}) = \bar{b}(\bar{x}, \bar{y}),$$

where $\bar{b} : A \times A \rightarrow \mathbb{F}_p$ is the bilinear form induced by the trace. If $B \in M_n(\mathbb{Z})$ is the matrix of b in a \mathbb{Z} -basis e of \mathcal{O}_K , then $\bar{B} \in M_n(\mathbb{F}_p)$ is the matrix of \bar{b} in the basis \bar{e} of A . Therefore, \bar{b} is degenerate iff $\det \bar{B} = \det B = 0$ iff $p \mid \det B = D_K$. It remains to show that \bar{b} is degenerate iff p ramifies in K . To do this, factorise $p\mathcal{O}_K = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_r^{e_r}$ and apply the Chinese Remainder Theorem to obtain the following isomorphism of \mathbb{F}_p -algebras:

$$A \simeq \bigoplus_{i=1}^r \mathcal{O}_K/\mathfrak{p}_i^{e_i}.$$

Thus $\bar{b} = \bigoplus_{i=1}^r \bar{b}_i$, with $\bar{b}_i = \text{tr}_{(\mathcal{O}_K/\mathfrak{p}_i^{e_i})/\mathbb{F}_p}$. Thus, \bar{b} is degenerate iff there exists $1 \leq i \leq r$ s.t. \bar{b}_i is degenerate. We shall now show that \bar{b}_i is degenerate iff $e_i > 1$. If $e_i > 1$, then $A_i = \mathcal{O}_K/\mathfrak{p}_i^{e_i}$ contains a nilpotent element \bar{x} , so $\bar{b}_i(\bar{x}, \bar{y}) = 0$ for all $\bar{y} \in A_i$, which shows that \bar{b}_i is degenerate. Conversely, assume that $e_i = 1$. Note that A_i is a finite (separable) extension of \mathbb{F}_p , so by Lemma 2.4.11, \bar{b}_i is nondegenerate. \square

Example 2.4.13. *By Theorem 2.4.12 and Corollary 1.5.11, p ramifies in $D_{\mathbb{Q}(\mu_n(\mathbb{C}))}$ iff $p \mid n$.*

2.5 Factorisation in Galois extensions

Theorem 2.5.1 (Galois Connection). *Let L/K be a finite Galois extension with Galois group $G = \text{Gal}(L/K)$. If \mathcal{G}_G is the set of subgroups of G and $\mathcal{F}_{L/K}$ is the set of subfields of L containing K , then we have two reciprocal bijections $\mathcal{G}_G \rightarrow \mathcal{F}_{L/K}$ given by $H \in \mathcal{G}_G \mapsto L^H \in \mathcal{F}_{L/K}$ and $K' \in \mathcal{F}_{L/K} \mapsto \text{Gal}(L/K') \in \mathcal{G}_G$.*

Definition 2.5.2 (Residue field). *Let K be a number field and let \mathfrak{p} be a nonzero prime ideal of \mathcal{O}_K . Then the residue field of \mathfrak{p} is defined by:*

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

Remark 2.5.3. *Let K be a number field and let L/K be a finite Galois extension. Consider a nonzero prime ideal \mathfrak{p} of \mathcal{O}_K .*

- (i) *We can factorise $\mathfrak{p}\mathcal{O}_L = \prod_{i=1}^r \mathfrak{P}_i^{e_i}$ in \mathcal{O}_L .*
- (ii) *If \mathfrak{P} is a prime ideal of \mathcal{O}_L with $\mathfrak{P} \mid \mathfrak{p}\mathcal{O}_L$, then $\kappa(\mathfrak{P}) = \mathcal{O}_L/\mathfrak{P}$ is a finite extension of $\kappa(\mathfrak{p}) = \mathcal{O}_K/\mathfrak{p}$.*
- (iii) *$\text{Gal}(L/K)$ acts on the set $\{\mathfrak{P} \text{ prime ideal of } \mathcal{O}_L, \mathfrak{P} \mid \mathfrak{p}\mathcal{O}_L\}$. Indeed, if $\mathfrak{P} \mid \mathfrak{p}\mathcal{O}_L$ and $g \in \text{Gal}(L/K)$, then $g(\mathfrak{p}\mathcal{O}_L) = \mathfrak{p}\mathcal{O}_L$ and therefore $g(\mathfrak{P})$ is a prime ideal of \mathcal{O}_L with $g(\mathfrak{P}) \mid \mathfrak{p}\mathcal{O}_L$.*

Proposition 2.5.4. *Let K be a number field and let L/K be a finite Galois extension. Consider a nonzero prime ideal \mathfrak{p} of \mathcal{O}_K .*

- (i) *$\text{Gal}(L/K)$ acts transitively on $\{\mathfrak{P} \text{ prime ideal of } \mathcal{O}_L, \mathfrak{P} \mid \mathfrak{p}\mathcal{O}_L\}$.*

- (ii) The integer $e(\mathfrak{P}/\mathfrak{p})$ (resp. $f(\mathfrak{P}/\mathfrak{p})$) does not depend on \mathfrak{P} and will be denoted by e (resp. f). Moreover, if g is the number of prime factors of $\mathfrak{p}\mathcal{O}_L$, then:

$$[L : K] = efg.$$

Thus $\mathfrak{p}\mathcal{O}_L = \prod_{i=1}^g \mathfrak{P}_i^e$, and $\dim_{\kappa(\mathfrak{p})} \kappa(\mathfrak{P}_i) = f$.

Proof. It suffices to prove (i). Let $\mathfrak{P}_1, \dots, \mathfrak{P}_g$ be the distinct prime factors of $\mathfrak{p}\mathcal{O}_L$. By the Chinese Remainder Theorem, there exists $x \in \mathfrak{P}_1 \setminus (\mathfrak{P}_2 \cup \dots \cup \mathfrak{P}_g)$. Now, consider $y = \prod_{\sigma \in \text{Gal}(L/K)} \sigma(x) \in \mathcal{O}_L^G = \mathcal{O}_K$, with $G = \text{Gal}(L/K)$. We have $y = x \prod_{\sigma \neq \text{id}} \sigma(x) \in \mathfrak{P}_1$, so $y \in \mathfrak{P}_1 \cap \mathcal{O}_K = \mathfrak{p}$. Thus, if $1 \leq i \leq g$, then $y = \prod_{\sigma \in \text{Gal}(L/K)} \sigma(x) \in \mathfrak{p} \subseteq \mathfrak{P}_i$, so there exists $\sigma \in \text{Gal}(L/K)$ s.t. $\sigma(x) \in \mathfrak{P}_i$ (by primality). But $\sigma(x) \in \sigma(\mathfrak{P}_1) \setminus (\sigma(\mathfrak{P}_2) \cup \dots \cup \sigma(\mathfrak{P}_g))$, which shows that $\mathfrak{P}_i = \sigma(\mathfrak{P}_1)$. \square

Definition 2.5.5 (Decomposition group and inertia group). Let K be a number field and let L/K be a finite Galois extension. Consider a nonzero prime ideal \mathfrak{p} of \mathcal{O}_K .

- (i) If $\mathfrak{P} \mid \mathfrak{p}\mathcal{O}_L$, define the decomposition group of \mathfrak{P} by:

$$D(\mathfrak{P}/\mathfrak{p}) = \text{Stab}_{\text{Gal}(L/K)}(\mathfrak{P}) = \{\sigma \in \text{Gal}(L/K), \sigma(\mathfrak{P}) = \mathfrak{P}\}.$$

- (ii) Each automorphism $\sigma \in D(\mathfrak{P}/\mathfrak{p})$ induces an automorphism of $\mathcal{O}_L/\mathfrak{P}$ which fixes $\kappa(\mathfrak{p})$. This defines a group homomorphism $\varphi_{\mathfrak{P}} : D(\mathfrak{P}/\mathfrak{p}) \rightarrow \text{Gal}(\kappa(\mathfrak{P})/\kappa(\mathfrak{p}))$. Now, the inertia group of \mathfrak{P} is defined by:

$$I(\mathfrak{P}/\mathfrak{p}) = \text{Ker } \varphi_{\mathfrak{P}} = \{\sigma \in D(\mathfrak{P}/\mathfrak{p}), \forall x \in \mathcal{O}_L, \sigma(x) \equiv x \pmod{\mathfrak{P}}\}.$$

Proposition 2.5.6. Let K be a number field and let L/K be a finite Galois extension. Consider a nonzero prime ideal \mathfrak{p} of \mathcal{O}_K and a prime ideal $\mathfrak{P} \mid \mathfrak{p}\mathcal{O}_L$. Then:

- (i) The group homomorphism $\varphi_{\mathfrak{P}} : D(\mathfrak{P}/\mathfrak{p}) \rightarrow \text{Gal}(\kappa(\mathfrak{P})/\kappa(\mathfrak{p}))$ is surjective.
(ii) With the notations of Proposition 2.5.4, we have:

$$|D(\mathfrak{P}/\mathfrak{p})| = ef \quad \text{and} \quad |I(\mathfrak{P}/\mathfrak{p})| = e.$$

Proof. (i) Consider a primitive element $a \in \kappa(\mathfrak{P})$, with minimal polynomial $g \in \kappa(\mathfrak{p})[T]$. By the Chinese Remainder Theorem, $\mathcal{O}_L/\mathfrak{p}\mathcal{O}_L$ is isomorphic to a direct sum $\mathcal{O}_L/\mathfrak{P}^e \mathcal{O}_L \oplus \bigoplus_{\mathfrak{Q} \neq \mathfrak{P}} \mathcal{O}_L/\mathfrak{Q}^e \mathcal{O}_L$. Now, choose $\alpha \in \mathcal{O}_L$ which corresponds to $(a, 0, \dots, 0)$ in the direct sum (i.e. \mathfrak{P} is the only prime ideal of \mathcal{O}_L dividing $\mathfrak{p}\mathcal{O}_L$ and not containing α). If $f \in \mathcal{O}_K[T]$ is the minimal polynomial of α over K , then g divides f in $\kappa(\mathfrak{p})[T]$. Now, let $\tau \in \text{Gal}(\kappa(\mathfrak{P})/\kappa(\mathfrak{p}))$. As $\tau(a)$ is a root of g , there is a root β of f in \mathcal{O}_L s.t. $\beta \equiv \tau(\alpha) \pmod{\mathfrak{P}}$. As $\text{Gal}(L/K)$ acts transitively on the roots of f in L , there exists $\sigma \in \text{Gal}(L/K)$ s.t. $\sigma(\alpha) = \beta$. We now see that $\sigma(\mathfrak{P}) = \mathfrak{P}$, i.e. $\sigma \in D(\mathfrak{P}/\mathfrak{p})$, and $\varphi_{\mathfrak{P}}(\sigma) = \tau$.
(ii) Use the fact that $[\kappa(\mathfrak{P}) : \kappa(\mathfrak{p})] = f$. \square

Corollary 2.5.7. Let K be a number field and let L/K be a finite Galois extension. Consider a nonzero prime ideal \mathfrak{p} of \mathcal{O}_K . Assume that $e = 1$, i.e. \mathfrak{p} is unramified in L , and write $\mathfrak{p}\mathcal{O}_L = \mathfrak{P}_1 \cdots \mathfrak{P}_g$. Then, for every $1 \leq i \leq g$, we have:

$$D(\mathfrak{P}_i/\mathfrak{p}) \simeq \text{Gal}(\kappa(\mathfrak{P}_i)/\kappa(\mathfrak{p})) = \langle \text{Frob}_p^{N(\mathfrak{p})} \rangle,$$

with $\mathfrak{p} \mid p$ and where $\text{Frob}_p^{N(\mathfrak{p})} : x \mapsto x^{N(\mathfrak{p})}$. The preimage of $\text{Frob}_p^{N(\mathfrak{p})}$ in $D(\mathfrak{P}_i/\mathfrak{p})$ will be called the Frobenius element of \mathfrak{P}_i and denoted by $(\mathfrak{P}_i, L/K)$.

Remark 2.5.8. Let K be a number field and let L/K be a finite Galois extension. Consider a nonzero prime ideal \mathfrak{p} of \mathcal{O}_K . Assume that $e = 1$. For $\mathfrak{P}_i \mid \mathfrak{p}$ and $\sigma \in \text{Gal}(L/K)$, we can show that $(\sigma(\mathfrak{P}_i), L/K) = \sigma(\mathfrak{P}_i, L/K) \sigma^{-1}$. Hence, \mathfrak{p} defines a conjugacy class in $\text{Gal}(L/K)$. If $\text{Gal}(L/K)$ is abelian, then \mathfrak{p} defines a unique element of $\text{Gal}(L/K)$, called the Frobenius element of \mathfrak{p} and denoted by $(\mathfrak{p}, L/K)$.

Remark 2.5.9. Let K be a number field and let L/K be a finite Galois extension. Let K' be a subfield of L containing K . Consider a prime ideal \mathfrak{p} of \mathcal{O}_K , a prime ideal \mathfrak{P} of \mathcal{O}_L s.t. $\mathfrak{P} \mid \mathfrak{p}\mathcal{O}_L$, and set $\mathfrak{p}' = \mathfrak{P} \cap \mathcal{O}_{K'}$.

- (i) We have $e(\mathfrak{P}/\mathfrak{p}) = e(\mathfrak{P}/\mathfrak{p}') \cdot e(\mathfrak{p}'/\mathfrak{p})$ and likewise for f and g .
- (ii) We have $D(\mathfrak{P}/\mathfrak{p}') = D(\mathfrak{P}/\mathfrak{p}) \cap \text{Gal}(L/K')$ and $I(\mathfrak{P}/\mathfrak{p}') = I(\mathfrak{P}/\mathfrak{p}) \cap \text{Gal}(L/K')$.

Proposition 2.5.10. Let K be a number field and let L/K be a finite Galois extension. Let K' be a subfield of L containing K . Consider a prime ideal \mathfrak{p} of \mathcal{O}_K , a prime ideal \mathfrak{P} of \mathcal{O}_L s.t. $\mathfrak{P} \mid \mathfrak{p}\mathcal{O}_L$, and set $\mathfrak{p}' = \mathfrak{P} \cap \mathcal{O}_{K'}$.

- (i) \mathfrak{p} is unramified in \mathfrak{p}' (i.e. $e(\mathfrak{p}'/\mathfrak{p}) = 1$) iff $I(\mathfrak{P}/\mathfrak{p}) \subseteq \text{Gal}(L/K')$.
- (ii) \mathfrak{p} is totally split in \mathfrak{p}' (i.e. $e(\mathfrak{p}'/\mathfrak{p}) f(\mathfrak{p}'/\mathfrak{p}) = 1$) iff $D(\mathfrak{P}/\mathfrak{p}) \subseteq \text{Gal}(L/K')$.

Corollary 2.5.11. Let F be a number field and let K_1, K_2 be two subfields s.t. $F = K_1 K_2$. Let p be a prime number.

- (i) p is unramified in F iff p is unramified in K_1 and in K_2 .
- (ii) p is totally split in F iff p is totally split in K_1 and in K_2 .

Proposition 2.5.12. Let $n \in \mathbb{N}^*$. Consider the isomorphism:

$$\chi : \text{Gal}(\mathbb{Q}(\mu_n(\mathbb{C}))/\mathbb{Q}) \longrightarrow (\mathbb{Z}/n\mathbb{Z})^\times,$$

given by $\sigma(\zeta_n) = \zeta_n^{\chi(\sigma)}$, where $\zeta_n \in \mu_n(\mathbb{C})$ is fixed. Let p be a prime number; let $a \in \mathbb{N}$ and $m \in \mathbb{N}$ with $p \nmid m$ s.t.

$$n = p^a m.$$

- (i) If $p \mid n$, then p is ramified in $\mathbb{Q}(\mu_n(\mathbb{C}))$, each prime divisor of p has ramification index $e = p^{a-1}(p-1)$ and residue degree f the order of p in $(\mathbb{Z}/m\mathbb{Z})^\times$.
- (ii) If $p \nmid n$, then p is unramified in $\mathbb{Q}(\mu_n(\mathbb{C}))$ and:

$$\chi((p, \mathbb{Q}(\mu_n(\mathbb{C}))/\mathbb{Q})) = p.$$

Moreover, $p\mathcal{O}_{\mathbb{Q}(\mu_n(\mathbb{C}))} = \mathfrak{P}_1 \cdots \mathfrak{P}_g$, with residue degree f the order of p in $(\mathbb{Z}/n\mathbb{Z})^\times$, and with $g = \frac{\varphi(n)}{f}$.

2.6 Quadratic Reciprocity Law

Definition 2.6.1 (Legendre symbol). Let $a \in \mathbb{Z}$, let p be a prime number. We define:

$$\left(\frac{a}{p}\right) = \begin{cases} 0 & \text{if } p \mid a \\ +1 & \text{if } \exists x \in \mathbb{Z}, a \equiv x^2 \pmod{p} \\ -1 & \text{otherwise} \end{cases}$$

This defines a p -periodic map $\left(\frac{\cdot}{p}\right) : \mathbb{Z} \rightarrow \{-1, 0, +1\}$.

Proposition 2.6.2. Let $d \in \mathbb{Z} \setminus \{0, 1\}$ be a square-free integer and let $K = \mathbb{Q}(\sqrt{d})$.

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

$$(ii) D_K = \begin{cases} 4d & \text{if } d \equiv 2, 3 \pmod{4} \\ d & \text{if } d \equiv 1 \pmod{4} \end{cases}.$$

$$(iii) \text{ If } p \text{ is an odd prime number, then } p \text{ is } \begin{cases} \text{ramified in } K & \text{if } \left(\frac{d}{p}\right) = 0 \\ \text{totally split in } K & \text{if } \left(\frac{d}{p}\right) = +1. \\ \text{inert in } K & \text{if } \left(\frac{d}{p}\right) = -1 \end{cases}.$$

Remark 2.6.3. We want to solve the two following problems:

(i) If p is a fixed prime number, what are the integers x s.t. $\left(\frac{x}{p}\right) = 1$?

(ii) If x is a fixed integer, what are the prime numbers p s.t. $\left(\frac{x}{p}\right) = 1$?

Proposition 2.6.4. Let p be an odd prime number.

(i) For $a \in \mathbb{Z}$, $\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod{p}$.

(ii) The map $\left(\frac{\cdot}{p}\right) : \mathbb{F}_p^\times \rightarrow \{\pm 1\}$ is a group homomorphism.

Proof. It suffices to prove (i). To do this, note that the group homomorphism $x \in \mathbb{F}_p^\times \mapsto x^2 \in \mathbb{F}_p^\times$ has kernel $\{\pm 1\}$, so its image $\mathbb{F}_p^{\times,2}$ has cardinal $\frac{p-1}{2}$. Now, consider the group homomorphism $g : x \in \mathbb{F}_p^\times \mapsto x^{\frac{p-1}{2}} \in \mathbb{F}_p^\times$. It is clear that $\text{Im } g \subseteq \{\pm 1\}$ and $\text{Ker } g \supseteq \mathbb{F}_p^{\times,2}$. As g is not trivial, we obtain $\text{Ker } g = \mathbb{F}_p^{\times,2}$, so $g(x) = \left(\frac{x}{p}\right)$ for all $x \in \mathbb{F}_p^\times$. \square

Remark 2.6.5. Let p and q be distinct odd prime numbers. The Galois group $\text{Gal}(\mathbb{Q}(\sqrt{q})/\mathbb{Q})$ is canonically isomorphic to $\{\pm 1\}$ via $\sigma \mapsto \frac{\sigma(\sqrt{q})}{\sqrt{q}}$. Moreover, $p \nmid D_{\mathbb{Q}(\sqrt{q})}$, so p is unramified in $\mathbb{Q}(\sqrt{q})$. Thus, we can consider the Frobenius element $(p, \mathbb{Q}(\sqrt{q})/\mathbb{Q})$, and we have:

$$\frac{(p, \mathbb{Q}(\sqrt{q})/\mathbb{Q})(\sqrt{q})}{\sqrt{q}} = \left(\frac{q}{p}\right).$$

In other words, the above isomorphism sends $(p, \mathbb{Q}(\sqrt{q})/\mathbb{Q})$ to $\left(\frac{q}{p}\right)$.

Theorem 2.6.6 (Quadratic Reciprocity Law, Gauß). Let p and q be two odd prime numbers.

$$(i) \left(\frac{p}{q}\right) \left(\frac{q}{p}\right) = (-1)^{\frac{(p-1)(q-1)}{4}},$$

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

$$(iii) \left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}.$$

Proof. It suffices to prove (i) and to use Proposition 2.6.4. Let $L = \mathbb{Q}(\mu_p(\mathbb{C}))$ and consider the isomorphism $\chi : \text{Gal}(L/\mathbb{Q}) \rightarrow \mathbb{F}_p^\times$ of Proposition 2.5.12. Define $H = \chi^{-1}(\mathbb{F}_p^{\times,2})$; H is the only subgroup of $\text{Gal}(L/\mathbb{Q})$ of order 2, so $K = L^H$ is the only quadratic subextension of L . As p is the only prime that ramifies in L , it is also the only prime that can ramify in K ; therefore D_K is a

power of p . But K/\mathbb{Q} is a quadratic extension, so $D_K = \pm p$. Therefore $D_K = p^* = \left(\frac{-1}{p}\right)p$ and $K = \mathbb{Q}(\sqrt{p^*})$. We now show that $\left(\frac{q}{p}\right) = \left(\frac{p^*}{q}\right)$:

$$\begin{aligned} \left(\frac{q}{p}\right) = 1 &\iff q \in \mathbb{F}_p^{\times,2} \iff \chi((q, \mathbb{Q}(\mu_p(\mathbb{C}))/\mathbb{Q})) \in \mathbb{F}_p^{\times,2} \\ &\iff (q, \mathbb{Q}(\mu_p(\mathbb{C}))/\mathbb{Q}) \in H = \text{Gal}(L/K) \\ &\iff q \text{ is totally split in } K = \mathbb{Q}(\sqrt{p^*}) \\ &\iff T^2 - T + \frac{1-p^*}{4} \text{ is split modulo } q \\ &\iff \left(\frac{p^*}{q}\right) = 1. \end{aligned}$$

□

Remark 2.6.7. If p^* is as in the proof of Theorem 2.6.6, it is possible to give an explicit expression of a square root of p^* . To do this, we define the Gauß sum:

$$g = \sum_{a \in \mathbb{F}_p} \zeta_p^{a^2} = \sum_{a \in \mathbb{F}_p} \left(\frac{a}{p}\right) \zeta_p^a.$$

Hence, we see that $g^2 = p^*$. Using this, we can give an alternative proof of the Quadratic Reciprocity Law. Indeed, we have $\left(\frac{p^*}{q}\right) \equiv (p^*)^{\frac{q-1}{2}} \equiv g^{q-1} \pmod{q\mathbb{Z}[\zeta_p]}$, and $g^q \equiv \sum_{a \in \mathbb{F}_p} \left(\frac{a}{p}\right)^q \zeta_p^{aq} \equiv \left(\frac{q}{p}\right) g \pmod{q\mathbb{Z}[\zeta_p]}$. Hence, we obtain $\left(\frac{p^*}{q}\right) \equiv \left(\frac{q}{p}\right) \pmod{q\mathbb{Z}[\zeta_p]}$ because g is invertible modulo q . Hence, $\left(\frac{p^*}{q}\right) = \left(\frac{q}{p}\right)$ because $2 \notin q\mathbb{Z}[\zeta_p]$.

3 Class group and unit group

3.1 Lattices

Notation 3.1.1. In this section, V is a real finite-dimensional vector space.

Definition 3.1.2 (Lattice). A lattice Λ in V is an additive subgroup of V which is discrete and which generates V as a vector space.

Example 3.1.3.

- (i) \mathbb{Z}^n is a lattice in \mathbb{R}^n . Actually, we shall see that every lattice is isomorphic to this one.
- (ii) $\{(a, b) \in \mathbb{Z}^2, a \equiv 2b \pmod{3}\}$ is a lattice in \mathbb{R}^2 .

Proposition 3.1.4. Let Λ be an additive subgroup of V . The following assertions are equivalent:

- (i) Λ is a lattice in V .
- (ii) Λ is generated by a basis of V .
- (iii) Λ is discrete and cocompact in V (i.e. V/Λ is compact).

Proof. (i) \Rightarrow (ii) If Λ is a lattice, then it generates V , so it contains a basis (e_1, \dots, e_n) of V . Let $\Lambda_0 = \bigoplus_{i=1}^n \mathbb{Z}e_i \subseteq \Lambda$. Then $V = \Lambda_0 + B$, with $B = \sum_{i=1}^n [0, 1]e_i$, a compact set. Therefore, $\Lambda = \Lambda_0 + (B \cap \Lambda)$. As $B \cap \Lambda$ is finite, we deduce that Λ/Λ_0 is finite. Hence, if $m = (\Lambda : \Lambda_0)$, then $\Lambda_0 \subseteq \Lambda \subseteq \frac{1}{m}\Lambda_0$, so Λ is a free abelian group of rank n . Moreover, there exists a basis $(\varepsilon_1, \dots, \varepsilon_n)$ of Λ_0 and $d_1, \dots, d_n \in \mathbb{N}^*$ s.t. $\left(\frac{d_1}{m}\varepsilon_1, \dots, \frac{d_n}{m}\varepsilon_n\right)$ is a \mathbb{Z} -basis of Λ , and it is clearly a \mathbb{R} -basis of V . (ii) \Rightarrow (iii) Note that, if \mathcal{B} is a basis of V that generates Λ , then the isomorphisms $\mathbb{Z}^n \rightarrow \Lambda$ and $\mathbb{R}^n \rightarrow V$ induced by \mathcal{B} give a commutative diagram of topological abelian groups:

$$\begin{array}{ccc} \mathbb{Z}^n & \xrightarrow{\subseteq} & \mathbb{R}^n \\ \simeq \downarrow & & \simeq \downarrow \\ \Lambda & \xrightarrow{\subseteq} & V \end{array}$$

As a consequence, $V/\Lambda \simeq \mathbb{R}^n/\mathbb{Z}^n$ is compact. (iii) \Rightarrow (i) Assume that Λ is discrete and cocompact in V . Let $W = \text{Vect}(\Lambda) \subseteq V$. Then we have an exact sequence of topological abelian groups:

$$0 \longrightarrow W/\Lambda \longrightarrow V/\Lambda \longrightarrow V/W \longrightarrow 0.$$

Therefore, V/W is a compact vector space, so $V/W = 0$, i.e. $V = W$. \square

Notation 3.1.5. We now assume that V is equipped with a scalar product $\langle \cdot, \cdot \rangle$.

Definition 3.1.6 (Volume). There exists a unique translation-invariant measure μ on V s.t.

$$\mu \left(\sum_{i=1}^n [0, 1] \varepsilon_i \right) = 1,$$

for any unitary (i.e. orthonormal) basis $(\varepsilon_1, \dots, \varepsilon_n)$ of V . This measure will be denoted by Vol .

Definition 3.1.7 (Covolume of a lattice). If Λ is a lattice in V , then the covolume of Λ is defined by:

$$\text{Covol}(\Lambda) = \text{Vol} \left(\sum_{i=1}^n [0, 1] e_i \right),$$

for any \mathbb{Z} -basis (e_1, \dots, e_n) of Λ . This does not depend on the choice of the \mathbb{Z} -basis: if (e'_1, \dots, e'_n) is another \mathbb{Z} -basis, then the matrix of change of basis is $A \in GL_n(\mathbb{Z})$, so that $|\det A| = 1$.

Lemma 3.1.8. If Λ is a lattice in V , then:

$$\text{Covol}(\Lambda) = \left| \det_{(\varepsilon_1, \dots, \varepsilon_n)} (e_1, \dots, e_n) \right|,$$

where $(\varepsilon_1, \dots, \varepsilon_n)$ is a unitary basis of V and (e_1, \dots, e_n) is a \mathbb{Z} -basis of Λ .

Proposition 3.1.9. Let Λ be a lattice in V and let Λ' be a subgroup of Λ . Then Λ' is a lattice in V iff $(\Lambda : \Lambda') < +\infty$. In this case, we have:

$$\text{Covol}(\Lambda') = (\Lambda : \Lambda') \cdot \text{Covol}(\Lambda).$$

Proof. Note that Λ' is discrete and that we have an exact sequence of topological abelian groups:

$$0 \longrightarrow \Lambda/\Lambda' \longrightarrow V/\Lambda' \longrightarrow V/\Lambda \longrightarrow 0.$$

From this, we obtain that V/Λ' is compact iff Λ/Λ' is finite. Now, assume that $(\Lambda : \Lambda') < +\infty$. Then there exists a \mathbb{Z} -basis (e_1, \dots, e_n) of Λ and $d_1, \dots, d_n \in \mathbb{N}^*$ s.t. $(d_1 e_1, \dots, d_n e_n)$ is a \mathbb{Z} -basis of Λ' . Thus:

$$\text{Covol}(\Lambda') = \left| \det_{(\varepsilon_1, \dots, \varepsilon_n)} (d_1 e_1, \dots, d_n e_n) \right| = d_1 \cdots d_n \left| \det_{(\varepsilon_1, \dots, \varepsilon_n)} (e_1, \dots, e_n) \right|,$$

and $d_1 \cdots d_n = (\Lambda : \Lambda')$. \square

Theorem 3.1.10 (Minkowski). Let Λ be a lattice in V . Let C be a nonempty subset of V that is bounded, convex and symmetric. If $\text{Vol}(C) > 2^n \text{Covol}(\Lambda)$, then $C \cap \Lambda \setminus \{0\} \neq \emptyset$. Moreover, if C is closed, it suffices to assume that $\text{Vol}(C) \geq 2^n \text{Covol}(\Lambda)$.

Proof. Consider $\Lambda' = 2\Lambda$. Then Λ' is a lattice and $\text{Covol}(\Lambda') = 2^n \text{Covol}(\Lambda)$. Pick a \mathbb{Z} -basis (e_1, \dots, e_n) of Λ' and let $\Pi = \sum_{i=1}^n [0, 1]e_i$. We have $V = \bigcup_{\lambda \in \Lambda'} (\lambda + \Pi)$, therefore:

$$C = \bigcup_{\lambda \in \Lambda'} (C \cap (\lambda + \Pi)) = \bigcup_{\lambda \in \Lambda'} (\lambda + (\Pi \cap (C - \lambda))).$$

Now, $\text{Vol}(C) > 2^n \text{Covol}(\Lambda) = \text{Covol}(\Lambda') = \text{Vol}(\Pi)$, therefore:

$$\text{Vol}(\Pi) < \text{Vol}(C) \leq \sum_{\lambda \in \Lambda'} \text{Vol}(\Pi \cap (C - \lambda)).$$

Therefore, the subsets $(\Pi \cap (C - \lambda))_{\lambda \in \Lambda'}$ must have a nonempty intersection (for otherwise we would have $\sum_{\lambda \in \Lambda'} \text{Vol}(\Pi \cap (C - \lambda)) = \text{Vol}(\Pi)$). Hence, there exist $\lambda \neq \mu$ in Λ' and $u, v \in C$ s.t. $u - \lambda = v - \mu$. Thus, $\frac{1}{2}(\mu - \lambda) = \frac{1}{2}(v - u) \in C \cap \frac{1}{2}\Lambda' = C \cap \Lambda$, and $\frac{1}{2}(\mu - \lambda) \neq 0$. \square

3.2 Finiteness of the class group

Notation 3.2.1. Let K be a number field. Then we have an isomorphism $K \otimes_{\mathbb{Q}} \mathbb{R} \simeq \mathbb{R}^{\Sigma_r} \oplus \mathbb{C}^{\Sigma'_c}$, which induces an embedding $K \rightarrow \mathbb{R}^{\Sigma_r} \oplus \mathbb{C}^{\Sigma'_c}$. This embedding will be denoted by Φ and is given by:

$$\forall x \in K, \Phi(x) = (\sigma(x))_{\sigma \in \Sigma_r \cup \Sigma'_c}.$$

Proposition 3.2.2. Let K be a number field. Then $\Phi(\mathcal{O}_K)$ is a lattice in $\mathbb{R}^{\Sigma_r} \oplus \mathbb{C}^{\Sigma'_c}$, and:

$$\text{Covol}(\Phi(\mathcal{O}_K)) = 2^{-r_2} |D_K|^{\frac{1}{2}},$$

where $\mathbb{R}^{\Sigma_r} \oplus \mathbb{C}^{\Sigma'_c}$ is equipped with the standard scalar product.

Proof. Write the matrix of $\Phi(\mathcal{O}_K)$ in the canonical basis of $\mathbb{R}^{\Sigma_r} \oplus \mathbb{C}^{\Sigma'_c}$, and use Proposition 1.3.6. \square

Corollary 3.2.3. Let K be a number field. If \mathfrak{a} is a fractional ideal of K , then $\Phi(\mathfrak{a})$ is a lattice in $\mathbb{R}^{\Sigma_r} \oplus \mathbb{C}^{\Sigma'_c}$, of covolume $2^{-r_2} |D_K|^{\frac{1}{2}} N(\mathfrak{a})$.

Remark 3.2.4. If we replace $\mathbb{R}^{\Sigma_r} \oplus \mathbb{C}^{\Sigma'_c}$ by the subspace $(\mathbb{R}^{\Sigma_r} \oplus \mathbb{C}^{\Sigma_c})^{\text{inv}}$ of $\mathbb{R}^{\Sigma_r} \oplus \mathbb{C}^{\Sigma_c}$ composed of the points that are invariant by complex conjugation, equipped with the scalar product induced by that of $\mathbb{R}^{\Sigma_r} \oplus \mathbb{C}^{\Sigma_c}$, then $\text{Covol}(\Phi(\mathcal{O}_K)) = |D_K|^{\frac{1}{2}}$.

Lemma 3.2.5. If $r_1, r_2 \in \mathbb{N}$, $R \in \mathbb{R}_+$, we define:

$$C(r_1, r_2, R) = \left\{ (x_1, \dots, x_{r_1}, z_1, \dots, z_{r_2}) \in \mathbb{R}^{r_1} \oplus \mathbb{C}^{r_2}, \sum_{i=1}^{r_1} |x_i| + 2 \sum_{j=1}^{r_2} |z_j| \leq R \right\} \subseteq \mathbb{R}^{r_1} \oplus \mathbb{C}^{r_2}.$$

Then $\text{Vol}(C(r_1, r_2, R)) = 2^{r_1} \left(\frac{\pi}{2}\right)^{r_2} \frac{R^n}{n!}$.

Theorem 3.2.6 (Minkowski). Let K be a number field of degree n and let \mathfrak{a} be a fractional ideal of K . Then there exists $a \in \mathfrak{a} \setminus \{0\}$ s.t.

$$|N(a)| \leq \underbrace{\left(\frac{n!}{n^n} \left(\frac{4}{\pi}\right)^{r_2} |D_K|^{\frac{1}{2}} \right)}_{M_K} N(\mathfrak{a}).$$

The number M_K will be called the Minkowski constant of K .

Proof. By Corollary 3.2.3, $\Phi(\mathfrak{a})$ is a lattice of covolume $2^{-r_2} |D_K|^{\frac{1}{2}} N(\mathfrak{a})$. Therefore, for $R \in \mathbb{R}_+$:

$$\frac{\text{Vol}(C(r_1, r_2, R))}{2^n \text{Covol}(\Phi(\mathfrak{a}))} = \frac{R^n}{n!} \left(\frac{\pi}{4}\right)^{r_2} |D_K|^{-\frac{1}{2}} N(\mathfrak{a})^{-1} = \frac{R^n}{n^n} \cdot M_K^{-1} N(\mathfrak{a})^{-1}.$$

Moreover, if $x \in K$ is s.t. $\Phi(x) \in C(r_1, r_2, R)$, then, using the inequality of arithmetic and geometric means:

$$\begin{aligned} |N(x)| &= |\sigma_1(x)| \cdots |\sigma_{r_1}(x)| \cdot |\tau_1(x)|^2 \cdots |\tau_{r_2}(x)|^2 \\ &\leq \frac{1}{n^n} (|\sigma_1(x)| + \cdots + |\sigma_{r_1}(x)| + 2|\tau_1(x)| + \cdots + 2|\tau_{r_2}(x)|)^n \leq \frac{R^n}{n^n}, \end{aligned}$$

with $\Sigma_r = \{\sigma_1, \dots, \sigma_{r_1}\}$ and $\Sigma'_c = \{\tau_1, \dots, \tau_{r_2}\}$. By Theorem 3.1.10, if R is chosen s.t. $\frac{R^n}{n^n} = M_K N(\mathfrak{a})$, then there exists $a \in \mathfrak{a} \cap \Phi^{-1}(C(r_1, r_2, R)) \setminus \{0\}$, and we have $|N(a)| \leq \frac{R^n}{n^n} = M_K N(\mathfrak{a})$. \square

Corollary 3.2.7. *Let K be a number field of degree n .*

- (i) *Each ideal class in $\text{Cl}(\mathcal{O}_K)$ contains an ideal $\mathfrak{a} \subseteq \mathcal{O}_K$ with $N(\mathfrak{a}) \leq M_K$.*
- (ii) *The group $\text{Cl}(\mathcal{O}_K)$ is finite and generated by prime ideals with norm $\leq M_K$.*
- (iii) *We have the inequality:*

$$|D_K| \geq \left(\frac{n^n}{n!} \left(\frac{\pi}{4}\right)^{r_2}\right)^2 \geq \frac{\pi^n}{4}.$$

In particular, $|D_K| > 1$ if $K \neq \mathbb{Q}$.

Proof. (i) Let $C \in \text{Cl}(\mathcal{O}_K)$. Let \mathfrak{a} be a fractional ideal in C^{-1} . We may assume that $\mathfrak{a} \subseteq \mathcal{O}_K$ by multiplying \mathfrak{a} by some $d \in \mathbb{N}$. Now, by Theorem 3.2.6, there exists $a \in \mathfrak{a} \setminus \{0\}$ with $|N(a)| \leq M_K N(\mathfrak{a})$. As $a\mathcal{O}_K \subseteq \mathfrak{a}$, we have $a\mathfrak{a}^{-1} \subseteq \mathcal{O}_K$, so that:

$$N(a\mathfrak{a}^{-1}) = |N(a)| \cdot N(\mathfrak{a})^{-1} \leq M_K,$$

and $a\mathfrak{a}^{-1} \in C$. (ii) By Proposition 2.4.6, the set of ideals with norm bounded by M_K is finite, so $\text{Cl}(\mathcal{O}_K)$ is finite. Now, write $\text{Cl}(\mathcal{O}_K) = \{\bar{\mathfrak{a}}_1, \dots, \bar{\mathfrak{a}}_N\}$, with $\mathfrak{a}_i \subseteq \mathcal{O}_K$, $N(\mathfrak{a}_i) \leq M_K$. For $i \in \{1, \dots, N\}$, we can write \mathfrak{a}_i as a product of prime ideals $\mathfrak{p}_j^{(i)}$ with $N(\mathfrak{p}_j^{(i)}) \leq N(\mathfrak{a}_i) \leq M_K$, so that $\text{Cl}(\mathcal{O}_K) = \left\langle \left(\bar{\mathfrak{p}}_j^{(i)}\right)_{i,j} \right\rangle$. (iii) Apply Theorem 3.2.6 with $\mathfrak{a} = \mathcal{O}_K$: there exists $x \in \mathcal{O}_K \setminus \{0\}$ s.t. $|N(x)| \leq M_K$. But $|N(x)| \in \mathbb{N}^*$, so $M_K \geq 1$, which gives the first inequality. For the second one, note that $n^n \geq 2^{n-1}n!$ and therefore $\frac{n^n}{n!} \left(\frac{\pi}{4}\right)^{r_2} \geq 2^{n-1} \left(\frac{\pi}{4}\right)^{r_2} \geq 2^{n-1} \left(\frac{\pi}{4}\right)^{\frac{n}{2}} = \left(\frac{\pi^n}{4}\right)^{\frac{1}{2}}$. \square

Remark 3.2.8. *By Theorem 2.4.12 and Corollary 3.2.7, \mathbb{Q} is the only number field in which no prime number ramifies.*

Corollary 3.2.9. *If K is a number field with $M_K < 2$, then $\text{Cl}(\mathcal{O}_K)$ is trivial.*

Example 3.2.10. *Let $K = \mathbb{Q}(\sqrt{5})$. Then $D_K = -20$, so $M_K = \frac{\pi}{2}\sqrt{5} < 3$. By Corollary 3.2.7, $\text{Cl}(\mathcal{O}_K)$ is generated by prime ideals with norm ≤ 2 ; these prime ideals are therefore divisors of $2\mathcal{O}_K$. Using Proposition 2.4.7, we see that $2\mathcal{O}_K = \mathfrak{p}_2^2$, where $\mathfrak{p}_2 = (2, 1 + \sqrt{-5})$ is prime. Therefore, $\text{Cl}(\mathcal{O}_K) = \langle \bar{\mathfrak{p}}_2 \rangle$, and $\bar{\mathfrak{p}}_2^2 = 1$. Now, \mathfrak{p}_2 is not principal, for otherwise there would exist $x, y \in \mathbb{Z}^2$ s.t. $2 = N(\mathfrak{p}_2) = |N_{K/\mathbb{Q}}(x + y\sqrt{-5})| = x^2 + 5y^2$, which is impossible. As a consequence, $\bar{\mathfrak{p}}_2 \neq 1$, which shows that:*

$$\text{Cl}(\mathcal{O}_K) \simeq \mathbb{Z}/2\mathbb{Z}.$$

This method allows one to compute $\text{Cl}(\mathcal{O}_K)$ for many number fields.

3.3 Binary quadratic forms and class groups

Definition 3.3.1 (Binary quadratic form). A binary quadratic form is a map $q : \mathbb{Z}^2 \rightarrow \mathbb{Z}$ of the form $q(x, y) = ax^2 + bxy + cy^2$ for some $(a, b, c) \in \mathbb{Z}^3$. The integers a, b, c are determined by q and we shall sometimes make the identification $q = (a, b, c)$. The discriminant of q is defined by:

$$\text{disc}(q) = b^2 - 4ac.$$

We have a natural action of $GL_2(\mathbb{Z})$ on the set of binary quadratic forms given by:

$$(q \cdot A)(x, y) = q((x, y)^t A).$$

We say that two binary quadratic forms q and q' are equivalent, and we write $q \sim q'$, if q and q' are in the same orbit under the action of $GL_2(\mathbb{Z})$; we say that q and q' are properly equivalent, and we write $q \overset{+}{\sim} q'$, if q and q' are in the same orbit under the action of $SL_2(\mathbb{Z})$.

Lemma 3.3.2. $SL_2(\mathbb{Z}) = \langle S, T \rangle$, with $S = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ and $T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$.

Remark 3.3.3. If $q = (a, b, c)$ is a binary quadratic form, then:

$$(a, b, c) \cdot S = (c, -b, a) \quad \text{and} \quad (a, b, c) \cdot T = (a, b + 2a, c + b + a),$$

with the notations of Lemma 3.3.2. These are called elementary equivalences; they generate the equivalence relation $\overset{+}{\sim}$.

Proposition 3.3.4. If q and q' are two equivalent binary quadratic forms, then $\text{disc}(q) = \text{disc}(q')$.

Vocabulary 3.3.5. We say that a binary quadratic form q represents (resp. primitively represents) an integer n if there exists $(x, y) \in \mathbb{Z}^2$ s.t. $n = q(x, y)$ (resp. $n = q(x, y)$ and $\gcd(x, y) = 1$). Note that, if q and q' are two equivalent binary quadratic forms, then they represent the same integers, and the same number of times.

Definition 3.3.6 (Fundamental discriminant). A fundamental discriminant is an integer $D \in \mathbb{Z}$ which satisfies one of the following two properties:

- Either D is square-free and $D \equiv 1 \pmod{4}$,
- Or $D \equiv 0 \pmod{4}$, $\frac{D}{4}$ is square-free and $\frac{D}{4} \not\equiv 1 \pmod{4}$.

In other words, a fundamental discriminant is the discriminant of a quadratic number field (c.f. Example 1.4.5). Given a fundamental discriminant D , we define:

$$\mathcal{F}^+(D) = \{q \text{ binary quadratic form, } \text{disc}(q) = D \text{ and } q > 0\}.$$

Remark 3.3.7. Let $D < 0$ be a fundamental discriminant. Consider $K = \mathbb{Q}(\sqrt{D})$, and assume that $\Im(\sqrt{D}) > 0$ (this amounts to choosing an orientation of K). Let $\alpha_K = \frac{\sqrt{D}}{2}$ if $D \equiv 0 \pmod{4}$, or $\alpha_K = \frac{1+\sqrt{D}}{2}$ if $D \equiv 1 \pmod{4}$. Then $\mathcal{O}_K = \mathbb{Z}[\alpha_K]$. Now, if $q = (a, b, c) \in \mathcal{F}^+(D)$, then:

$$q(x, y) = a(x - \tau(q)y)(x - \overline{\tau(q)}y),$$

with $\tau(q) = \frac{-b+\sqrt{D}}{2}$. Thus, if $\mathfrak{h} = \{z \in \mathbb{C}, \Im(z) > 0\}$, then we have a map:

$$\tau : \mathcal{F}^+(D) \rightarrow \mathfrak{h}.$$

Proposition 3.3.8. Consider the action of $SL_2(\mathbb{Z})$ on $\mathfrak{h} = \{z \in \mathbb{C}, \Im(z) > 0\}$ given by:

$$\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} z = \frac{\alpha z + \beta}{\gamma z + \delta}.$$

- (i) With the notations of Lemma 3.3.2, we have $S \cdot z = -\frac{1}{z}$ and $T \cdot z = z + 1$.
- (ii) Choose a fundamental discriminant $D < 0$. If $\tau : \mathcal{F}^+(D) \rightarrow \mathfrak{h}$ is the map of Remark 3.3.7, then for $q \in \mathcal{F}^+(D)$ and $A \in SL_2(\mathbb{Z})$:

$$\tau(q \cdot A) = A^{-1} \cdot \tau(q).$$

Lemma 3.3.9. Choose a fundamental discriminant $D < 0$. If $q = (a, b, c) \in \mathcal{F}^+(D)$, then the subgroup $\mathfrak{a} = \mathbb{Z}a + \mathbb{Z}a\tau(q)$ of $K = \mathbb{Q}(\sqrt{D})$ is an ideal of \mathcal{O}_K of norm a , and:

$$q(x, y) = \frac{1}{a} N_{K/\mathbb{Q}}(ax - a\tau(q)y).$$

Proof. We start by showing that $a\tau(q) \in \mathbb{Z} + \alpha_K$. Using this, we show that $a\alpha_K \in \mathfrak{a}$ and $a\tau(q)\alpha_K \in \mathfrak{a}$, so \mathfrak{a} is an ideal of \mathcal{O}_K . Moreover, its norm is given by:

$$N(\mathfrak{a}) = (\mathcal{O}_K : \mathfrak{a}) = \left| \det \text{Mat}_{(1, \alpha_K)}(a, a\tau(q)) \right| = \left| \det \begin{pmatrix} a & * \\ 0 & 1 \end{pmatrix} \right| = a.$$

Finally $q(x, y) = a(x - \tau(q)y)(x - \overline{\tau(q)}y) = \frac{1}{a} N_{K/\mathbb{Q}}(ax - a\tau(q)y)$. \square

Proposition 3.3.10. Choose a fundamental discriminant $D < 0$. Let $K = \mathbb{Q}(\sqrt{D})$. By Lemma 3.3.9, we have a map:

$$\Phi : \begin{cases} \mathcal{F}^+(D) \longrightarrow I(K) \\ q \longmapsto \mathbb{Z}a + \mathbb{Z}a\tau(q) \end{cases}.$$

Composing Φ with the natural projection $I(K) \rightarrow \text{Cl}(\mathcal{O}_K)$, we obtain a map:

$$\tilde{\varphi} : \mathcal{F}^+(D) \longrightarrow \text{Cl}(\mathcal{O}_K).$$

Then $\tilde{\varphi}$ is invariant under the action of $SL_2(\mathbb{Z})$: $\tilde{\varphi}(q \cdot A) = \tilde{\varphi}(q)$ for all $A \in SL_2(\mathbb{Z})$.

Proof. By Lemma 3.3.2, it suffices to prove that $\tilde{\varphi}(q \cdot S) = \tilde{\varphi}(q \cdot T) = \tilde{\varphi}(q)$. \square

Theorem 3.3.11. Choose a fundamental discriminant $D < 0$. Let $K = \mathbb{Q}(\sqrt{D})$. Then the map $\tilde{\varphi} : \mathcal{F}^+(D) \rightarrow \text{Cl}(\mathcal{O}_K)$ of Proposition 3.3.10 induces a map:

$$\varphi : \mathcal{F}^+(D)/SL_2(\mathbb{Z}) \longrightarrow \text{Cl}(\mathcal{O}_K),$$

and this map is a bijection.

Proof. We shall construct the inverse of φ . Let $\mathfrak{a} \subseteq K$ be a fractional ideal; write $\mathfrak{a} = \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2$, with $\det_{(1, \alpha_K)}(\omega_1, \omega_2) > 0$. We may assume that $\mathfrak{a} \subseteq \mathcal{O}_K$. Consider:

$$q_{\omega_1, \omega_2}(x, y) = \frac{1}{N(\mathfrak{a})} N_{K/\mathbb{Q}}(x\omega_1 - y\omega_2).$$

This defines a binary quadratic form. We compute $\text{disc}(q_{\omega_1, \omega_2}) = D$. Note that the image of q_{ω_1, ω_2} in $\mathcal{F}^+(D)/SL_2(\mathbb{Z})$ does not depend on the choice of the oriented basis (ω_1, ω_2) of \mathfrak{a} . Thus, we have a map $I(K) \longrightarrow \mathcal{F}^+(D)/SL_2(\mathbb{Z})$. Moreover, for $z \in K$ with $N_{K/\mathbb{Q}}(z) > 0$, we see that $q_{z\omega_1, z\omega_2} = q_{\omega_1, \omega_2}$. This implies that the map $I(K) \longrightarrow \mathcal{F}^+(D)/SL_2(\mathbb{Z})$ induces a map $\text{Cl}(\mathcal{O}_K) \longrightarrow \mathcal{F}^+(D)/SL_2(\mathbb{Z})$, which is an inverse of φ . \square

3.4 Reduced forms

Definition 3.4.1 (Reduced form). A binary quadratic form $q = (a, b, c)$ is said to be reduced if $|b| \leq a \leq c$ and if $b \geq 0$ as soon as one of the two inequalities is an equality.

Remark 3.4.2. Choose a fundamental discriminant $D < 0$. Consider the map $\tau : \mathcal{F}^+(D) \rightarrow \mathfrak{h}$ of Remark 3.3.7. Then, for $q \in \mathcal{F}^+(D)$, we have that q is reduced iff $\tau(q) \in \mathcal{D}$, where:

$$\mathcal{D} = \left\{ z \in \mathfrak{h}, -\frac{1}{2} \leq \Re(z) < \frac{1}{2} \text{ and } |z| > 1 \right\} \cup \left\{ z \in \mathfrak{h}, |z| = 1 \text{ and } -\frac{1}{2} \leq \Re(z) \leq 0 \right\}.$$

Note that \mathcal{D} is a fundamental domain for the action of $SL_2(\mathbb{Z})$ on \mathfrak{h} .

Proposition 3.4.3 (Gauß). Choose a fundamental discriminant $D < 0$. Let $K = \mathbb{Q}(\sqrt{D})$.

(i) Every proper equivalence class in $\mathcal{F}^+(D)$ contains a unique reduced form.

(ii) The set of reduced forms in $\mathcal{F}^+(D)$ is finite and reduced forms (a, b, c) satisfy $|b| \leq a \leq \sqrt{\frac{|D|}{3}}$.

(iii) The class number $h_K = |\text{Cl}(\mathcal{O}_K)|$ is the number of reduced forms in $\mathcal{F}^+(D)$.

Example 3.4.4. Let $D = -20$, $K = \mathbb{Q}(\sqrt{-20}) = \mathbb{Q}(\sqrt{-5})$. Let us find the reduced forms of discriminant -20 . Let $(a, b, c) \in \mathbb{Z}^3$ s.t. $b^2 - 4ac = -20$, with $|b| \leq a \leq \sqrt{\frac{20}{3}} < 3$. Thus, $a \in \{1, 2\}$. If $a = 1$, we obtain $q_1 = (1, 0, 5)$; if $a = 2$, we obtain $q_2 = (2, 2, 3)$. Thus:

$$h_{\mathbb{Q}(\sqrt{-5})} = 2.$$

In general, this method is very efficient for computing the class number of a number field.

3.5 Unit group

Definition 3.5.1 (Unit group). Let K be a number field. The unit group of \mathcal{O}_K is by definition its group \mathcal{O}_K^\times of invertible elements. We have:

$$\mathcal{O}_K^\times = \left\{ x \in \mathcal{O}_K, N_{K/\mathbb{Q}}(x) \in \{\pm 1\} \right\}.$$

Lemma 3.5.2. If K is a number field and $m \geq 1$, then the set $\left\{ a \in \mathcal{O}_K, |N_{K/\mathbb{Q}}(a)| = m \right\}$ is a finite union of cosets of \mathcal{O}_K^\times .

Proof. If $a \in \mathcal{O}_K$ with $|N_{K/\mathbb{Q}}(a)| = m$ then $|\mathcal{O}_K/a\mathcal{O}_K| = m$ and $m\mathcal{O}_K \subseteq a\mathcal{O}_K$, hence $a\mathcal{O}_K$ belongs to the set of principal divisors of $m\mathcal{O}_K$, which is finite. If $a_1, \dots, a_s \in \mathcal{O}_K$ represent these principal ideals, then each $a \in \mathcal{O}_K$ with $|N_{K/\mathbb{Q}}(a)| = m$ can be written as $a = \varepsilon a_i$ for some $\varepsilon \in \mathcal{O}_K^\times$ and $i \in \{1, \dots, s\}$. Therefore $\left\{ a \in \mathcal{O}_K, |N_{K/\mathbb{Q}}(a)| = m \right\} = \bigcup_{i=1}^s a_i \mathcal{O}_K^\times$. \square

Lemma 3.5.3. Let K be a number field. Consider the subgroup:

$$G = \left\{ (x, z) \in \mathbb{R}^{\Sigma_r} \oplus \mathbb{C}^{\Sigma_c}, |x_1| \cdots |x_{r_1}| \cdot |z_1|^2 \cdots |z_{r_2}|^2 = 1 \right\},$$

of $(\mathbb{R}^\times)^{\Sigma_r} \times (\mathbb{C}^\times)^{\Sigma_c}$. Then the quotient $G/\Phi(\mathcal{O}_K^\times)$ is compact and Hausdorff, where $\Phi : K \rightarrow \mathbb{R}^{\Sigma_r} \oplus \mathbb{C}^{\Sigma_c}$ is the natural embedding (c.f. Notation 3.2.1).

Proof. Write $V = \mathbb{R}^{\Sigma_r} \oplus \mathbb{C}^{\Sigma_c}$. Let $C \subseteq V$ be a bounded convex symmetric subset with volume $\text{Vol}(C) > 2^n \text{Covol}(\Phi(\mathcal{O}_K))$, where $n = [K : \mathbb{Q}]$. For $g \in G$, the set $g^{-1}C$ is bounded convex symmetric and $\text{Vol}(g^{-1}C) = \text{Vol}(C)$ since g^{-1} induces an isomorphism $V \rightarrow V$ with determinant ± 1 . Consider the following map:

$$N : (x, z) \in V \mapsto |x_1| \cdots |x_{r_1}| \cdot |z_1|^2 \cdots |z_{r_2}|^2 \in \mathbb{R}.$$

Then $N(g^{-1}C) = N(g^{-1})N(C) = N(C)$. By Minkowski's Theorem (Theorem 3.1.10), $g^{-1}C$ contains a nonzero element $a \in \Phi(\mathcal{O}_K)$. As $a \in g^{-1}C$, we have $|N_{K/\mathbb{Q}}(a)| \in N(C)$, and $N(C)$ is finite. By Lemma 3.5.2, there exist $a_1, \dots, a_s \in \mathcal{O}_K$ s.t.

$$\emptyset \subsetneq g^{-1}C \cap \Phi(\mathcal{O}_K) \setminus \{0\} \subseteq g^{-1}C \cap \bigcup_{i=1}^s \Phi(a_i \mathcal{O}_K^\times).$$

This shows that $g \in \Phi(\mathcal{O}_K^\times) \cdot \bigcup_{i=1}^s C\Phi(a_i)$. Therefore, $G/\Phi(\mathcal{O}_K^\times)$ is Hausdorff (because $\Phi(\mathcal{O}_K^\times)$ is closed) and it is equal to the continuous image of the bounded set $\bigcup_{i=1}^s C\Phi(a_i)$, so $G/\Phi(\mathcal{O}_K^\times)$ is compact. \square

Theorem 3.5.4 (Dirichlet). *Let K be a number field. Then \mathcal{O}_K^\times is of finite type. Its torsion subgroup is:*

$$\mu(K) = \{x \in K \mid \exists m \geq 1, x^m = 1\}.$$

The group $\mathcal{O}_K^\times/\mu(K)$ is free abelian of rank $r = r_1 + r_2 - 1$, where r_1 (resp. $2r_2$) is the number of real (resp. complex) embeddings $K \hookrightarrow \mathbb{C}$. In other words, there exist $\varepsilon_1, \dots, \varepsilon_r \in \mathcal{O}_K^\times$ s.t. the map:

$$\begin{cases} \mu(K) \times \mathbb{Z}^r & \longrightarrow \mathcal{O}_K^\times \\ (\varepsilon, a_1, \dots, a_r) & \longmapsto \varepsilon \varepsilon_1^{a_1} \dots \varepsilon_r^{a_r} \end{cases},$$

is an isomorphism.

Proof. With the notations of Lemma 3.5.3, we have $\Phi(\mathcal{O}_K^\times) = \Phi(\mathcal{O}_K) \cap G$. Therefore, we know that $\Phi(\mathcal{O}_K^\times)$ is discrete and cocompact in G . Now if $V = \mathbb{R}^{\Sigma_r} \oplus \mathbb{C}^{\Sigma_c}$, consider the map:

$$L : (x, z) \in V^\times \longmapsto (\log|x_1|, \dots, \log|x_{r_1}|, 2\log|z_1|, \dots, 2\log|z_{r_2}|) \in \mathbb{R}^{r+1}.$$

Set $H = L(G) = \{y \in \mathbb{R}^{r+1}, y_1 + \dots + y_{r+1} = 0\}$ and $\Lambda = L(\Phi(\mathcal{O}_K^\times))$, so that Λ is a lattice in H . In particular, Λ is a free abelian group of rank $\dim H = r$. And we check that $\mu(K) = \text{Ker}(L \circ \Phi)$. Thus, we have an exact sequence:

$$1 \longrightarrow \mu(K) \longrightarrow \mathcal{O}_K^\times \xrightarrow{L \circ \Phi} \Lambda \longrightarrow 0.$$

This gives the result. \square

Remark 3.5.5. *If K is a real number field (i.e. $K \subseteq \mathbb{R}$), then $\mu(K) = \{\pm 1\}$.*

Example 3.5.6. *Let $K = \mathbb{Q}(\sqrt{2})$. By Dirichlet's Theorem (Theorem 3.5.4), there exists $\varepsilon \in \mathcal{O}_K^\times$ s.t. $\mathcal{O}_K^\times = \{\pm 1\} \times \varepsilon^\mathbb{Z}$. Let $\eta = 1 + \sqrt{2}$. We see that $N_{K/\mathbb{Q}}(\eta) = -1$, so $\eta \in \mathcal{O}_K^\times$. Now, let us show that η generates $\mathcal{O}_K^\times/\{\pm 1\}$. If $u \in \mathcal{O}_K^\times$ is a generator of $\mathcal{O}_K^\times/\{\pm 1\}$, then $\eta = \pm u^k$, with $k \in \mathbb{Z}$. We may assume that $k \geq 0$ and we wish to show that $k = 1$. Let σ be the embedding $K \hookrightarrow \mathbb{C}$ given by $\sigma(\sqrt{2}) = -\sqrt{2}$. If $k \geq 2$, then $|u| = |\eta|^{\frac{1}{k}} = (1 + \sqrt{2})^{\frac{1}{k}} \leq \sqrt{1 + \sqrt{2}}$ and $|\sigma(u)| = |\sigma(\eta)|^{\frac{1}{k}} < 1$. Therefore $(u, \sigma(u)) \in F = \{(y, z) \in \mathbb{R}^2, |y| \leq \sqrt{1 + \sqrt{2}} \text{ and } |z| < 1\} \subseteq \mathbb{R}^{\Sigma_r} \oplus \mathbb{C}^{\Sigma_c}$. We finally prove that $F \cap \Phi(\mathcal{O}_K) = \{0\}$, so $u = 0$, which is a contradiction. Therefore:*

$$\mathcal{O}_K^\times = \{\pm 1\} \times (1 + \sqrt{2})^\mathbb{Z}.$$

3.6 Application to the Pell-Fermat Equation

Theorem 3.6.1 (Lagrange). *Let $d \geq 0$ be a square-free integer. Then there exists a nontrivial solution $(x_1, y_1) \in \mathbb{N}^* \times \mathbb{N}^*$ of the equation $X^2 - dY^2 = 1$ s.t. every solution of this equation in \mathbb{Z}^2 is of the form $(\pm x_n, \pm y_n)$, with $x_n + \sqrt{d}y_n = (x_1 + \sqrt{d}y_1)^n$ for $n \in \mathbb{Z}$.*

Proof. Let $K = \mathbb{Q}(\sqrt{d})$. We know that $\mathbb{Z}[\sqrt{d}]^\times$ is a subgroup of \mathcal{O}_K^\times with finite index. By Dirichlet's Theorem (Theorem 3.5.4), there exists $\varepsilon \in \mathbb{Z}[\sqrt{d}]^\times$ s.t.

$$\mathbb{Z}[\sqrt{d}]^\times = \{\pm 1\} \times \varepsilon^\mathbb{Z}.$$

Write $\varepsilon = u + v\sqrt{d}$, with $u, v \in \mathbb{Z}$. If $N_{K/\mathbb{Q}}(\varepsilon) = 1$, then take $x_1 = |u|$ and $x_2 = |v|$; otherwise $N_{K/\mathbb{Q}}(\varepsilon) = -1$ and take $x_1 = |s|$ and $x_2 = |t|$ where $\varepsilon^2 = s + t\sqrt{d}$. \square

Proposition 3.6.2. *Let $x, y \in \mathbb{N}^*$. Then:*

$$x^2 - dy^2 = 1 \iff \left| \frac{x}{y} - \sqrt{d} \right| < \frac{1}{2\sqrt{dy^2}}.$$

Proof. Show that $0 < x^2 - dy^2 < 2 \iff \left| \frac{x}{y} - \sqrt{d} \right| < \frac{1}{2\sqrt{dy^2}}$. \square

Remark 3.6.3. *Proposition 3.6.2 means that solutions of the Pell-Fermat Equation correspond to good rational approximations of \sqrt{d} . These approximations can actually be computed using continued fractions.*

4 Introduction to analytic methods

4.1 Dirichlet series

Definition 4.1.1 (Dirichlet series). *A Dirichlet series is a function of the form $f(s) = \sum_{n \in \mathbb{N}^*} a_n n^{-s}$, with $(a_n)_{n \in \mathbb{N}^*} \in \mathbb{C}^{\mathbb{N}^*}$.*

Proposition 4.1.2. *Let $(a_n)_{n \in \mathbb{N}^*} \in \mathbb{C}^{\mathbb{N}^*}$. Suppose that there exists $s_0 \in \mathbb{C}$ s.t. $\sum_{n \in \mathbb{N}^*} a_n n^{-s_0}$ converges. Then, for any $\theta \in [0, \frac{\pi}{2})$, $\sum_{n \in \mathbb{N}^*} a_n n^{-s}$ converges uniformly over $(s_0 + \mathbb{R}_+ e^{i\theta} + \mathbb{R}_+ e^{-i\theta})$.*

Corollary 4.1.3. *Let $(a_n)_{n \in \mathbb{N}^*} \in \mathbb{C}^{\mathbb{N}^*}$. Then there exists $\rho \in \overline{\mathbb{R}}$ s.t. $\sum_{n \in \mathbb{N}^*} a_n n^{-s}$ converges if $\Re(s) > \rho$ and diverges if $\Re(s) < \rho$. Moreover, the function defined by $f(s) = \sum_{n \in \mathbb{N}^*} a_n n^{-s}$ is holomorphic over $\{\Re(s) > \rho\}$.*

Example 4.1.4 (Riemann ζ -function). *Consider the function:*

$$\zeta(s) = \sum_{n \in \mathbb{N}^*} \frac{1}{n^s}.$$

Then, with the notations of Corollary 4.1.3, we have $\rho = 1$.

Proposition 4.1.5. *The Riemann ζ -function of Example 4.1.4 can be extended to a meromorphic function on $\{\Re(s) > 0\}$, with only one pole at 1, which is simple and with residue 1.*

Proof. For $\Re(s) > 1$, we have:

$$\zeta(s) = \int_1^\infty t^{-s} dt + \underbrace{\sum_{n \in \mathbb{N}^*} \int_n^{n+1} \left(\frac{1}{n^s} - \frac{1}{t^s} \right) dt}_{\varphi(s)} = \frac{1}{s-1} + \varphi(s).$$

Therefore, it suffices to prove that φ defines a holomorphic function on $\{\Re(s) > 0\}$. \square

Remark 4.1.6. *The Riemann ζ -function can actually be extended to a meromorphic function on \mathbb{C} , with two simple poles at 0 and 1, and vanishing on $2\mathbb{Z}_{<0}$.*

4.2 Dedekind ζ -function of a number field

Definition 4.2.1 (Dedekind ζ -function). *Let K be a number field. We define the Dedekind ζ -function of K by:*

$$\zeta_K(s) = \sum_{\mathfrak{a} \in I^+(\mathcal{O}_K)} N(\mathfrak{a})^{-s} = \sum_{n \in \mathbb{N}^*} a_n n^{-s},$$

where $a_n = |\{\mathfrak{a} \in I^+(\mathcal{O}_K), N(\mathfrak{a}) = n\}|$ for $n \in \mathbb{N}^*$.

Example 4.2.2. *For $K = \mathbb{Q}$, $\zeta_{\mathbb{Q}} = \zeta$ is the Riemann ζ -function.*

Proposition 4.2.3. *Let K be a number field. Then:*

$$\zeta_K(s) = \sum_{\mathfrak{a} \in I^+(\mathcal{O}_K)} N(\mathfrak{a})^{-s} = \prod_{\mathfrak{p} \in P} (1 - N(\mathfrak{p})^{-s})^{-1},$$

where both the series and the product converge locally uniformly over $\{\Re(s) > 1\}$, and where P is the set of prime ideals of \mathcal{O}_K .

Proof. Let $d = [K : \mathbb{Q}]$. Note that, for $\mathfrak{p} \in P$, $N(\mathfrak{p}) = p^{f(\mathfrak{p}/p)} \geq p$ and for any prime number p , $|\{\mathfrak{p} \in P, \mathfrak{p} | p\}| \leq d$. Therefore:

$$\sum_{\substack{\mathfrak{p} \in P \\ N(\mathfrak{p}) \leq X}} |N(\mathfrak{p})^{-s}| \leq d \sum_{\substack{p \text{ prime} \\ p \leq X}} |p^{-s}| \leq d \sum_{1 \leq n \leq X} n^{-\Re(s)}.$$

This shows the convergence of $\sum_{\mathfrak{p} \in P} N(\mathfrak{p})^{-s}$, and therefore of $\prod_{\mathfrak{p} \in P} (1 - N(\mathfrak{p})^{-s})^{-1}$, over $\{\Re(s) > 1\}$. Now, for $s \in \mathbb{R}$ with $s > 1$, we have:

$$\begin{aligned} \sum_{\substack{\mathfrak{a} \in I^+(\mathcal{O}_K) \\ N(\mathfrak{a}) \leq X}} N(\mathfrak{a})^{-s} &\leq \prod_{\substack{\mathfrak{p} \in P \\ N(\mathfrak{p}) \leq X}} (1 + N(\mathfrak{p})^{-s} + N(\mathfrak{p})^{-2s} + \dots) = \prod_{\substack{\mathfrak{p} \in P \\ N(\mathfrak{p}) \leq X}} (1 - N(\mathfrak{p})^{-s})^{-1} \\ &\leq \prod_{\mathfrak{p} \in P} (1 - N(\mathfrak{p})^{-s})^{-1}. \end{aligned}$$

This shows the convergence of $\sum_{\mathfrak{a} \in I^+(\mathcal{O}_K)} N(\mathfrak{a})^{-s}$ on $\{\Re(s) > 1\}$. Moreover, for any s with $\Re(s) > 1$:

$$\left| \sum_{\substack{\mathfrak{a} \in I^+(\mathcal{O}_K) \\ N(\mathfrak{a}) \leq X}} N(\mathfrak{a})^{-s} - \prod_{\mathfrak{p} \in P} (1 - N(\mathfrak{p})^{-s})^{-1} \right| \leq \sum_{\substack{\mathfrak{a} \in I^+(\mathcal{O}_K) \\ N(\mathfrak{a}) > X}} |N(\mathfrak{a})|^{-s} \xrightarrow{X \rightarrow +\infty} 0.$$

□

Example 4.2.4. *Let $K = \mathbb{Q}(i)$. Then:*

$$\zeta_{\mathbb{Q}(i)}(s) = \left(1 - \frac{1}{2^s}\right)^{-1} \prod_{\substack{p \equiv 1 \\ \text{mod } 4}} \left(1 - \frac{1}{p^s}\right)^{-2} \prod_{\substack{p \equiv 2,3 \\ \text{mod } 4}} \left(1 - \frac{1}{p^{2s}}\right)^{-1}.$$

This example shows that ζ_K encodes the behaviour of prime numbers in \mathcal{O}_K .

Corollary 4.2.5. *Let K be a number field. Then:*

$$\sum_{\mathfrak{p} \in P} N(\mathfrak{p})^{-s} \underset{1}{\sim} -\log(s-1) \underset{1}{\sim} \sum_{\substack{\mathfrak{p} \in P \\ f(\mathfrak{p}/p)=1}} N(\mathfrak{p})^{-s}.$$

Proof. Use the formula of Proposition 4.2.3 to compute $\log \zeta_K(s)$, and write:

$$\log \zeta_K(s) = \sum_{\substack{\mathfrak{p} \in P \\ f(\mathfrak{p}/p)=1}} N(\mathfrak{p})^{-s} + \sum_{\substack{\mathfrak{p} \in P \\ f(\mathfrak{p}/p)=2}} N(\mathfrak{p})^{-s} + \sum_{\substack{\mathfrak{p} \in P \\ m \geq 2}} \frac{1}{m} N(\mathfrak{p})^{-ms}.$$

Show that the two latter sums converge for $\Re(s) > \frac{1}{2}$. Using the fact that ζ_K extends to a meromorphic function over $\left\{ \Re(s) > 1 - \frac{1}{[K:\mathbb{Q}]} \right\}$ with a simple pole at 1 (c.f. Theorem 4.3.6), we have $\log \zeta_K(s) \sim -\log(s-1)$. The result follows. \square

Corollary 4.2.6. *Let K be a number field.*

- (i) *The set of prime ideals in \mathcal{O}_K of degree 1 is infinite.*
- (ii) *If K/\mathbb{Q} is Galois, then the set of prime numbers which split totally in K is infinite.*

Definition 4.2.7 (Analytic density). *Let K be a number field. Let S be a subset of the set of prime ideals of \mathcal{O}_K . If the quantity:*

$$\frac{\sum_{\mathfrak{p} \in S} N(\mathfrak{p})^{-s}}{\sum_{\mathfrak{p} \in P} N(\mathfrak{p})^{-s}} \underset{1}{\sim} \frac{\sum_{\mathfrak{p} \in S} N(\mathfrak{p})^{-s}}{\log(s-1)},$$

has a limit δ as $s \rightarrow 1$, we say that S has analytic density δ .

Corollary 4.2.8. *If K is a number field, then the set of prime ideals of \mathcal{O}_K of degree 1 has analytic density 1.*

4.3 Class Number Formula

Definition 4.3.1 (Regulator). *Let K be a number field. Recall that $\Psi(\mathcal{O}_K^\times)$ is a lattice in $H = \{y \in \mathbb{R}^{r+1}, y_1 + \dots + y_{r+1} = 0\}$, where $\Psi = L \circ \Phi$ with the notations of Theorem 3.5.4. We define the regulator of K by:*

$$R_K = \frac{1}{\sqrt{r+1}} \text{Covol} \left(\Psi \left(\mathcal{O}_K^\times \right) \right),$$

where H is equipped with the Euclidean structure induced by \mathbb{R}^{r+1} .

Proposition 4.3.2. *Let K be a number field. Let $1 \leq i_0 \leq r+1$ and let $\pi : \mathbb{R}^{r+1} \rightarrow \mathbb{R}^r$ be the projection on the hyperplane $\{y_{i_0} = 0\}$. Then:*

$$R_K = \text{Covol} \left(\pi \circ \Psi \left(\mathcal{O}_K^\times \right) \right).$$

In other words, if $\varepsilon_1, \dots, \varepsilon_r$ form a basis of $\mathcal{O}_K^\times / \mu(K)$, and if we write $\Sigma_r = \{\sigma_1, \dots, \sigma_{r_1}\}$ and $\Sigma'_c = \{\sigma_{r_1+1}, \dots, \sigma_{r_1+r_2}\}$, then:

$$R_K = \left| \det \left(\log |\sigma_i(\varepsilon_j)| \right)_{\substack{1 \leq i \leq r+1 \\ i \neq i_0 \\ 1 \leq j \leq r}} \right|.$$

Remark 4.3.3. *Let K be a quadratic number field.*

- (i) *If K is real, then $R_K = \log |\varepsilon|$, where ε is a fundamental unit of \mathcal{O}_K .*
- (ii) *If K is imaginary, then $R_K = 1$.*

Lemma 4.3.4. *Let $(a_n)_{n \in \mathbb{N}^*} \in \mathbb{C}^{\mathbb{N}^*}$. Consider the Dirichlet series $\sum_{n \in \mathbb{N}^*} a_n n^{-s}$.*

- (i) *If $(a_n)_{n \in \mathbb{N}^*}$ is bounded, then the series converges over $\{\Re(s) > 1\}$.*

(ii) Let $A_N = \sum_{n=1}^N a_n$. If $A_N = \kappa N + \mathcal{O}(N^{1-\delta})$ for some $\kappa \in \mathbb{C}$ and $\delta \in (0, 1]$, then $\sum_{n \in \mathbb{N}^*} a_n n^{-s}$ has a meromorphic extension to $\{\Re(s) > 1 - \delta\}$ with a simple pole at 1, and with residue κ .

Proof. Use an Abel Transform. □

Lemma 4.3.5. Let $\Lambda \subseteq \mathbb{R}^n$ be a lattice, and let $\Gamma \subseteq \mathbb{R}^n$ be a bounded subset s.t. $\partial\Gamma$ is covered by images of a finite number of Lipschitz maps $[0, 1]^{n-1} \rightarrow \mathbb{R}^n$. Then:

$$|\Lambda \cap t\Gamma| = \frac{\text{Vol}(\Gamma)}{\text{Covol}(\Lambda)} t^n + \mathcal{O}_\infty(t^{n-1}).$$

Theorem 4.3.6 (Class Number Formula). Let K be a number field. Then the Dedekind ζ -function ζ_K admits a meromorphic extension to $\{\Re(s) > 1 - \frac{1}{[K:\mathbb{Q}]}\}$ with only a simple pole at 1, and with:

$$\text{Res}_1(\zeta_K) = \frac{2^{r_1} (2\pi)^{r_2} R_K h_K}{w_K |D_K|^{\frac{1}{2}}},$$

where $w_k = |\mu(K)|$ is the number of roots of unity, and $h_K = |\text{Cl}(\mathcal{O}_K)|$ is the class number.

Proof. By Lemma 4.3.4, it is enough to study the asymptotic behaviour of:

$$A_N = \left| \left\{ \mathfrak{a} \in I^+(\mathcal{O}_K), N(\mathfrak{a}) \leq N \right\} \right|.$$

For $C \in \text{Cl}(\mathcal{O}_K)$, we consider $A_{N,C} = |\{\mathfrak{a} \in C \cap I^+(\mathcal{O}_K), N(\mathfrak{a}) \leq N\}|$; thus $A_N = \sum_{C \in \text{Cl}(\mathcal{O}_K)} A_{N,C}$. Now, fix $\mathfrak{a}_0 \in C$ and note that:

$$\begin{aligned} A_{N,C} &= \left| \left\{ (x)\mathfrak{a}_0, x \in \mathfrak{a}_0^{-1} \setminus \{0\} \text{ and } |N_{K/\mathbb{Q}}(x)| \leq N \cdot N(\mathfrak{a}_0)^{-1} \right\} \right| \\ &= \left| \left\{ x \in \mathfrak{a}_0^{-1} \setminus \{0\}, |N_{K/\mathbb{Q}}(x)| \leq N \cdot N(\mathfrak{a}_0)^{-1} \right\} / \mathcal{O}_K^\times \right| \\ &= \frac{1}{w_K} \left| \left\{ x \in \mathfrak{a}_0^{-1} \setminus \{0\}, |N_{K/\mathbb{Q}}(x)| \leq N \cdot N(\mathfrak{a}_0)^{-1} \right\} / U_K \right|, \end{aligned}$$

where U_K is the free abelian part of $\text{Cl}(\mathcal{O}_K)^\times$, i.e. such that $\mathcal{O}_K^\times \simeq \mu(K) \times U_K$ (c.f. Theorem 3.5.4). Hence, in order to compute $A_{N,C}$, we are led to find a fundamental domain for the action $U_K \curvearrowright K^\times$. Recall that we have a map $\Psi : K^\times \rightarrow \mathbb{R}^{r+1}$ s.t. $\Psi(\mathcal{O}_K^\times)$ is a lattice in H (c.f. Theorem 3.5.4). Consider a fundamental domain $P \subseteq H$ for the action $\Psi(U_K) \curvearrowright H$. Then, if $w = (1, \dots, 1, 2, \dots, 2) \in \mathbb{R}^{r+1}$, $\Psi^{-1}(P + \mathbb{R}w)$ is a fundamental domain for the action $U_K \curvearrowright K^\times$. Hence, we deduce that:

$$A_{N,C} = \frac{1}{w_K} \left| \Gamma_{N \cdot N(\mathfrak{a}_0)^{-1}} \cap \mathfrak{a}_0^{-1} \setminus \{0\} \right|,$$

where $\Gamma_t = \Psi^{-1}(P + (-\infty, \frac{1}{n} \log t] \cdot w)$. Now, note that $\Gamma_t = t^{1/n} \Gamma_1$. Hence, using Lemma 4.3.5, we obtain:

$$A_{N,C} = \frac{1}{w_K} \cdot \frac{\text{Vol}(\Phi(\Gamma_1))}{\text{Covol}(\Phi(\mathfrak{a}_0^{-1}))} \cdot N \cdot N(\mathfrak{a}_0)^{-1} + \mathcal{O}(N^{1-\frac{1}{n}}).$$

Using the facts that $\text{Vol}(\tilde{\Gamma}_1) = 2^{r_1} (2\pi)^{r_2} 2^{-r_2} R_K$ and $A_N = \sum_{C \in \text{Cl}(\mathcal{O}_K)} A_{N,C}$, we obtain:

$$A_N = \frac{2^{r_1} (2\pi)^{r_2} R_K h_K}{w_K |D_K|^{\frac{1}{2}}} N + \mathcal{O}(N^{1-\frac{1}{n}}).$$

The result follows by Lemma 4.3.4. □

4.4 Dirichlet characters and Dirichlet L -functions

Notation 4.4.1. Let $a, N \geq 2$ with $\gcd(a, N) = 1$. We define:

$$\mathcal{P}_{a,N} = \{p \in \mathcal{P}, p \equiv a \pmod{N}\},$$

where \mathcal{P} is the set of all prime numbers. Our goal is to prove that $\mathcal{P}_{a,N}$ is infinite.

Remark 4.4.2. We have a holomorphic function defined by $\sum_{p \in \mathcal{P}_{a,N}} p^{-s}$ on $\{\Re(s) > 1\}$. Our aim will be to prove that it diverges at 1. In particular, this will imply that $\mathcal{P}_{a,N}$ is infinite. We note that:

$$\sum_{p \in \mathcal{P}_{a,N}} p^{-s} = \sum_{p \in \mathcal{P}} \mathbf{1}_{\bar{a}}(p) p^{-s},$$

where \bar{a} is the class of a in $\mathbb{Z}/N\mathbb{Z}$. The map $\mathbf{1}_{\bar{a}}: \mathbb{Z} \rightarrow \{0, 1\}$ induces a map $\mathbf{1}_{\bar{a}}: (\mathbb{Z}/N\mathbb{Z})^\times \rightarrow \{0, 1\}$. But Representation Theory tells us that the set X of irreducible characters on $(\mathbb{Z}/N\mathbb{Z})^\times$ forms a unitary basis of the set of maps $(\mathbb{Z}/N\mathbb{Z})^\times \rightarrow \mathbb{C}$, relative to the Hermitian scalar product $(\cdot | \cdot)$ given by $(f | g) = \frac{1}{\varphi(N)} \sum_{x \in (\mathbb{Z}/N\mathbb{Z})^\times} f(x) \overline{g(x)}$. Therefore, we have:

$$\mathbf{1}_{\bar{a}} = \sum_{\chi \in X} (\chi | \mathbf{1}_{\bar{a}}) \chi = \frac{1}{\varphi(N)} \sum_{\chi \in X} \overline{\chi(a)} \chi.$$

Thus:

$$\sum_{p \in \mathcal{P}_{a,N}} p^{-s} = \frac{1}{\varphi(N)} \sum_{\chi \in X} \overline{\chi(a)} \underbrace{\sum_{p \in \mathcal{P}} \chi(p) p^{-s}}_{f_\chi(s)}.$$

Now, for every irreducible character χ , f_χ defines a holomorphic function on $\{\Re(s) > 1\}$ which has the same behaviour at 1 as:

$$-\log \prod_{p \in \mathcal{P}} (1 - \chi(p) p^{-s}) = f_\chi(s) + \sum_{\substack{m \geq 2 \\ p \in \mathcal{P}}} \frac{\chi(p)^m}{m p^{ms}}.$$

Notation 4.4.3. If χ is a character on $(\mathbb{Z}/N\mathbb{Z})^\times$ and $s \in \mathbb{C}$ with $\Re(s) > 1$, we define:

$$L(\chi, s) = \prod_{p \in \mathcal{P}} (1 - \chi(p) p^{-s})^{-1} = \sum_{n \in \mathbb{N}^*} \chi(n) n^{-s}.$$

For any χ , $L(\chi, \cdot)$ is a holomorphic function on $\{\Re(s) > 1\}$.

Lemma 4.4.4. If χ is a nontrivial character on $(\mathbb{Z}/N\mathbb{Z})^\times$, then $L(\chi, \cdot)$ can be extended to a holomorphic function on $\{\Re(s) > 0\}$.

Proof. Note that $\sum_{n=1}^N \chi(n) = (\chi | 1) = 0 = \mathcal{O}(1)$ and apply Lemma 4.3.4. \square

Lemma 4.4.5. If χ_0 is the trivial character on $(\mathbb{Z}/N\mathbb{Z})^\times$, then $L(\chi_0, \cdot)$ can be extended to a meromorphic function on $\{\Re(s) > 0\}$, with a simple pole at 1. Therefore:

$$\log L(\chi_0, s) = -\log(s-1) + \mathcal{O}_1(1).$$

Definition 4.4.6 (Dirichlet characters). Let $N \geq 1$. A Dirichlet character modulo N is a group homomorphism $\chi: (\mathbb{Z}/N\mathbb{Z})^\times \rightarrow \mathbb{C}$ which extends to \mathbb{Z} by defining $\chi(n) = 0$ if $\gcd(n, N) \neq 1$. The conductor of χ , denoted by $\text{cond}(\chi)$, is the smallest integer $M | N$ s.t. χ factors through $(\mathbb{Z}/M\mathbb{Z})^\times$. We say that χ is primitive if $\text{cond}(\chi) = N$.

Definition 4.4.7 (Dirichlet L -functions). The Dirichlet L -function of a Dirichlet character χ is the function $L(\tilde{\chi}, \cdot)$ (c.f. Notation 4.4.3), where $\tilde{\chi}$ is the unique primitive character induced by χ .

Example 4.4.8. If χ is the trivial character modulo N , then $\tilde{\chi}$ is the trivial character modulo 1 and $L(\tilde{\chi}, \cdot)$ is the Riemann ζ -function.

Proposition 4.4.9. Let K be a subfield of $\mathbb{Q}(\mu_N(\mathbb{C}))$. Thus, K/\mathbb{Q} is a Galois extension; we write $G = \text{Gal}(K/\mathbb{Q})$. Then, if \hat{G} is the set of group homomorphisms $G \rightarrow \mathbb{C}$, we have:

$$\zeta_K = \prod_{\chi \in \hat{G}} L(\chi, \cdot).$$

Corollary 4.4.10. Let χ be a nontrivial character on $(\mathbb{Z}/N\mathbb{Z})^\times$. We know that $L(\chi, \cdot)$ extends to a holomorphic function on $\{\Re(s) > 0\}$ (c.f. Lemma 4.4.4), and we have $L(\chi, 1) \neq 0$.

Theorem 4.4.11 (Dirichlet). Let $a, N \geq 2$ with $\gcd(a, N) = 1$. Then the set $\mathcal{P}_{a,N}$ is infinite. Moreover, it has analytic density $\frac{1}{\varphi(N)}$.

Proof. Consider the holomorphic function defined by $\sum_{p \in \mathcal{P}_{a,N}} p^{-s}$ on $\{\Re(s) > 1\}$. Then we have:

$$\sum_{p \in \mathcal{P}_{a,N}} p^{-s} = -\frac{1}{\varphi(N)} \log(s-1) + \frac{1}{\varphi(N)} \sum_{\chi \neq \chi_0} \overline{\chi(a)} f_\chi(s) + \mathcal{O}_1(1).$$

Using Corollary 4.4.10, we conclude that $\sum_{p \in \mathcal{P}_{a,N}} p^{-s}$ has a pole at 1, and therefore $\mathcal{P}_{a,N}$ is infinite. \square

References

- [1] K. Ireland and M. Rosen. *A Classical Introduction to Modern Number Theory*.
- [2] J. Neukirch. *Algebraic Number Theory*.
- [3] P. Samuel. *Théorie algébrique des nombres*.
- [4] H.P.F. Swinnerton-Dyer. *A Brief Guide to Algebraic Number Theory*.