1

Basic algebraic number theory

We have collected some basic facts about algebraic number fields (finite field extensions of $\mathbb{Q}$), p-adic numbers, and related topics. For further details and proofs, we refer to Lang (1970), chapters I–V, Neukirch (1992), Kapitel I–III and Koblitz (1984).

In the present book, a *ring* is by default a commutative ring with unit element, and an *integral domain* is a commutative ring with unit element and without divisors of 0. Given a ring A, we denote by A^+ its underlying additive group, and by A^* its unit group (multiplicative group of invertible elements).

The ring of integers of an algebraic number field K, that is the integral closure of $\mathbb{Z}$ in K, is denoted by O_K.

1.1 Characteristic polynomial, trace, norm, discriminant

For the moment, let K be any field of characteristic 0. Choose an algebraic closure $\overline{K}$ of K. For every $\alpha \in \overline{K}$, there is a unique, monic, irreducible polynomial $f_\alpha \in K[X]$, such that $f_\alpha(\alpha) = 0$, and f_α divides g for every polynomial $g \in K[X]$ with $g(\alpha) = 0$. We call f_α the *monic minimal polynomial* of α.

Let $f \in K[X]$ be a non-zero polynomial. Then $f = a(X - \alpha_1)\dots(X - \alpha_r)$ with $a \in K^*, \alpha_1, \dots, \alpha_r \in K$. We call $K(\alpha_1, \dots, \alpha_r)$ the splitting field of f over K.

Let L be a finite extension of K of degree n. Then there are precisely n distinct K-isomorphic embeddings $L \hookrightarrow \overline{K}$, $\sigma_1, \dots, \sigma_n$, say. The composition of the fields $\sigma_1(L), \dots, \sigma_n(L)$ is called the normal closure of L over K. We define the *characteristic polynomial* of $\alpha \in L$ with respect to L/K by

$$\chi_{L/K,\alpha} := \prod_{i=1}^{n}(X - \sigma_i(\alpha)).$$

In fact, we have $\chi_{L/K,\alpha} = f_\alpha^{[L:K(\alpha)]}$ and $\chi_{L/K,\alpha}$ is the characteristic polynomial of the K-linear map $x \mapsto \alpha x$ from L to L. So $\chi_{L/K,\alpha} \in K[X]$.

We define the *trace* and *norm* of $\alpha \in L$ over K by

$$\mathrm{Tr}_{L/K}(\alpha) := \sum_{i=1}^{n} \sigma_i(\alpha), \quad N_{L/K}(\alpha) := \prod_{i=1}^{n} \sigma_i(\alpha).$$

These are up to sign coefficients of $\chi_{L/K,\alpha}$. So we have

$$\mathrm{Tr}_{L/K}(\alpha), \quad N_{L/K}(\alpha) \in K \quad \text{for } \alpha \in L. \tag{1.1.1}$$

Notice that $\mathrm{Tr}_{L/K}$ is a K-linear map $L \to K$ and that $N_{L/K}$ is a multiplicative map $L \to K$. Further, the trace and norm are transitive in towers: let $M \supset L \supset K$ be a tower of finite extension fields; then

$$\left.\begin{aligned} \mathrm{Tr}_{M/K}(\alpha) &= \mathrm{Tr}_{L/K}(\mathrm{Tr}_{M/L}(\alpha)), \\ N_{M/K}(\alpha) &= N_{L/K}(N_{M/L}(\alpha)) \end{aligned}\right\} \quad \text{for } \alpha \in M.$$

Let again L be a finite extension of K of degree n. Take a K-basis $\{\omega_1, \ldots, \omega_n\}$ of L. Then the *discriminant* of this basis is given by

$$D_{L/K}(\omega_1, \ldots, \omega_n) := \det(\mathrm{Tr}_{L/K}(\omega_i \omega_j))_{i,j=1,\ldots,n}.$$

By (1.1.1) we have $D_{L/K}(\omega_1, \ldots, \omega_n) \in K$. The discriminant can be expressed otherwise as

$$D_{L/K}(\omega_1, \ldots, \omega_n) = (\det(\sigma_i(\omega_j))_{i,j=1,\ldots,n})^2,$$

where $\sigma_1, \ldots, \sigma_n$ are the K-isomorphic embeddings of L in $\overline{K}$. For instance, if $L = K(\theta)$, then $\{1, \theta, \ldots, \theta^{n-1}\}$ is a K-basis of L and by Vandermonde's identity,

$$D_{L/K}(1, \theta, \ldots, \theta^{n-1}) = \prod_{1 \le i < j \le n} (\sigma_i(\theta) - \sigma_j(\theta))^2 \neq 0. \tag{1.1.2}$$

Let $\{\theta_1, \ldots, \theta_n\}$, $\{\omega_1, \ldots, \omega_n\}$ be any two K-bases of L. Then

$$\omega_i = \sum_{j=1}^{n} a_{ij}\theta_j \quad \text{for } i = 1, \ldots, n$$

with $a_{ij} \in K$ and $\det(a_{ij}) \neq 0$. By a straightforward computation we have

$$D_{L/K}(\omega_1, \ldots, \omega_n) = (\det(a_{ij})_{i,j=1,\ldots,n})^2 D_{L/K}(\theta_1, \ldots, \theta_n). \tag{1.1.3}$$

By applying this relation with $\{1, \theta, \ldots, \theta^{n-1}\}$ for $\{\theta_1, \ldots, \theta_n\}$, and using (1.1.2), we deduce that if $\{\omega_1, \ldots, \omega_n\}$ is any K-basis of L, then

$$D_{L/K}(\omega_1, \ldots, \omega_n) \neq 0.$$

We give an application to linear algebra. Let again K be a field of characteristic 0, and let G be a Galois extension of K. For a vector $\mathbf{x} = (x_1, \ldots, x_g) \in G^g$

and for σ in the Galois group $\mathrm{Gal}(G/K)$ of G over K, we define $\sigma(\mathbf{x}) := (\sigma(x_1), \dots, \sigma(x_g))$.

Lemma 1.1.1 *Let $g \geq 1$, and let V be a G-linear subspace of G^g such that*

$$\sigma(\mathbf{x}) \in V \quad \text{for } \mathbf{x} \in V, \sigma \in \mathrm{Gal}(G/K).$$

Then V has a basis consisting of vectors from K^g.

Proof. Pick a non-zero vector $\mathbf{b} \in V$. Let $L \subseteq G$ be the smallest Galois extension of K containing the coefficients of $\mathbf{b}$ and choose a K-basis $\{\omega_1, \dots, \omega_n\}$ of L. Let $\mathrm{Gal}(L/K) = \{\sigma_1, \dots, \sigma_n\}$. We have $\mathbf{b} = \sum_{j=1}^n \omega_j \mathbf{y}_j$ with $\mathbf{y}_j \in K^g$ for $j = 1, \dots, n$. Then also $\sigma_i(\mathbf{b}) = \sum_{j=1}^n \sigma_i(\omega_j)\mathbf{y}_j$ for $i = 1, \dots, n$. The matrix $(\sigma_i(\omega_j))_{i,j=1,\dots,n}$ is invertible (the square of its determinant being the discriminant of $\omega_1, \dots, \omega_n$), hence $\mathbf{y}_1, \dots, \mathbf{y}_n$ are L-linear combinations of $\sigma_i(\mathbf{b})$ $(i = 1, \dots, n)$. Now our assumption on V implies that $\mathbf{y}_1, \dots, \mathbf{y}_n \in V$. It follows that V is generated by vectors from K^g, hence it has a basis from K^g. □

Now let K be an algebraic number field and L a finite extension of K. Then for $\alpha \in L$ we have

$$\alpha \in O_L \iff \chi_{L/K,\alpha} \in O_K[X].$$

As a consequence,

$$\mathrm{Tr}_{L/K}(\alpha), N_{L/K}(\alpha) \in O_K \quad \text{for } \alpha \in O_L,$$

and

$$D_{L/K}(\omega_1, \dots, \omega_n) \in O_K$$

for every K-basis $\{\omega_1, \dots, \omega_n\}$ of L with $\omega_1, \dots, \omega_n \in O_L$.

1.2 Ideal theory for algebraic number fields

We start with some general notation. Let A be an integral domain with quotient field K. For $\alpha \in K$ and a subset $\mathcal{F}$ of K, we define $\alpha\mathcal{F} := \{\alpha x : x \in \mathcal{F}\}$. A *fractional ideal* of A is a subset $\mathfrak{a}$ of K such that $\mathfrak{a} \neq \{0\}$ and there is $\alpha \in A \setminus \{0\}$ such that $\alpha\mathfrak{a}$ is an ideal of A. In particular, for $\alpha \in K^*$, the set αA is a fractional ideal, which we denote by (α) when it is clear from the context what the underlying domain A is. More generally, given a subset $\mathcal{S} \neq \{0\}$ of K such that there is $\alpha \in A \setminus \{0\}$ with $\alpha\mathcal{S} \subset A$, the set of all finite A-linear combinations with elements from $\mathcal{S}$ is a fractional ideal of A, denoted by $\mathcal{S}A$, called the fractional ideal generated by $\mathcal{S}$.

Let K be an algebraic number field. Recall that its ring of integers O_K is a *Dedekind domain*, that is, O_K is integrally closed, every ideal of O_K is finitely generated, and every non-zero prime ideal of O_K is a maximal ideal (see Lang (1970), chapter 1, sections 2, 3). Henceforth, when we are dealing with prime ideals of O_K, we always exclude (0).

Let $\mathfrak{a}$, $\mathfrak{b}$ be two fractional ideals of O_K. We define their greatest common divisor or sum, lowest common multiple and product by

$$\gcd(\mathfrak{a},\mathfrak{b}) = \mathfrak{a}+\mathfrak{b} := \{\alpha+\beta : \alpha\in\mathfrak{a}, \beta\in\mathfrak{b}\},$$

$$\mathrm{lcm}(\mathfrak{a},\mathfrak{b}) := \mathfrak{a}\cap\mathfrak{b},$$

$$\mathfrak{a}\mathfrak{b} := O_K\text{-module generated by all products } \alpha\beta \text{ with } \alpha\in\mathfrak{a} \text{ and } \beta\in\mathfrak{b},$$

respectively. Further, the inverse of a fractional ideal $\mathfrak{a}$ of O_K is defined by

$$\mathfrak{a}^{-1} := \{\alpha\in K : \alpha\mathfrak{a}\subseteq O_K\}.$$

The gcd, lcm and product of two fractional ideals of O_K, and the inverse of a fractional ideal of O_K are again fractional ideals of O_K.

We denote by $\mathcal{P}(O_K)$ the collection of non-zero prime ideals of O_K. The following result comprises the ideal theory for O_K.

Theorem 1.2.1

(i) *The fractional ideals of O_K form an abelian group with product and inverse as defined above, and with unit element $O_K = (1)$.*

(ii) *Every fractional ideal $\mathfrak{a}$ of O_K can be decomposed uniquely as a product of powers of prime ideals*

$$\mathfrak{a} = \prod_{\mathfrak{p}\in\mathcal{P}(O_K)} \mathfrak{p}^{\mathrm{ord}_{\mathfrak{p}}(\mathfrak{a})},$$

where the exponents $\mathrm{ord}_{\mathfrak{p}}(\mathfrak{a})$ are rational integers, at most finitely many of which are non-zero.

(iii) *A fractional ideal $\mathfrak{a}$ of O_K is contained in O_K if and only if $\mathrm{ord}_{\mathfrak{p}}(\mathfrak{a})\geq 0$ for every $\mathfrak{p}\in\mathcal{P}(O_K)$.*

Proof. See Lang (1970), chapter 1, section 6. □

The group of fractional ideals of O_K is denoted by $I(O_K)$.

The following consequences are obvious.

Corollary 1.2.2 *Let $\mathfrak{a}$, $\mathfrak{b}$ be two fractional ideals of O_K. Then*

$$\mathfrak{a}\subseteq\mathfrak{b} \iff \mathrm{ord}_{\mathfrak{p}}(\mathfrak{a})\geq\mathrm{ord}_{\mathfrak{p}}(\mathfrak{b}) \text{ for every } \mathfrak{p}\in\mathcal{P}(O_K).$$

Further, we have for every $\mathfrak{p} \in \mathcal{P}(O_K)$,

$$\begin{aligned} \mathrm{ord}_{\mathfrak{p}}(\mathfrak{a} \cdot \mathfrak{b}) &= \mathrm{ord}_{\mathfrak{p}}(\mathfrak{a}) + \mathrm{ord}_{\mathfrak{p}}(\mathfrak{b}), \\ \mathrm{ord}_{\mathfrak{p}}(\mathfrak{a} + \mathfrak{b}) &= \min(\mathrm{ord}_{\mathfrak{p}}(\mathfrak{a}), \mathrm{ord}_{\mathfrak{p}}(\mathfrak{b})), \\ \mathrm{ord}_{\mathfrak{p}}(\mathfrak{a} \cap \mathfrak{b}) &= \max(\mathrm{ord}_{\mathfrak{p}}(\mathfrak{a}), \mathrm{ord}_{\mathfrak{p}}(\mathfrak{b})). \end{aligned}$$

For $\mathfrak{p} \in \mathcal{P}(O_K)$ we define

$$\mathrm{ord}_{\mathfrak{p}}(x) := \mathrm{ord}_{\mathfrak{p}}((x)) \quad \text{if } x \in K^*, \quad \mathrm{ord}_{\mathfrak{p}}(0) := \infty.$$

Corollary 1.2.2 implies that for every $\mathfrak{p} \in \mathcal{P}(O_K)$, $\mathrm{ord}_{\mathfrak{p}}$ defines a *discrete valuation* on K, i.e., $\mathrm{ord}_{\mathfrak{p}}$ is a surjective map from K to $\mathbb{Z} \cup \{\infty\}$ such that for $x, y \in K$ we have

$$\begin{aligned} &\mathrm{ord}_{\mathfrak{p}}(xy) = \mathrm{ord}_{\mathfrak{p}}(x) + \mathrm{ord}_{\mathfrak{p}}(y); \\ &\mathrm{ord}_{\mathfrak{p}}(x + y) \geq \min(\mathrm{ord}_{\mathfrak{p}}(x), \mathrm{ord}_{\mathfrak{p}}(y)), \\ &\mathrm{ord}_{\mathfrak{p}}(x) = \infty \Longleftrightarrow x = 0. \end{aligned}$$

The next corollary, whose proof is straightforward, gives some other consequences.

Corollary 1.2.3

(i) Let $\mathfrak{a}$ *be a fractional ideal of* O_K. *Then*

$$x \in \mathfrak{a} \Longleftrightarrow \mathrm{ord}_{\mathfrak{p}}(x) \geq \mathrm{ord}_{\mathfrak{p}}(\mathfrak{a}) \text{ for all } \mathfrak{p} \in \mathcal{P}(O_K).$$

In particular,

$$x \in O_K \Longleftrightarrow \mathrm{ord}_{\mathfrak{p}}(x) \geq 0 \text{ for all } \mathfrak{p} \in \mathcal{P}(O_K).$$

(ii) Let $\mathfrak{a}$ *be the fractional ideal of* O_K *generated by a set* $\mathcal{S}$. *Then*

$$\mathrm{ord}_{\mathfrak{p}}(\mathfrak{a}) = \min\{\mathrm{ord}_{\mathfrak{p}}(\alpha) : \alpha \in \mathcal{S}\} \quad \text{for } \mathfrak{p} \in \mathcal{P}(O_K).$$

1.3 Extension of ideals; norm of ideals

Let K be an algebraic number field and L a finite extension of K of degree n. Every fractional ideal $\mathfrak{a}$ of O_K can be extended to a fractional ideal of O_L,

$$\mathfrak{a}O_L := \{\alpha y : \alpha \in \mathfrak{a}, y \in O_L\},$$

and the map $\mathfrak{a} \mapsto \mathfrak{a}O_L$ gives an injective group homomorphism from the group of fractional ideals of O_K to the group of fractional ideals of O_L. The extension of a prime ideal $\mathfrak{p}$ of O_K can be decomposed in a unique way as a product of

powers of prime ideals of O_L, that is,

$$\mathfrak{p}O_L = \prod_{i=1}^{g} \mathfrak{P}_i^{e_i},$$

where $\mathfrak{P}_1, \dots, \mathfrak{P}_g$ are distinct prime ideals of O_L and $e_1, \dots, e_g$ are positive integers. We call $\mathfrak{P}_1, \dots, \mathfrak{P}_g$ the prime ideals of O_L lying above $\mathfrak{p}$. The exponent e_i, henceforth denoted by $e(\mathfrak{P}_i|\mathfrak{p})$, is called the *ramification index* of $\mathfrak{P}_i$ over $\mathfrak{p}$. The residue class ring $O_L/\mathfrak{P}_i$ is a finite field extension of $O_K/\mathfrak{p}$. The degree $[O_L/\mathfrak{P}_i : O_K/\mathfrak{p}]$ of this extension, called the *residue class degree* of $\mathfrak{P}_i$ over $\mathfrak{p}$, is denoted by $f(\mathfrak{P}_i|\mathfrak{p})$. The next proposition gives some properties of ramification indices and residue class degrees.

Proposition 1.3.1 *Let L, $\mathfrak{p}$, $\mathfrak{P}_1, \dots, \mathfrak{P}_g$ be as above.*

(i) We have $\sum_{i=1}^{g} e(\mathfrak{P}_i|\mathfrak{p}) f(\mathfrak{P}_i|\mathfrak{p}) = [L : K]$.
(ii) Assume that L/K is a Galois extension. Then for any two prime ideals $\mathfrak{P}_i, \mathfrak{P}_j \in \{\mathfrak{P}_1, \dots, \mathfrak{P}_g\}$ there is $\sigma \in \mathrm{Gal}(L/K)$ such that $\mathfrak{P}_j = \sigma\mathfrak{P}_i$. Further, $e(\mathfrak{P}_1|\mathfrak{p}) = \cdots = e(\mathfrak{P}_g|\mathfrak{p})$ and $f(\mathfrak{P}_1|\mathfrak{p}) = \cdots = f(\mathfrak{P}_g|\mathfrak{p})$.

Proof. See Lang (1970), chapter 1, section 7, proposition 21, corollary 2. □

Proposition 1.3.2 (transitivity in towers) *Let $M \supset L \supset K$ be a tower of finite field extensions. Further, let $\mathfrak{P}$ be a prime ideal of O_L in the prime ideal factorization of $\mathfrak{p}O_L$ and $\mathfrak{Q}$ a prime ideal in the prime ideal factorization of $\mathfrak{P}O_M$. Then*

$$e(\mathfrak{Q}|\mathfrak{p}) = e(\mathfrak{Q}|\mathfrak{P}) \cdot e(\mathfrak{P}|\mathfrak{p}), \qquad f(\mathfrak{Q}|\mathfrak{p}) = f(\mathfrak{Q}|\mathfrak{P}) \cdot f(\mathfrak{P}|\mathfrak{p}).$$

Proof. See Lang (1970), chapter 1, section 7, proposition 20. □

Let again K be an algebraic number field and L a finite extension of K. We define the *norm* over K of a prime ideal $\mathfrak{P}$ of O_L by $\mathfrak{N}_{L/K}(\mathfrak{P}) := \mathfrak{p}^{f(\mathfrak{P}|\mathfrak{p})}$, where $\mathfrak{p}$ is the prime ideal of O_K such that $\mathfrak{P}$ occurs in the prime ideal factorization of $\mathfrak{p}O_L$. Then the norm $\mathfrak{N}_{L/K}(\mathfrak{A})$ of an arbitrary fractional ideal $\mathfrak{A}$ of O_L is defined by multiplicativity, i.e.,

$$\mathfrak{N}_{L/K}(\mathfrak{A}) := \prod_{\mathfrak{p} \in \mathcal{P}(O_K)} \mathfrak{p}^{\sum_{\mathfrak{P}|\mathfrak{p}} f(\mathfrak{P}|\mathfrak{p}) \cdot \mathrm{ord}_{\mathfrak{P}}(\mathfrak{A})}, \tag{1.3.1}$$

where the sum is over all prime ideals of O_L lying above $\mathfrak{p}$. Thus, $\mathfrak{N}_{L/K}$ defines a homomorphism from the group of fractional ideals of O_L to the group of fractional ideals of O_K.

Below, we give some properties of the norm.

Proposition 1.3.3 *Let L be a finite extension of K.*

(i) *Let $\mathfrak{A}$ be a fractional ideal of O_L. Then $\mathfrak{N}_{L/K}(\mathfrak{A})$ is equal to the fractional ideal generated by the numbers $N_{L/K}(\alpha)$, $\alpha \in \mathfrak{A}$.*

(ii) *For every $\alpha \in L^*$ we have $\mathfrak{N}_{L/K}(\alpha O_L) = N_{L/K}(\alpha)O_K$.*

(iii) *Let $\mathfrak{p}$ be a prime ideal of O_K, and $\mathfrak{P}_1, \ldots, \mathfrak{P}_g$ the prime ideals of O_L dividing $\mathfrak{p}$. Then for every $\alpha \in O_L$,*

$$\mathrm{ord}_{\mathfrak{p}}(N_{L/K}(\alpha)) = \sum_{i=1}^{g} f(\mathfrak{P}_i|\mathfrak{p})\mathrm{ord}_{\mathfrak{P}_i}(\alpha).$$

(iv) *For every fractional ideal $\mathfrak{a}$ of O_K we have $\mathfrak{N}_{L/K}(\mathfrak{a}O_L) = \mathfrak{a}^{[L:K]}$.*

(v) *Let M be a finite extension of L. Then for every fractional ideal $\mathfrak{C}$ of O_M,*

$$\mathfrak{N}_{M/K}(\mathfrak{C}) = \mathfrak{N}_{L/K}(\mathfrak{N}_{M/L}(\mathfrak{C})).$$

Proof. For (i), (iv), (v) see Neukirch (1992), Kapitel III, Satz 1.6. Part (ii) is a consequence of (i), and part (iii) a consequence of (ii) and (1.3.1). □

Let K be an algebraic number field. The norm $\mathfrak{N}_{K/\mathbb{Q}}(\mathfrak{a})$ of a fractional ideal $\mathfrak{a}$ of O_K is a fractional ideal of $\mathbb{Z}$. Hence there is a positive rational number a such that $\mathfrak{N}_{K/\mathbb{Q}}(\mathfrak{a}) = (a)$. This number a is called the *absolute norm* of $\mathfrak{a}$, notation $N_K(\mathfrak{a})$ (often written as $N(\mathfrak{a})$ if it is clear from the context which is the underlying number field). It is obvious that the absolute norm is multiplicative. From parts (ii) and (iv) of Proposition 1.3.3, we obtain at once:

$$N_K((\alpha)) = |N_{K/\mathbb{Q}}(\alpha)| \text{ for } \alpha \in K^*, \quad N_K((a)) = |a|^{[K:\mathbb{Q}]} \text{ for } a \in \mathbb{Q}^*.$$

If $\mathfrak{p}$ is a prime ideal of O_K dividing a prime number p, we have $N_K(\mathfrak{p}) = p^{f(\mathfrak{p}|p)} = |O_K/\mathfrak{p}|$. More generally, for any non-zero ideal $\mathfrak{a}$ of O_K we have

$$N_K(\mathfrak{a}) = |O_K/\mathfrak{a}|.$$

1.4 Discriminant, class number, unit group and regulator

Let K be an algebraic number field of degree d over $\mathbb{Q}$. There are d distinct isomorphic embeddings of K in $\mathbb{C}$, which we denote by $\sigma_1, \ldots, \sigma_d$; further, we will write $\alpha^{(i)} := \sigma_i(\alpha)$ for $\alpha \in K$. We assume that among these embeddings there are precisely r_1 real embeddings, i.e., embeddings σ with $\sigma(K) \subset \mathbb{R}$, and r_2 pairs of complex conjugate embeddings, i.e., pairs $\{\sigma, \overline{\sigma}\}$ where $\overline{\sigma}(\alpha) = \overline{\sigma(\alpha)}$ for $\alpha \in K$. Thus, $d = r_1 + 2r_2$ and after reordering the embeddings we

may assume that σ_i $(i = 1, \dots, r_1)$ are the real embeddings and $\{\sigma_i, \sigma_{i+r_2}\}$ $(i = r_1 + 1, \dots r_1 + r_2)$ the pairs of complex conjugate embeddings.

Viewed as a $\mathbb{Z}$-module, O_K is free of rank d. Taking any $\mathbb{Z}$-basis $\{\omega_1, \dots, \omega_d\}$ of O_K, we define the *discriminant* of K by

$$D_K := D_{K/\mathbb{Q}}(\omega_1, \dots, \omega_d) = \left(\det\left(\omega_j^{(i)}\right)_{i,j=1,\dots,d}\right)^2.$$

This is a non-zero rational integer which, by (1.1.3), is independent of the choice of the basis.

Denote as before by $I(O_K)$ the group of fractional ideals of O_K. Further, denote by $P(O_K)$ the subgroup of principal fractional ideals of O_K. The quotient group $\mathrm{Cl}(O_K) = I(O_K)/P(O_K)$ is called the *class group* of K.

Theorem 1.4.1 *The class group* $\mathrm{Cl}(O_K)$ *of* O_K *is finite.*

Proof. See Neukirch (1992), Kapitel I, Satz 6.3. □

The cardinality of the class group is called the *class number* of K, and we denote this by h_K.

We denote by W_K the multiplicative group consisting of all roots of unity in K. This is a finite, cyclic subgroup of K^*. We denote the number of roots of unity of K by ω_K.

We recall the following fundamental theorem of Dirichlet concerning the unit group O_K^* of O_K. Elements of O_K^* will usually be referred to as units of K. Recall that if V is an n-dimensional vector space over $\mathbb{R}$, then a *full lattice* in V is an additive subgroup

$$\{z_1\mathbf{a}_1 + \cdots + z_n\mathbf{a}_n : z_1, \dots, z_n \in \mathbb{Z}\},$$

where $\{\mathbf{a}_1, \dots, \mathbf{a}_n\}$ is a basis of V.

Theorem 1.4.2 *The map*

$$LOG_K : \varepsilon \mapsto \left(e_1 \log|\varepsilon^{(1)}|, \dots, e_{r_1+r_2} \log|\varepsilon^{(r_1+r_2)}|\right)$$

(where $e_j = 1$ *for* $j = 1, \dots r_1$ *and* $e_j = 2$ *for* $j = r_1 + 1, \dots, r_1 + r_2$*) defines a surjective homomorphism from* O_K^* *to a full lattice in the real vector space given by*

$$\{\mathbf{x} = (x_1, \dots, x_{r_1+r_2}) \in \mathbb{R}^{r_1+r_2} : x_1 + \cdots + x_{r_1+r_2} = 0\}$$

with kernel W_K.

Proof. See Neukirch (1992), Kapitel I, Satz 7.1. □

The following consequence is immediate.

Corollary 1.4.3 *Put* $r = r_K := r_1 + r_2 - 1$. *Then*

$$O_K^* \cong W_K \times \mathbb{Z}^r.$$

More explicitly, there are $\varepsilon_1, \dots, \varepsilon_r \in O_K^*$ *such that every* $\varepsilon \in O_K^*$ *can be expressed uniquely as*

$$\varepsilon = \zeta \varepsilon_1^{b_1} \dots \varepsilon_r^{b_r}$$

where ζ *is a root of unity in* K *and* $b_1, \dots b_r$ *are rational integers.*

The number r_K (denoted by r if it is clear to which number field it refers) is called the *unit rank* of K. A set of units $\{\varepsilon_1, \dots, \varepsilon_r\}$ as above is called a *fundamental system of units* for K. Given such a system, we define the *regulator* of K by

$$R_K := \left| \det\left(e_j \log \left| \varepsilon_i^{(j)} \right| \right)_{i,j=1,\dots,r} \right|.$$

This regulator is non-zero, and independent of the choice of $\varepsilon_1, \dots, \varepsilon_r$.

1.5 Explicit estimates

We have collected from the literature some estimates for the field parameters defined above. As before, K is an algebraic number field of degree d.

For the number ω_K of roots of unity of K we have the estimate

$$\omega_K \le 20d \log\log d \quad \text{if } d \ge 3. \tag{1.5.1}$$

This follows from the observation that the degree of the maximal cyclotomic subfield of K, which is $\varphi(\omega_K)$ where φ is Euler's totient function, divides d, and from Rosser and Schoenfeld (1962), Theorem 15, which gives an explicit lower bound for $\varphi(n)$ of the order $n/\log\log n$.

For the class number and regulator of K we have

$$h_K R_K \le |D_K|^{1/2} (\log^* |D_K|)^{d-1}. \tag{1.5.2}$$

The first inequality of this type was proved by Landau (1918). The above version follows from Louboutin (2000) and (1.5.1); see (59) in Győry and Yu (2006). The following lower bound for the regulator is due to Friedman (1989):

$$R_K > 0.2052. \tag{1.5.3}$$

We recall an important lower estimate for discriminants. By an inequality due to Minkowski (see, e.g., Lang (1970), chapter V, section 4, proof of corollary

of theorem 4) we have

$$|D_K| > \left(\frac{\pi}{4}\right)^d \left(\frac{d^d}{d!}\right)^2. \tag{1.5.4}$$

Further, we need the following lemma.

Lemma 1.5.1 *Let $g \in \mathbb{Z}[X]$ be a monic polynomial of degree m with non-zero discriminant. Assume that the coefficients of g have absolute values at most M. Let $K = \mathbb{Q}(\theta)$, where θ is a zero of g. Then*

$$|D_K| \le m^{2m-1} M^{2m-2}.$$

Proof. The monic minimal polynomial, say f, of θ is in $\mathbb{Z}[X]$ and it divides g in $\mathbb{Z}[X]$. Suppose K has degree d. Using the expression of the discriminant of a monic polynomial as the product of the squares of the differences of its zeros, one easily shows that the discriminant $D(f)$ of f divides $D(g)$ in the ring of algebraic integers and so also in $\mathbb{Z}$. Further, by (1.1.2), we have $D(f) = D_{K/\mathbb{Q}}(1, \theta, \ldots, \theta^{d-1})$. Writing $1, \theta, \ldots, \theta^{d-1}$ as $\mathbb{Z}$-linear combinations of a $\mathbb{Z}$-basis of O_K, and using (1.1.3), we infer that D_K divides $D(f)$. Therefore, D_K divides $D(g)$. Using for instance an estimate from Lewis and Mahler (1961) (bottom of p. 335), which uses a determinantal expression for $D(g)$, one obtains

$$|D(g)| \le m^{2m-1} M^{2m-2}.$$

This proves our lemma. □

Remark There is an analogue for this lemma where for g one can take any non-zero polynomial in $\mathbb{Z}[X]$, not necessarily monic or of non-zero discriminant. We will not work this out.

1.6 Absolute values: generalities

We have collected some facts on absolute values. Our basic reference is Neukirch (1992), Kapitel II.

Let K be an infinite field. An *absolute value* on K is a function $|\cdot| : K \to \mathbb{R}_{\ge 0}$ satisfying the following conditions:

$|xy| = |x| \cdot |y|$ for all $x, y \in K$;

there is $C \ge 1$ such that $|x + y| \le C \max(|x|, |y|)$ for all $x, y \in K$;

$|x| = 0 \iff x = 0$.

These conditions imply that $|1| = 1$. An absolute value $|\cdot|$ on K is called *trivial* if $|x| = 1$ for $x \in K^*$. Henceforth, all absolute values we will consider