Algebraic number theory

Olivier Haution

Technische Universität München

Summer semester 2022

Foreword

These are notes for a course given at the Technische Universität München in Summer 2022. The course is based on the book [**Sam70**] by Pierre Samuel. We follow this reference very closely in certain sections, but also diverge somewhat in other sections.

Formally the prerequisites for this course are rather minimal: mostly familiarity with rings, fields, modules, and basic linear algebra (say, over fields). We will occasionally use the tensor product of modules, but only in the simple case of free modules. Familiarity with localisation and Galois theory will be helpful, but not strictly required (at least until the last part of the course). Basic analytic methods will also be used (Fubini's Theorem, Lebesgue measure on $\mathbb{R}^n$).

Contents

Introduction

In this introduction we provide some motivation for the general theory that will be developed in this course. In particular, we will prove in this section the following result, attributed to Girard in 1625: if p is an odd prime number, then

$$p = a^2 + b^2 \text{ for some } a, b \in \mathbb{Z} \quad \iff \quad p = 1 \mod 4.$$

This result is sometimes attributed instead to Fermat, and the first proof is due to Euler in 1749. We will present a proof due to Dedekind which appeared in 1894, whose main idea is to use the so-called Gaussian integers:

DEFINITION 0.1. The ring of *Gaussian integers* $\mathbb{Z}[i]$ is the subring of $\mathbb{C}$ consisting of the elements of the form $a + bi$ with $a, b \in \mathbb{Z}$ (as usual $i \in \mathbb{C}$ denotes a chosen element such that $i^2 = -1$).

We define the *norm* function as the restriction of the map $\mathbb{C} \to \mathbb{N}, \alpha \mapsto |\alpha^2|$, namely:

$$\mathrm{N} \colon \mathbb{Z}[i] \to \mathbb{N}, \quad a + bi \mapsto a^2 + b^2.$$

Note that $\mathrm{N}(0) = 0$, $\mathrm{N}(1) = 1$, and that $\mathrm{N}(\alpha) \geq 1$ whenever $\alpha \neq 0$. Further, it is easy to verify that

$$\mathrm{N}(\alpha\beta) = \mathrm{N}(\alpha)\,\mathrm{N}(\beta) \quad \text{for any } \alpha, \beta \in \mathbb{Z}[i].$$

We recall that in a commutative ring R, an element is called a unit if it admits a multiplicative inverse. The set of units is a group, denoted by $R^\times$.

LEMMA 0.2. *An element $\alpha \in \mathbb{Z}[i]$ is a unit if and only if $\mathrm{N}(\alpha) = 1$.*

PROOF. Indeed, if $\alpha \in \mathbb{Z}[i]^\times$, we have

$$1 = \mathrm{N}(1) = \mathrm{N}(\alpha\alpha^{-1}) = \mathrm{N}(\alpha)\,\mathrm{N}(\alpha^{-1}),$$

hence we must have $\mathrm{N}(\alpha) = 1$. Conversely if $\mathrm{N}(\alpha) = 1$, write $\alpha = a + bi$ with $a, b \in \mathbb{Z}$. Then $\overline{\alpha} = a - bi$ satisfies

$$\alpha\overline{\alpha} = a^2 + b^2 = \mathrm{N}(\alpha) = 1,$$

and so $\overline{\alpha}$ is the inverse of α. □

REMARK 0.3. In fact, it is easy to see that $\mathbb{Z}[i]^\times = \{1, -1, i, -i\}$.

DEFINITION 0.4. A commutative (unital associative) ring A is called a *principal ideal domain* if every ideal of A is of the form aA for some $a \in A$.

EXAMPLE 0.5. Prominent examples of principal ideal domains are $\mathbb{Z}$, and the polynomial ring $k[X]$ when k is a field.

LEMMA 0.6. *Let $\alpha, \beta \in \mathbb{Z}[i]$, with $\beta \neq 0$. Then there exists elements $\gamma, \rho \in \mathbb{Z}[i]$ such that*

$$\alpha = \gamma\beta + \rho \quad \textit{and} \quad \mathrm{N}(\rho) < \mathrm{N}(\beta).$$

Proof. Let us write $\alpha/\beta = x + iy \in \mathbb{C}$, with $x, y \in \mathbb{R}$. Then we may find $a, b \in \mathbb{Z}$ such that $|x - a| \leq 1/2$ and $|y - b| \leq 1/2$. Set $\gamma = a + bi \in \mathbb{Z}[i]$, and $\rho = \alpha - \beta\gamma$. Then

$$\mathrm{N}(\rho) = |\alpha - \beta\gamma|^2 = |\beta|^2 \cdot \left|\frac{\alpha}{\beta} - \gamma\right|^2 = |\beta|^2 \cdot ((x-a)^2 + (y-b)^2) \leq \frac{|\beta|^2}{2} < \mathrm{N}(\beta). \quad \square$$

Proposition 0.7. *The ring $\mathbb{Z}[i]$ is a principal ideal domain.*

Proof. Let I be an ideal of $\mathbb{Z}[i]$. Let us pick a nonzero element $\beta \in A$ such that $\mathrm{N}(\beta) \in \mathbb{N} \smallsetminus \{0\}$ is minimal. Then for any $\alpha \in A$, by Lemma 0.6 we may write $\alpha = \gamma\beta + \rho$ with $\gamma, \rho \in \mathbb{Z}[i]$ and $\mathrm{N}(\rho) < \mathrm{N}(\beta)$. By minimality of $\mathrm{N}(\beta)$, we must have $\rho = 0$, and thus $\alpha = \gamma\beta$. We have proved that $I = \beta \cdot \mathbb{Z}[i]$. $\square$

Recall that an element x in a ring R is called *irreducible* if $x \notin R^\times \cup \{0\}$, and for all $a, b \in R$

$$x = ab \implies a \in R^\times \text{ or } b \in R^\times.$$

Proposition 0.8 (Girard, Dedekind). *Let p be an odd prime number. Then the following conditions are equivalent:*

(i) p is congruent to 1 modulo 4,
(ii) -1 is a square in $\mathbb{Z}/p\mathbb{Z}$,
(iii) p is not irreducible in $\mathbb{Z}[i]$,
(iv) $p = a^2 + b^2$ for some $a, b \in \mathbb{Z}$.

Proof. (i) $\Rightarrow$ (ii) : The ring $\mathbb{Z}/p\mathbb{Z}$ is a finite field, and so its group of units $(\mathbb{Z}/p\mathbb{Z})^\times$ is cyclic (we will reprove this classical fact later) of order $p-1$. We thus have an isomorphism $(\mathbb{Z}/p\mathbb{Z})^\times \simeq \mathbb{Z}/(p-1)\mathbb{Z}$; the element $-1 \in (\mathbb{Z}/p\mathbb{Z})^\times$ corresponds to $(p-1)/2 \in \mathbb{Z}/(p-1)\mathbb{Z}$ (those are the unique elements of order 2). If p is congruent to 1 modulo 4, then $(p-1)/2$ is divisible by 2 in $\mathbb{Z}/(p-1)\mathbb{Z}$, which means that -1 is a square in $(\mathbb{Z}/p\mathbb{Z})^\times$.

(ii) $\Rightarrow$ (iii) : If -1 is a square in $\mathbb{Z}/p\mathbb{Z}$, then we may find an integer $x \in \mathbb{Z}$ such that $p \mid x^2 + 1 = (x + i)(x - i)$. We now assume that p is irreducible in $\mathbb{Z}[i]$, and come to a contradiction. Let $I \subset \mathbb{Z}[i]$ be the ideal generated by p and $x + i$. As the ring $\mathbb{Z}[i]$ is a principal ideal domain (Lemma 0.7), we have $I = \alpha \cdot \mathbb{Z}[i]$ for some $\alpha \in \mathbb{Z}[i]$. Then α divides p in $\mathbb{Z}[i]$. As p is irreducible in $\mathbb{Z}[i]$, the element $\alpha \in \mathbb{Z}[i]$ is either a unit, or divisible by p. But p does not divide $x + i$ in $\mathbb{Z}[i]$ (an element of $\mathbb{Z}$ divides $a + bi$ in $\mathbb{Z}[i]$ if and only if it divides a and b; in our case $b = 1$), hence p does not divide α in $\mathbb{Z}[i]$. We deduce that α must be a unit in $\mathbb{Z}[i]$, and so $I = \mathbb{Z}[i]$. In particular we may find elements $\beta, \gamma \in \mathbb{Z}[i]$ such that

$$1 = p\beta + (x + i)\gamma \in \mathbb{Z}[i].$$

Multiplying with $x - i$ and using the relation $(x+i)(x-i) = p$ shows that $x - i$ is divisible by p in $\mathbb{Z}[i]$, a contradiction (this is the case $b = -1$ in the remark above).

(iii) $\Rightarrow$ (iv) : Assume that $p = \alpha\beta$, where $\alpha, \beta \in \mathbb{Z}[i]$ are not units. Then

$$p^2 = \mathrm{N}(p) = \mathrm{N}(\alpha) \cdot \mathrm{N}(\beta) \in \mathbb{N}.$$

Since by Lemma 0.2 we have $\mathrm{N}(\alpha) \neq 1$ and $\mathrm{N}(\beta) \neq 1$, and as p is prime, we must have $p = \mathrm{N}(\alpha)$. Writing $\alpha = a + bi$ with $a, b \in \mathbb{Z}$, yields the required pair (a, b).

(iv) $\Rightarrow$ (i) : Observe that for any $x \in \mathbb{Z}$, we have

$$x^2 = \begin{cases} 0 \mod 4 & \text{if } x = 0 \mod 2, \\ 1 \mod 4 & \text{if } x = 1 \mod 2. \end{cases} \tag{0.a}$$

Therefore for any $a, b \in \mathbb{Z}$, the integer a^2+b^2 is congruent modulo 4 to $0, 1$ or 2. If a^2+b^2 is an odd prime, the only possibility is 1 modulo 4. □

Remark 0.9. Beside the norm function, the *trace* function

$$\mathrm{Tr}\colon \mathbb{Z}[i] \to \mathbb{Z}, \quad a+bi \mapsto 2a$$

can be useful. In particular, for any $\alpha \in \mathbb{Z}[i]$, we have

$$\alpha^2 - \alpha\,\mathrm{Tr}(\alpha) + \mathrm{N}(\alpha) = 0$$

(this may be verified using by a direct computation, writing $\alpha = a + bi$). Thus the elements of $\mathbb{Z}[i]$ are always the solutions of a monic polynomial equation with coefficients in $\mathbb{Z}$.

CHAPTER 1

Basic commutative ring theory

All rings will be assumed unital, associative and commutative. When R is a ring, we denote by $R^\times$ the multiplicative group consisting of the invertible elements of R. When A is a subring of B, we will sometimes say that $A \subset B$ is a ring extension.

Let A be a ring. An *A-algebra* is a ring R equipped with a ring morphism $\iota_R \colon A \to R$. When R, S are A-algebra, a ring morphism $f \colon R \to S$ is called a morphism of A-algebras if $f \circ \iota_R = \iota_S$.

1. Prime and maximal ideals

Recall that a nonzero ring A is called a *domain*, or integral domain, if for every $x, y \in A$ we have

$$xy = 0 \in A \quad \implies x = 0 \text{ or } y = 0.$$

The *fraction field* K of a domain A is a field containing A, which is minimal (with respect to field inclusions) among such fields. Its elements are the fractions a/b for $a, b \in A$ with $b \neq 0$, subject to the relations $a/b = a'/b'$ whenever $ab' = a'b$. In particular every element of K is of the form ab^{-1} with $a, b \in A$.

Let A be a ring. We recall that an ideal $\mathfrak{p}$ of A is called *prime* if it satisfies any of the following equivalent conditions:

(i) $\mathfrak{p} \neq A$, and for all $x, y \in A$ such that $xy \in \mathfrak{p}$, we have $x \in \mathfrak{p}$ or $y \in \mathfrak{p}$.
(ii) the ring $A/\mathfrak{p}$ is a domain.

An ideal $\mathfrak{m}$ of A is called *maximal* if it satisfies any of the following equivalent conditions:

(i') $\mathfrak{m} \neq A$, and for all ideals I of A such that $\mathfrak{m} \subset I$, we have $\mathfrak{m} = I$ or $A = I$.
(ii') the ring $A/\mathfrak{m}$ is a field.

Remark 1.1.1. Since a field is a domain, every maximal ideal is prime. The converse does not hold; for instance the zero ideal in $\mathbb{Z}$ is prime but not maximal.

We now prove a few lemmas on prime ideals that will be useful.

Lemma 1.1.2. *Let $A \subset B$ be a ring extension. If $\mathfrak{q}$ is a prime ideal of B, then $\mathfrak{q} \cap A$ is a prime ideal of A.*

Proof. Indeed, the morphism $A/(\mathfrak{q} \cap A) \to B/\mathfrak{q}$ is injective, and $B/\mathfrak{q}$ is a domain. Thus $A/(\mathfrak{q} \cap A)$ is a subring of domain, and therefore it is a domain. Equivalently $\mathfrak{q} \cap A$ is a prime ideal of A. □

Lemma 1.1.3. *Let A be a ring, and $\mathfrak{p}$ a prime ideal of A. If $I_1, \dots, I_n$ are ideals of A such that $I_1 \cdots I_n \subset \mathfrak{p}$, then there exists $i \in \{1, \dots, n\}$ such that $I_i \subset \mathfrak{p}$.*

Proof. Assume the contrary, so that $\mathfrak{p}$ contains no I_i. Then there for each $i \in \{1, \dots, n\}$ there exists an element $a_i \in I_i$ such that $a_i \notin \mathfrak{p}$. Then $a_1 \cdots a_n \notin \mathfrak{p}$ because $\mathfrak{p}$ is prime. But $a_1 \cdots a_n \in I_1 \cdots I_n$, a contradiction. □

The next lemma might seem similar, but will have somewhat deeper consequences:

Lemma 1.1.4 (Prime avoidance). *Let $I, \mathfrak{p}_1, \dots, \mathfrak{p}_n$ be ideals in a ring A. Assume that the ideal $\mathfrak{p}_i$ is prime for $i \geq 3$. If $I \subset \mathfrak{p}_1 \cup \cdots \cup \mathfrak{p}_n$, then $I \subset \mathfrak{p}_i$ for some $i \in \{1, \dots, n\}$.*

Proof. We assume that I is contained in no $\mathfrak{p}_i$ and find $x \in I$ belonging to no $\mathfrak{p}_i$. This is clear for $n \in \{0, 1\}$. If $n = 2$, we find for $i = 1, 2$ elements $x_i \in I$ such that $x_i \notin \mathfrak{p}_i$. We may assume that $x_1 \in \mathfrak{p}_2$ and $x_2 \in \mathfrak{p}_1$ (otherwise the statement is proved, by taking $x = x_1$ or $x = x_2$). Then $x = x_1 + x_2$ works.

We now assume that $n > 2$, and proceed by induction on n. For each $j = 1, \dots, n$, we can find by induction an element $x_j \in I$ which is in none of the ideals $\mathfrak{p}_i$ for $i \neq j$. As above, we may assume that $x_j \in \mathfrak{p}_j$, for all $j \in \{1, \dots, n\}$ (otherwise $x = x_j$ works). Then we claim

$$x = x_n + x_1 \cdots x_{n-1} \in I$$

does the job (here $x_1 \cdots x_{n-1}$ denotes the product). Indeed assume that $x \in \mathfrak{p}_j$ for some $j \in \{1, \dots, n\}$. If $j \neq n$, then $x_1 \cdots x_{n-1} \in \mathfrak{p}_j$ (because $x_j \in \mathfrak{p}_j$), and thus $x_n = x - x_1 \cdots x_{n-1} \in \mathfrak{p}_j$, contradicting the choice of x_n. If $j = n$, then $x_1 \cdots x_{n-1} = x - x_n \in \mathfrak{p}_n$, and as the ideal $\mathfrak{p}_n$ is prime by assumption (because $n \geq 3$), we deduce that $x_i \in \mathfrak{p}_n$ for some $i \in \{1, \dots, n-1\}$, contradicting the choice of x_i. □

We will also need the so-called Chinese remainder theorem:

Lemma 1.1.5. *Let A be a ring, and $I_1, \dots, I_n$ ideals of A such that $I_i + I_j = A$ for all $i \neq j$.*

(i) We have

$$I_1 \cdots I_n = I_1 \cap \cdots \cap I_n.$$

(ii) The natural ring morphism

$$A/(I_1 \cdots I_n) \to (A/I_1) \times \cdots \times (A/I_n)$$

is bijective.

Proof. (i): Clearly $I_1 \cdots I_n \subset I_1 \cap \cdots \cap I_n$. We prove the other inclusion by induction on n, the case $n = 1$ being trivial. Assume that $n = 2$. Pick $a_1 \in I_1, a_2 \in I_2$ such that $a_1 + a_2 = 1$. Then for any $x \in I_1 \cap I_2$ we have

$$x = x(a_1 + a_2) \in (I_1 \cap I_2)I_1 + (I_1 \cap I_2)I_2 \subset I_1 I_2,$$

proving (i) for $n = 2$. Assume now that $n \geq 3$. Let $I = I_1 \cdots I_{n-1}$. By induction, we know that $I = I_1 \cap \cdots \cap I_{n-1}$. For each $i \in \{1, \dots, n-1\}$, as $I_i + I_n = A$, we find elements $x_i \in I_i, y_i \in I_n$ such that $x_i + y_i = 1$. Thus

$$x_1 \cdots x_{n-1} = (1 - y_1) \cdots (1 - y_{n-1}) = 1 \mod I_n.$$

As $x_1 \cdots x_{n-1} \in I$, this shows that $I_n + I = A$, hence by the case $n = 2$ considered above, we have

$$I_1 \cap \cdots \cap I_n = I \cap I_n = I I_n = I_1 \cdots I_n.$$

(ii): Consider the natural ring morphism

$$A \to (A/I_1) \times \cdots \times (A/I_n) \quad a \mapsto (a \mod I_1, \dots, a \mod I_n). \tag{1.1.a}$$

Its kernel is $I_1 \cap \cdots \cap I_n$, hence it follows from (i) that the morphism of (ii) is injective. For all $i, j \in \{1, \ldots, n\}$ with $i \neq j$, using the relations $I_i + I_j = A$ we find elements $e_{ij} \in I_j$ such that $e_{ij} = 1 \mod I_i$. We set, for all $i \in \{1, \ldots, n\}$

$$e_i = \prod_{j \neq i} e_{ij}.$$

Then $e_i = 1 \mod I_i$, and $e_i \in I_j$ for all $j \neq i$. Now if $(x_1, \ldots, x_n) \in A^n$, the element

$$\sum_{i=1}^{n} e_i x_i \in A$$

maps to $(x_1 \mod I_1, \ldots, x_n \mod I_n)$ under the map (1.1.a). We have proved that the map (ii) is surjective. □

2. Noetherian rings

Proposition 1.2.1. *Let A be a ring, and M an A-module. The following conditions are equivalent:*

(i) every nonempty family of A-submodules of M admits a maximal element (for the relation of inclusion),

(ii) if P_n for $n \in \mathbb{N}$ are A-submodules of M satisfying $P_n \subset P_{n+1}$ for all n, there exists $s \in \mathbb{N}$ such that $P_n = P_s$ for all $n \geq s$,

(iii) every A-submodule of M is finitely generated.

Proof. (i) ⇒ (iii) : Let N be an A-submodule of M. Consider the set Σ of all finitely generated A-submodules of M which are contained in N. The set Σ is nonempty, because it contains the zero ideal, so by (i) we may find a maximal element N in the set Σ (ordered by inclusion). Let $x \in N$. As $N' \subset N' + Ax \subset N$, we must have $N' = N' + Ax$ by maximality of N', and so $x \in N'$. We have proved that $N = N'$, and in particular the A-module N is finitely generated.

(ii) ⇒ (i) : Let E be a nonempty set of A-submodules of M. If the set E has no maximal element (for the relation of inclusion), we can find inductively elements $P_n \in E$ for all $n \in \mathbb{N}$, in such a way that $P_n \subsetneq P_{n+1}$ for all n. This contradicts (ii).

(iii) ⇒ (ii) : Consider a family of A-submodules P_n of M, for $n \in \mathbb{N}$, which satisfies $P_n \subset P_{n+1}$ for all $n \in \mathbb{N}$. Then $P = \bigcup_{n \in \mathbb{N}} P_n$ is an A-submodule of M, it is thus finitely generated by (iii), say by the elements $x_1, \ldots, x_m \in P_n$. For s large enough, we have $x_1, \ldots, x_m \in P_s$, and so $P_s = P$. In particular for $n \geq s$, we have $P_s \subset P_n \subset P = P_s$, and so $P_n = P_s$. □

Definition 1.2.2. Let A be a ring. An A-module M will be called *noetherian* if it satisfies the conditions of Proposition 1.2.1. A ring A is called *noetherian* if it is noetherian as a module over itself.

Example 1.2.3. Let k be a field, and A a k-algebra. If A is of finite dimension as a k-vector space, then the ring A is noetherian; indeed, a chain of ideals of A is in particular a chain of k-vector spaces.

Proposition 1.2.4. *Let A be a ring.*

(i) Let $f \colon M \to P$ be a surjective morphism of A-modules. If the A-module M is noetherian, then so is P.

(ii) If M and N are noetherian A-modules, then so is $M \oplus N$.

Proof. (i): Consider a family of A-submodules P_n of P, for $n \in \mathbb{N}$, such that $P_n \subset P_{n+1}$ for all $n \in \mathbb{N}$. For each $n \in \mathbb{N}$, consider the A-submodule $M_n = f^{-1}P_n$ in M. Then $M_n \subset M_{n+1}$ for all $n \in \mathbb{N}$, and $f(M_n) = P_n$ because f is surjective. As M is noetherian we may find $s \in \mathbb{N}$ such that $M_n = M_s$ for $n \geq s$, and thus $P_n = f(M_n) = f(M_s) = P_s$ for $n \geq s$. We have proved that P is noetherian.

(ii): Let $P_n \subset M \oplus N$ for $n \in \mathbb{N}$ be a family of A-submodules such that $P_n \subset P_{n+1}$ for all $n \in \mathbb{N}$. Consider the second projection $\pi\colon M \oplus N \to N$. Then the family $\pi(P_n)$ for $n \in \mathbb{N}$ satisfies $\pi(P_n) \subset \pi(P_{n+1})$ for all n, and as N is a noetherian A-module, we find an integer $s \in \mathbb{N}$ such that $\pi(P_n) = \pi(P_s)$ for all $n \geq s$.

Let $n \geq s$, and $x \in P_n$. As $\pi(P_n) = \pi(P_s)$, we find $y \in P_s$ such that $\pi(x) = \pi(y)$, or equivalently $z = x - y \in M$ (we view M as an A-submodule of $M \oplus N$ via $m \mapsto (m, 0)$). Thus $x = z + y \in M + P_s$, and thus

$$P_n \subset M + P_s \subset M \oplus N \quad \text{for all } n \geq s. \tag{1.2.a}$$

For $m \in \mathbb{N}$, consider that A-submodule $Q_m = P_{m+s}/P_s$ of $(M \oplus N)/P_s$. It follows from (1.2.a) for all $m \in \mathbb{N}$, the A-submodule Q_m is contained in $(M + P_s)/P_s = M/(P_s \cap M)$. But the A-module $M/(P_s \cap M)$ is noetherian by (i) (because M is assumed noetherian), and as $Q_m \subset Q_{m+1}$ for $m \in \mathbb{N}$, we find $r \in \mathbb{N}$ such that $Q_m = Q_r$ for $m \geq r$. Thus $P_n/P_s = P_{r+s}/P_s$ for all $n \geq r + s$, which implies that $P_n = P_{r+s}$. We have proved that the A-module $M \oplus N$ is noetherian. □

Corollary 1.2.5. *Let A be a noetherian ring, and M a finitely generated A-module. Then every A-submodule of M is finitely generated.*

Proof. Let $x_1, \ldots, x_n$ be a set of generators for the A-module M. We define a morphism of A-modules $A^{\oplus n} \to M$ by mapping the i-th element of the canonical A-basis of $A^{\oplus n}$ to x_i, for $i = 1, \ldots, n$. This morphism is surjective (because $x_1, \ldots, x_n$ generate M), the A-module $A^{\oplus n}$ is noetherian by Proposition 1.2.4 (ii) (applied $n - 1$ times), and thus the A-module M is noetherian by Proposition 1.2.4 (i). This proves the corollary, in view of Proposition 1.2.1. □

Proposition 1.2.6. *Every principal ideal domain is a noetherian ring.*

Proof. Indeed, every ideal is generated by a single element, and is thus finitely generated. □

Lemma 1.2.7. *Let A be a noetherian ring, and I an ideal of A. If $I \neq A$, then I is contained in a maximal ideal.*

Proof. The set of ideals of A containing I and distinct from A is nonempty (it contains the element I), hence as A is noetherian it admits a maximal element. Such an element is a maximal ideal of A which contains I. □

Remark 1.2.8. In fact, in any ring every proper ideal is contained in a maximal ideal. This is a consequence of the so-called Zorn's Lemma. We will not use this fact.

Lemma 1.2.9. *Let A be a noetherian ring.*

(i) Every ideal of A contains a product of prime ideals.

(ii) Assume that A is a domain. Then every nonzero ideal of A contains a product of nonzero prime ideals of A.

Repetitions are allowed in those products (i.e. the prime ideals need not be pairwise distinct), and those products are finite. Moreover, the ideal A itself is considered a product of prime ideals (over the empty family).

Proof. In case (i), we let Φ be the set of ideals of A which contain no product of prime ideals. In case (ii), we let Φ be the set of nonzero ideals of A which contain no product of nonzero prime ideals. To prove the lemma, it suffices to show that the set Φ is empty. So we assume $\Phi \neq \varnothing$ and find a contradiction. As the ring A is noetherian, the set Φ contains a maximal element I (for the inclusion of ideals). The ideal I is certainly not prime, as otherwise it would be a product of prime ideals (resp. nonzero prime ideals in case (ii)). Also $A \notin \Phi$ (because it is the product of the empty family of nonzero prime ideals), and thus $I \neq A$. So we may find $x, y \in A \smallsetminus I$ such that $xy \in I$. The ideals $I' = I + xA$ and $I'' = I + yA$ contain strictly I, hence by the choice of the ideal I, each of these ideals contains a product of prime ideals (resp. nonzero prime ideals). Then their product $I'I''$ contains a product of prime ideals (resp. nonzero prime ideals). Now

$$I'I'' = (I + xA)(I + yA) \subset I^2 + xI + yI + xyA \subset I,$$

which implies that the ideal I itself contains a product of prime ideals (resp. nonzero prime ideals). We have obtained a contradiction. □

Lemma 1.2.10. *Let A be a noetherian ring, and I an ideal of A. Then the set of prime ideals of A which are minimal (for the relation of inclusion) among those containing I, is finite.*

Proof. For every ideal J of A, let us denote by $\mathcal{M}(J)$ the set of prime ideals of A, which are minimal among those containing J. Let Φ be the set of ideals J of A such that the set $\mathcal{M}(J)$ is infinite. It will suffice to prove that the set Φ is empty. So we assume $\Phi \neq \varnothing$ and find a contradiction. As the ring A is noetherian, the set Φ admits a maximal element J. The ideal J is not prime, as otherwise the set $\mathcal{M}(J) = \{J\}$ would be finite. Also $J \neq A$, because $\mathcal{M}(A) = \varnothing$ is finite. Thus we may find $x, y \in A \smallsetminus J$ such that $xy \in J$. The ideals $J + xA$ and $J + yA$ both strictly contain J, hence $\mathcal{M}(J + xA)$ and $\mathcal{M}(J + yA)$ are both finite (by the choice of the ideal J). Now for any $\mathfrak{p} \in \mathcal{M}(J)$, we have $xy \in J \subset \mathfrak{p}$, hence $x \in \mathfrak{p}$ or $y \in \mathfrak{p}$ (as the ideal $\mathfrak{p}$ is prime). It follows that

$$\mathcal{M}(J) \subset \mathcal{M}(J + xA) \cup \mathcal{M}(J + yA)$$

(here we use the following fact: if $\mathfrak{p}$ is a prime ideal of A minimal among those containing J, and J' is an ideal of A such that $J \subset J' \subset \mathfrak{p}$, then $\mathfrak{p}$ is minimal among the prime ideals containing J'). In particular the set $\mathcal{M}(J)$ must be finite, a contradiction. □

3. Modules over principal ideal domains

Let A be a ring, and $n \in \mathbb{N}$. Recall that an A-module M is called *free of rank n* if it there exist elements $e_1, \ldots, e_n \in M$ such that

$$M = Ae_1 \oplus \cdots \oplus Ae_n.$$

The family $(e_1, \ldots, e_n)$ is then called an A-basis of M.

Remark 1.3.1. Looking at the case $A = 0$ (and thus $M = 0$), it is clear that the integer n such that M is free of rank n is not unique, if it exists. In fact, one may prove that n is unique as soon as $A \neq 0$. The case when A is a principal ideal domain will

follow from Lemma 1.3.8 below (whose arguments only use the fact that the ring A is a domain; a different argument is required for the general case).

Theorem 1.3.2. *Let A be a principal ideal domain. Let F be a free A-module of rank $n \in \mathbb{N}$, and $M \subset F$ a submodule. Then the A-module M is free of rank q, for some integer $q \in \mathbb{N}$ such that $q \leq n$.*

In addition there exist an A-basis $(e_1, \dots, e_n)$ of F, and elements $a_1, \dots, a_q \in A$ such that $(a_1 e_1, \dots, a_q e_q)$ is an A-basis of M, and $a_i \mid a_{i+1}$ for $i = 1, \dots, q-1$.

Before proving Theorem 1.3.2, we discuss some classical consequences.

Corollary 1.3.3. *Let A be a principal ideal domain, and M a finitely generated A-module. Then*

$$M \simeq (A/a_1 A) \oplus \cdots \oplus (A/a_n A),$$

for some $a_1, \dots, a_n \in A$ such that $a_i \mid a_{i+1}$ for $i = 1, \dots, n-1$.

Proof. As M is finitely generated, we may find a surjective morphism of A-modules $f \colon A^{\oplus n} \to M$, for some integer n (by mapping the canonical basis of $A^{\oplus n}$ to a system of n generators of M). We apply Theorem 1.3.2 to the free A-module $A^{\oplus n}$ of rank n, and its submodule $\ker f$. Then

$$\begin{aligned} M \simeq A^{\oplus n}/(\ker f) &= (Ae_1 \oplus \cdots \oplus Ae_q \oplus \cdots \oplus Ae_n)/(Aa_1 e_1 \oplus \cdots \oplus Aa_q e_q) \\ &\simeq (A/a_1 A) \oplus \cdots \oplus (A/a_q A) \oplus A^{\oplus(n-q)}. \end{aligned}$$

Here we have used the following fact: if M_1, M_2 are A-modules and $N_1 \subset M_1, N_2 \subset M_2$ submodules, we have an isomorphism

$$(M_1 \oplus M_2)/(N_1 \oplus N_2) \simeq (M_1/N_1) \oplus (M_2/N_2).$$

To conclude, we set $a_i = 0$ for $i = q, \dots, n$. □

When A is a ring, an A-module M is called *torsion-free* if for all $a \in A$ and $m \in M$

$$am = 0 \implies m = 0 \text{ or } a = 0.$$

Corollary 1.3.4. *Every finitely generated, torsion-free module over a principal ideal domain is free of finite rank.*

Proof. Let A be a principal ideal domain. Assume that M is a finitely generated, torsion-free A-module. We apply Corollary 1.3.3 to obtain elements $a_1, \dots, a_n$ and an isomorphism of A-modules $\varphi \colon M \xrightarrow{\sim} (A/a_1 A) \oplus \cdots \oplus (A/a_n A)$. Assume that $i \in \{1, \dots, n\}$ is such that a_i is not a unit in A. Then the element $x = \varphi^{-1}(0, \dots, 0, 1, 0, \dots, 0) \in M$ (where the i-th entry is 1) is nonzero (because $a_i \notin A^\times$) and satisfies $a_i x = 0$. As M is assumed to be torsion-free, this implies that $a_i = 0$. We have proved that each a_i is either a unit (in which case $A/a_i A = 0$), or zero (in which case $A/a_i A = A$). This implies that M is free of rank r, for some $r \in \mathbb{N}$ (equal to the number of indices i such that $a_i = 0$). □

Proposition 1.3.5. *Let A be an integral domain. Then any finite subgroup of $A^\times$ is cyclic.*

Proof. Let $G \subset A^\times$ be a finite subgroup. By Corollary 1.3.3, we have a group isomorphism $\varphi \colon G \xrightarrow{\sim} (\mathbb{Z}/a_1\mathbb{Z}) \times \cdots \times (\mathbb{Z}/a_n\mathbb{Z})$, where $a_1, \dots, a_n \in \mathbb{Z}$, and $a_i \mid a_{i+1}$ for $i = 1, \dots, n-1$. Set $m = a_n$. Since G is finite, the integer m is nonzero (otherwise G would

contain a subgroup isomorphic to $\mathbb{Z}$, and would thus be infinite). Since $a_i \mid m$ for each $i \in \{1, \dots, n\}$, every element $g \in G$ satisfies $g^m = 1$ (to see this, consider the components of the element $\varphi(g)$). On the other hand, the element $x = \varphi^{-1}(0, \dots, 0, 1) \in G$ has order m.

Let now K be the fraction field of A. Then in the field K, the polynomial $X^m - 1$ has at most m distinct roots. We have just seen that every element of G is a root of that polynomial, and so $\operatorname{card} G \leq m$. The m-elements $1, x, \dots, x^{m-1}$ of G are pairwise distinct (as x has order m), so that G must coincide with the set $\{1, x, \dots, x^{m-1}\}$, and in particular the group G is cyclic. □

The proof of Theorem 1.3.2 is quite long, so we break it into a series of lemmas. Let us put ourselves in the situation of Theorem 1.3.2, and let K be the fraction field of A. Let us choose a K-vector space V, such that F is an A-submodule of V. Such V does exist, because the A-module F is free of rank n (for instance, pick a basis $x_1, \dots, x_n$ of F, set $V = K^n$ and define the inclusion $F \subset V$ by mapping x_i to the i-th vector in the canonical basis of K^n). When $N \subset F$ is an A-submodule, we let $\widetilde{N}$ be the K-vector space spanned by N in V.

Lemma 1.3.6. *Let $N \subset F$ be an A-submodule. For all $x \in \widetilde{N}$, there exists a nonzero element $a \in A$ such that $ax \in N$.*

Proof. Let us write

$$x = \sum_{i=1}^{s} \lambda_i y_i, \text{ with } \lambda_1, \dots, \lambda_s \in K \text{ and } y_1, \dots, y_s \in N.$$

For $i \in \{1, \dots, s\}$, write $\lambda_i = a_i / b_i$ with $a_i, b_i \in A$. Then we may take $a = b_1 \cdots b_s$. □

For an A-submodule $N \subset F$, we define

$$r(N) = \dim_K \widetilde{N}. \tag{1.3.a}$$

Remark 1.3.7. The integer $r(N)$ is sometimes called the rank of N (even when N is not free). It is possible to give a (seemingly) more intrinsic definition using the tensor product, by setting $r(N) = \dim_K(N \otimes_A K)$. In particular, one may prove that the integer (1.3.a) is independent of the choice of V.

Lemma 1.3.8. *If the A-module N is free of rank m, then $r(N) = m$.*

Proof. Let $(e_1, \dots, e_m)$ be an A-basis of N. Then the system $(e_1, \dots, e_m) \in V^n$ certainly generates the K-vector space $\widetilde{N}$. Assume that $\lambda_1, \dots, \lambda_n \in K$ are such that

$$\sum_{i=1}^{m} \lambda_i e_i = 0 \in \widetilde{N} \subset V.$$

Letting $b \in A \smallsetminus \{0\}$ be such that $b\lambda_i \in A$ for all $i \in \{1, \dots, m\}$ (the element b is a common denominator of $\lambda_1, \dots, \lambda_m$, see the proof of Lemma 1.3.6), we thus have

$$\sum_{i=1}^{m} (b\lambda_i) e_i = 0.$$

This equality holds in $N \subset V$, hence by A-linear independence of the system $(e_1, \dots, e_m)$, we deduce that $b\lambda_1 = \cdots = b\lambda_m = 0$ in A, and thus in K. As $b \neq 0$, we obtain

$\lambda_1 = \cdots = \lambda_m = 0$ in K. We have proved that the system $(e_1, \ldots, e_m)$ is K-linearly independent. Therefore $(e_1, \ldots, e_m)$ is a K-basis of $\widetilde{N}$, and so $\dim_K \widetilde{N} = m$. □

Lemma 1.3.9. *Let N_1, N_2 be A-modules such that $N_1 \oplus N_2$ is a submodule of F. Then*

$$r(N_1 \oplus N_2) = r(N_1) + r(N_2).$$

Proof. Since the A-module $N_1 \oplus N_2$ is generated by $N_1 \cup N_2$, the K-vector space $\widetilde{N_1 \oplus N_2}$ is generated by $\widetilde{N_1} \cup \widetilde{N_2}$, and thus $\widetilde{N_1 \oplus N_2} = \widetilde{N_1} + \widetilde{N_1}$. To conclude the proof of the lemma, it will suffice to prove that $\widetilde{N_1} \cap \widetilde{N_2} = 0$ in V. If $x \in \widetilde{N_1} \cap \widetilde{N_2}$, then by Lemma 1.3.6 we may find nonzero elements $a_1, a_2 \in A$ such that $a_1 x \in N_1$ and $a_2 x \in N_2$. Setting $a = a_1 a_2$, we have $ax \in N_1 \cap N_2$. Then $ax = 0$ in F, and thus also in V. This yields $x = a^{-1} a x = 0 \in V$. □

We will denote by $\mathrm{Hom}_A(F, A)$ the set of morphisms of A-modules $F \to A$. Let us choose $\varphi \in \mathrm{Hom}_A(F, A)$ such that the subset $\varphi(M)$ is maximal (for the inclusion relation); this is possible because those subsets are ideals of A, and the ring A is noetherian (Proposition 1.2.6). As A is a principal ideal domain, we may find an element $\alpha \in A$ such that $\varphi(M) = \alpha A$.

Let us choose an A-basis $(x_1, \ldots, x_n)$ of F. Let $\pi_1, \ldots, \pi_n \in \mathrm{Hom}_A(F, A)$ be the system defined by the relations

$$\pi_i(x_j) = \delta_{ij} \quad \text{for } 1 \leq i, j \leq n,$$

where we use the *Kronecker symbol*:

$$\delta_{ij} = \begin{cases} 1 & \text{if } i = j, \\ 0 & \text{if } i \neq j. \end{cases} \tag{1.3.b}$$

Let us now assume that the A-module M is nonzero. Then we have $\pi_i(M) \neq 0$ for some $i \in \{1, \ldots, n\}$, and in particular

$$\alpha \neq 0. \tag{1.3.c}$$

Recall that by definition $\alpha A = \varphi(M)$, so let us pick an element

$$e' \in M \text{ such that } \varphi(e') = \alpha.$$

Lemma 1.3.10. *For all $\psi \in \mathrm{Hom}_A(F, A)$, we have $\psi(e') \in \alpha A$.*

Proof. As A is a principal ideal domain, the ideal of A generated by $\psi(e')$ and α in A is of the form dA, for some $d \in A$. Let us write $d = u\psi(e') + v\alpha$, with $u, v \in A$. Set $\rho = u\psi + v\varphi \in \mathrm{Hom}_A(F, A)$, so that $d = \rho(e')$. We have

$$\varphi(M) = \alpha A \subset dA = \rho(e'A) \subset \rho(M),$$

hence by maximality of φ, we deduce that $\varphi(M) = \rho(M)$, and so $\alpha A = dA$. As $\psi(e') \in dA$, the statement follows. □

Lemma 1.3.10 implies in particular that for each $i \in \{1, \ldots, n\}$, we may find an element $b_i \in A$ such that $\pi_i(e') = \alpha b_i$. Set

$$e = \sum_{i=1}^{n} b_i x_i \in F.$$

Then $e' = \alpha e$ (because their components in the basis $(x_1, \dots, x_n)$ coincide). Now

$$\alpha = \varphi(e') = \varphi(\alpha e) = \alpha\varphi(e).$$

Since the ring A is a domain, and $\alpha \neq 0$ (see (1.3.c)), this implies that

$$\varphi(e) = 1.$$

Lemma 1.3.11. *We have*

(i) $F = Ae \oplus \ker\varphi$,

(ii) $M = Ae' \oplus (M \cap \ker\varphi)$.

Proof. Every element $x \in F$ decomposes as

$$x = \varphi(x)e + (x - \varphi(x)e),$$

which shows that $F = Ae + \ker\varphi$. Let now $y \in M$. As $\varphi(M) = \alpha A$, we have $\varphi(y) = b\alpha$ for some $b \in A$. Then

$$y = be' + (y - be'),$$

which shows that $M = Ae' + (M \cap \ker\varphi)$.

Now, if $a \in A$ is such that $ae \in \ker\varphi$, then $0 = a\varphi(e) = a$, and thus $ae = 0$. This shows that $Ae \cap (\ker\varphi) = 0$. As $Ae' \cap (M \cap \ker\varphi) \subset Ae \cap (\ker\varphi)$, we also have $Ae' \cap (M \cap \ker\varphi) = 0$. □

Lemma 1.3.12. *The A-module M is free of rank r, for some integer $r \leq n$.*

Proof. Let $r = r(M)$. As $M \subset F$, we have $\widetilde{M} \subset \widetilde{F}$, and thus

$$r = r(M) = \dim_K \widetilde{M} \leq \dim_K \widetilde{F} = r(F).$$

Since $r(F) = n$ by Lemma 1.3.8, we have proved that $r \leq n$. To conclude, we prove that M is free of rank r.

We proceed by induction on the integer r. If $r = 0$, then $M = 0$ and the statement is true. Assume that $r > 0$, so that $M \neq 0$. Pick φ, α, e, e' as above. Then by Lemma 1.3.11 (ii) and Lemma 1.3.9 we have $r(M \cap \ker\varphi) = r - 1$. Therefore by induction the A-module $M \cap \ker\varphi$ is free of rank $r - 1$, and it follows from Lemma 1.3.11 (ii) that the A-module M is free of rank r. □

Proof of Theorem 1.3.2. We proceed by induction on n. The statement is clear when $n = 0$, so we assume that $n > 0$. We use the notation φ, α, e, e' given above. We know by Lemma 1.3.12, applied to the submodule $\ker\varphi \subset F$, that the A-modules $\ker\varphi$ is free of rank $m \leq n$. By Lemma 1.3.11 (i), Lemma 1.3.8 and Lemma 1.3.9, we have

$$m = r(\ker\varphi) = r(F) - 1 = n - 1.$$

Thus we may apply the inductive hypothesis to the free A-module $\ker\varphi$ and its submodule $M \cap \ker\varphi$. We obtain an A-basis $(e_2, \dots, e_n)$ of $\ker\varphi$, and nonzero elements $a_2, \dots, a_q \in A$ such that $(a_2e_2, \dots, a_qe_q)$ is an A-basis of $M \cap \ker\varphi$, and $a_i \mid a_{i+1}$ for $i = 2, \dots, q-1$. Here we may assume that $q \geq 1$. Setting $a_1 = \alpha$ and $e_1 = e$, in view of Lemma 1.3.11 we obtain that $(e_1, \dots, e_n)$ is an A-basis of F, and that $(a_1e_1, \dots, a_qe_q)$ is an A-basis of M.

If $q = 1$, this concludes the proof of Theorem 1.3.2. Let us assume that $q \geq 2$, and prove that $a_1 \mid a_2$. Consider the linear form $\xi \in \mathrm{Hom}_A(F, A)$ defined by $\xi(e_1) = \xi(e_2) = 1$ and $\xi(e_i) = 0$ for $i \in \{3, \dots, n\}$. Then $\xi(e') = \alpha$, hence $\varphi(M) = \alpha A \subset \xi(M)$. By maximality of φ, it follows that $\alpha A = \xi(M)$. As $\xi(a_2e_2) = a_2 \in \xi(M)$, we have $a_1 = \alpha \mid a_2$. This concludes the proof of Theorem 1.3.2. □

Finally, it will be convenient to record now the following complement to Theorem 1.3.2:

Proposition 1.3.13. *In the situation of Theorem 1.3.2, let K be the fraction field of A. Let $m \in \mathbb{N}$, and consider the integer $q \in \mathbb{N}$ given by Theorem 1.3.2. Then the following conditions are equivalent:*

(i) the A-module M is free of rank m,
(ii) the A-module F is a submodule of a K-vector space V, in which the set M spans a K-subspace of dimension m,
(iii) $q = m$.

Proof. (i) $\Rightarrow$ (ii): As observed above, the A-module F is always contained in some K-vector space V. The K-subspace $\widetilde{M}$ spanned by M in V has dimension $r(M)$ (see (1.3.a)), and we have $r(M) = m$ by Lemma 1.3.8.

(ii) $\Rightarrow$ (iii): The A-module M is free of rank q by Theorem 1.3.2. Using the given K-vector space V to define the integer $r(M)$, we have $r(M) = m$ by definition (see (1.3.a)), and it follows from Lemma 1.3.8 that $m = q$.

(iii) $\Rightarrow$ (i): Certainly if $(a_1e_1, \ldots, a_qe_q)$ is an A-basis of M, then M is free of rank q. □

CHAPTER 2

Integral extensions

1. Integral dependence

DEFINITION 2.1.1. Let R be a ring and $A \subset R$ a subring. An element $x \in R$ is called *integral over* A if there exist elements $a_0, \ldots, a_{n-1} \in A$ such that

$$x^n + a_{n-1}x^{n-1} + \cdots + a_0 = 0.$$

A polynomial $P \in A[X]$ whose leading term is equal to 1 will be called *monic*. Thus an element of R is integral over A if it is a zero of a monic polynomial with coefficients in A.

REMARK 2.1.2. When $A \subset R$ is a subring, every element of $a \in A$ is integral over A, being a zero of the monic polynomial $X - a$.

EXAMPLE 2.1.3. Consider the subring $\mathbb{Z} \subset \mathbb{R}$. Then $\sqrt{2}$ is integral over $\mathbb{Z}$, while $1/2$ is not.

LEMMA 2.1.4. *Let B be a ring, and A a subring. Assume that B is finitely generated as an A-module. Then every finitely generated B-module is also finitely generated as an A-module.*

PROOF. Let M be a finitely generated B-module. Let $(b_1, \ldots, b_n)$ be a finite system of generators for the A-module B, and $(m_1, \ldots, m_s)$ a finite system of generators for the B-module M. Then

$$(b_i m_j) \quad \text{for } 1 \leq i \leq n \text{ and } 1 \leq j \leq s$$

is a finite system of generators for the A-module M. □

Let R be a ring and $A \subset R$ a subring. Let $x \in R$. We will denote by $A[x] \subset R$ the A-subalgebra generated by x. This is the smallest (for the inclusion) subring of R containing A and x. Its elements are those elements of R of the form $a_n x^n + \cdots + a_0$, where $a_0, \ldots, a_n \in A$. We warn the reader that, despite the notation, the ring $A[x]$ depends on the extension $A \subset R$, and will not necessarily isomorphic to the polynomial ring in one variable over A. We will reserve the notation $A[X]$ for the polynomial ring (using capital letters for indeterminates). More generally, we will denote by $A[x_1, \ldots, x_n]$ the A-subalgebra of R generated by the elements $x_1, \ldots, x_n \in R$.

We will need the following observation:

LEMMA 2.1.5. *Let R be a ring, and elements $x_1, \ldots, x_n \in R$. Assume that $1 \in R$ is an R-linear combination of the elements $x_1, \ldots, x_n$. If $M \in M_n(R)$ is such that the column vector $(x_1, \ldots, x_n)$ lies in the kernel of M, then $\det M = 0 \in R$.*

PROOF. Consider the *adjugate matrix* N to M, i.e. the transpose of the comatrix of M (the (i,j)-th entry of the comatrix is $(-1)^{i+j}$ times the determinant of the matrix obtained from M by deleting the i-th row and j-th column). Then a basic property of the determinant (namely, the Laplace expansion) can be expressed as

$$NM = (\det M) \cdot I_n \in M_n(R),$$

where I_n is the $n \times n$ identity matrix. We deduce that for each $i \in \{1, \dots, n\}$, the element x_i is annihilated in R by the element $\det M$. Since by assumption we have

$$1 = \sum_{i=1}^{n} a_i x_i, \quad \text{for some } a_1, \dots, a_n \in R,$$

it follows that

$$\det M = (\det M) \cdot 1 = (\det M) \sum_{i=1}^{n} a_i x_i = \sum_{i=1}^{n} a_i (\det M) x_i = 0. \qquad \square$$

PROPOSITION 2.1.6. *Let R be a ring and $A \subset R$ a subring. Let $x \in R$. The following conditions are equivalent:*

(i) the element x is integral over A,
(ii) the A-module $A[x]$ is finitely generated,
(iii) the subring $A[x]$ is contained in a subring C of R, and C is finitely generated as an A-module.

PROOF. (i) $\Rightarrow$ (ii) : By assumption, we have an equation

$$x^n = -a_{n-1}x^{n-1} - \cdots - a_0, \quad \text{where } a_0, \dots, a_{n-1} \in A.$$

Multiplying with x^j for $j \geq 0$, we obtain

$$x^{n+j} = -a_{n-1}x^{n+j-1} - \cdots - a_0 x^j, \quad \text{where } a_0, \dots, a_{n-1} \in A.$$

We deduce by induction on j that x^{n+j} belongs to the A-submodule of R generated by $1, \dots, x^{n-1}$, for all $j \in \mathbb{N}$. Since $A[x]$ is the A-submodule of R generated by the elements x^i for $i \in \mathbb{N}$, we have proved that $A[x]$ is generated by $1, \dots, x^{n-1}$.

(ii) $\Rightarrow$ (iii) : Take $C = A[x]$.

(iii) $\Rightarrow$ (i) : Let $(y_1, \dots, y_n)$ be a generating system for the A-module C. As $x \in A[x] \subset C$, and C is a subring of R, we have $xy_i \in C$ for all $i \in \{1, \dots, n\}$. Therefore we may write, for each $i \in \{1, \dots, n\}$

$$xy_i = \sum_{j=1}^{n} a_{ij} y_j, \quad \text{with } a_{ij} \in A. \tag{2.1.a}$$

So we have equations in R, for $i = 1, \dots, n$

$$\sum_{j=1}^{n} (\delta_{ij} x - a_{ij}) y_j = 0, \tag{2.1.b}$$

where δ_{ij} is the Kronecker symbol (see (1.3.b)).

Consider the $n \times n$ matrix $M \in M_n(R)$, whose coefficients are $\delta_{ij}x - a_{ij} \in R$. Then (2.1.b) expresses the fact that the column vector $(y_1, \dots, y_n) \in R^n$ lies in the kernel of M. In addition 1 is an A-linear combination of the elements $y_1, \dots, y_n$, as is any element of

C by the choice of the family $y_1, \dots, y_n$. Therefore by Lemma 2.1.5, we have $\det M = 0$. Expanding the determinant $\det M$, we obtain

$$0 = \det M = x^n + a_{n-1}x^{n-1} + \cdots + a_0, \quad \text{where } a_0, \dots, a_{n-1} \in A.$$

(If $P \in A[X]$ is the characteristic polynomial of the matrix $(a_{ij}) \in M_n(A)$, then $\det M = P(x) \in R$, and $1, a_{n-1}, \dots, a_0$ are the coefficients of P.) This is the required equation of integral dependence to prove that x is integral over A. □

COROLLARY 2.1.7. *Let R be a ring, and $A \subset R$ a subring. If $x_1, \dots, x_n \in R$ are all integral over A, then the A-module $A[x_1, \dots, x_n]$ is finitely generated.*

PROOF. We proceed by induction on n, the case $n = 0$ being Remark 2.1.2. Assume that $n \geq 1$. Set $A' = A[x_1, \dots, x_{n-1}]$. Then by induction the A-module A' is finitely generated. Since x_n is integral over A, it is also integral over A' (because $A \subset A'$). Therefore by the implication (i) $\Rightarrow$ (ii) in Proposition 2.1.6, the A'-module $A'[x_n] = A[x_1, \dots, x_n]$ is finitely generated. We conclude using Lemma 2.1.4 that the A-module $A[x_1, \dots, x_n]$ is finitely generated. □

PROPOSITION 2.1.8. *Let R be a ring and $A \subset R$ a subring. If $x, y \in R$ are both integral over A, then so are xy and $x + y$.*

PROOF. By Corollary 2.1.7, the subring $A[x, y] \subset R$ is finitely generated as an A-module. For $z \in \{xy, x+y\}$, the subring $A[z]$ is contained in $A[x, y]$, and so the statement follows from the implication (iii) $\Rightarrow$ (i) in Proposition 2.1.6. □

DEFINITION 2.1.9. Let R be a ring, and $A \subset R$ a subring. By Proposition 2.1.8 and Remark 2.1.2, the set of elements of R which are integral over A is a subring of R which contains A, called the *integral closure of A in R*. If A coincides with its integral closure in R, we say that A is *integrally closed* in R.

When A is a domain, the integral closure of A in its fraction field K is simply called the integral closure of A, and we say that A is integrally closed when it coincides with its integral closure.

DEFINITION 2.1.10. A *number field* is a field extension of $\mathbb{Q}$ having finite degree. When K is a number field, the integral closure of $\mathbb{Z}$ in K is called the *ring of integers* of K, and will be denoted by $\mathcal{O}_K \subset K$.

PROPOSITION 2.1.11. *Every principal ideal domain is integrally closed.*

PROOF. Let A be a principal ideal domain, with fraction field K. Let $x \in K$ be integral over A. So we have an equation in K

$$x^n + a_{n-1}x^{n-1} + \cdots + a_0 = 0, \tag{2.1.c}$$

with $a_0, \dots, a_{n-1} \in A$. Now we find elements $a, b \in A$ with $b \neq 0$ such that $x = ab^{-1}$. The ideal $aA + bA$ in the principal ideal domain A must be of the form dA, for some $d \in A$. In particular $a = da'$ and $b = db'$ for some $a', b' \in A$. Replacing (a, b) with (a', b'), we may assume that $d = 1$, which means that there exist $u, v \in A$ such that $au + bv = 1$. Multiplying (2.1.c) with b^n and using the relation $bx = a$, we obtain in $A \subset K$

$$a^n + a_{n-1}ba^{n-1} + \cdots + a_0b^n = 0,$$

and therefore

$$a^n = b(-a_{n-1}a^{n-1} - \cdots - a_0b^{n-1}).$$

Thus b divides a^n. It follows that b divides

$$a^n u^n = (au)^n = (1 - bv)^n = 1 \mod bA,$$

and thus b divides 1, which means that $b \in B^\times$. This implies that $a = ab^{-1} \in A \subset K$. □

Remark 2.1.12. In particular, it follows from Proposition 2.1.11 that the domain $\mathbb{Z}$ is integrally closed (in $\mathbb{Q}$), a fact the will be used repeatedly.

Definition 2.1.13. Let R be a ring, and $A \subset R$ a subring. If every element of R is integral over A, we say that R is *integral over* A, or that the extension $A \subset R$ is integral.

Example 2.1.14. Let k be a field and A a nonzero k-algebra. Then we claim that the associated morphism $\varphi\colon k \to A$ (mapping $\lambda \in k$ to $\lambda \cdot 1 \in A$) is injective. Indeed its kernel is an ideal of k, and there are only two such ideals in the field k, namely 0 and k. As 1 belongs to the image of φ, and $1 \neq 0$ as A is nonzero, the kernel of φ can only be zero. This proves the claim.

If in addition, the k-vector space A has finite dimension, then A is integral over k, by the second criterion of Proposition 2.1.6.

Proposition 2.1.15. *Let C be a ring, and $A \subset B \subset C$ subrings. If B is integral over A and C is integral over B, then C is integral over A.*

Proof. Let $x \in C$. As C is integral over B, we can find elements $b_0, \dots, b_{n-1} \in B$ such that

$$0 = x^n + b_{n-1}x^{n-1} + \cdots + b_0. \tag{2.1.d}$$

Let $A' = A[b_0, \dots, b_{n-1}] \subset B$. As B is integral over A, the elements $b_0, \dots, b_{n-1}$ are integral over A. Therefore by Corollary 2.1.7, the A-module A' is finitely generated. On the other hand, the relation (2.1.d) shows that x is integral over A', so that by the implication (i) ⇒ (ii) in Proposition 2.1.6 the A'-module $A'[x]$ is finitely generated. We conclude using Lemma 2.1.4 that the A-module $A'[x]$ is finitely generated. Since $A[x] \subset A'[x]$ it follows from the implication (iii) ⇒ (i) in Proposition 2.1.6 that x is integral over A. □

Remark 2.1.16. Let R be a ring and $A \subset R$ a subring. It follows from Proposition 2.1.15 that the integral closure of A in R is integrally closed in R.

Lemma 2.1.17. *Let $A \subset R$ be a subring, and $\sigma\colon R \to S$ a ring morphism. Consider the subring $B = \sigma(A) \subset S$. If $x \in R$ is integral over A, then $\sigma(x) \in S$ is integral over B.*

Proof. If $P \in A[X]$ is a monic polynomial such that $P(x) = 0$, then its image $Q = \sigma(P) \in B[X]$ is a monic polynomial such that $Q(\sigma(x)) = 0$. □

Lemma 2.1.18. *Let $A \subset R$ be an integral ring extension. Then for any ideal J of R, the ring extension $A/(J \cap A) \subset R/J$ is integral.*

Proof. Consider the quotient morphism $\sigma\colon R \to R/J$. Then any element $y \in R/J$ is the image of some element $x \in R$ under σ. The element x is integral over A by assumption, hence it follows from Lemma 2.1.17 that $\sigma(x) = y$ is integral over $\sigma(A) = A/(J \cap A) \subset R/J$. □

Lemma 2.1.19. *Let $A \subset R$ be an integral ring extension. Assume that the ring R is a domain. Then for any nonzero ideal J of R, the ideal $J \cap A$ of A is nonzero.*

PROOF. Let $x \in J$ be a nonzero element. Since x is integral over A, we have

$$x^n + a_{n-1}x^{n-1} + \cdots + a_0 = 0, \quad \text{for some } a_0, \ldots, a_{n-1} \in A.$$

We may arrange that the integer $n \in \mathbb{N} \smallsetminus \{0\}$ is minimal among those appearing in such an equation (i.e. the integer n is the minimal degree of a monic polynomial with coefficients in A admitting x as a zero). If $a_0 = 0$, as R is a domain and $x \neq 0$, we obtain an equation

$$x^{n-1} + a_{n-1}x^{n-2} + \cdots + a_1 = 0,$$

which contradicts the minimality of the integer n. We thus have $a_0 \neq 0$. Then

$$a_0 = x(-x^{n-1} - a_{n-2}x^{n-2} - \cdots - a_1) \in xR \subset J$$

is a nonzero element of $J \cap A$. □

PROPOSITION 2.1.20. *Let $A \subset R$ be an integral ring extension. Assume that R is a domain. Then R is a field if and only if A is a field.*

PROOF. Assume that R is a field. Let $x \in A$. Then by assumption the element $x^{-1} \in R$ is integral over A, hence satisfies an equation of the form

$$x^{-n} + a_{n-1}x^{1-n} + \cdots + a_0 = 0,$$

with $a_0, \ldots, a_{n-1} \in A$. Multiplying with x^{1-n}, we obtain

$$x^{-1} = -a_{n-1} - \cdots - a_0 x^{n-1} \in R,$$

which visibly belongs to A. We have proved that A is a field.

Recall that a domain D is a field if and only if its only ideals are $0, D$. Assume that A is a field, and let J be a nonzero ideal of R. Then the ideal $I = J \cap R$ of A is nonzero by Lemma 2.1.19. As A is a field, we must have $I = A$. Then $1 \in J \cap A \subset J$, hence $J = R$. We have proved that R is a field. □

COROLLARY 2.1.21. *Let k be a field, and A a finite-dimensional k-algebra. Then every prime ideal of A is maximal.*

PROOF. Let $\mathfrak{p}$ be a prime ideal of A. Then the ring $A/\mathfrak{p}$ is nonzero by definition of a prime ideal, so that the ring morphism $k \to A/\mathfrak{p}$ is injective, and makes the ring $A/\mathfrak{p}$ integral over k (see Example 2.1.14). Therefore the ring $A/\mathfrak{p}$ is a field by Proposition 2.1.20, which means that the ideal $\mathfrak{p}$ is maximal. □

2. Integers in quadratic fields

When $\alpha \in \mathbb{C}$ and $K \subset \mathbb{C}$ is a subfield, we denote by $K(\alpha)$ the subset of $\mathbb{C}$ consisting of the elements $P(\alpha)/Q(\alpha)$, with $P, Q \in K[X]$, and $Q(\alpha) \neq 0$. Then $K(\alpha)$ is the smallest subfield of $\mathbb{C}$ containing α and K. When α is algebraic over K, then we have $K(\alpha) = K[\alpha]$.

DEFINITION 2.2.1. A *quadratic field* is a field extension of degree 2 of the field of rational numbers $\mathbb{Q}$. A quadratic field is called *real* if it admits an embedding into $\mathbb{R}$ as a subfield, and *imaginary* otherwise.

Examples of quadratic fields include the fields $\mathbb{Q}(\sqrt{d})$, where $d \in \mathbb{Z}$ is not a square.[1] This quadratic field is real if $d > 0$ and imaginary if $d < 0$.

[1] By $\sqrt{d}$ we denote one of the two elements of $\mathbb{C}$ whose square is d; this choice does not affect the field $\mathbb{Q}(\sqrt{d}) = \mathbb{Q}(-\sqrt{d})$.

We will say that an integer $d \in \mathbb{Z}$ is *square-free* when 1 is the only square dividing d. An equivalent condition is that either d or $-d$ can be written as a product of pairwise distinct primes.

Proposition 2.2.2. *Every quadratic field is isomorphic to $\mathbb{Q}(\sqrt{d})$ for some $d \in \mathbb{Z} \smallsetminus \{1\}$, where d is square-free.*

Proof. Let K be a quadratic field. Pick an element $x \in K \smallsetminus \mathbb{Q}$. Then x generates K as a $\mathbb{Q}$-algebra. Its minimal polynomial has degree 2 (its degree is at most 2 because $\dim_{\mathbb{Q}} K = 2$, and is not equal to 1 because $x \notin K$), hence we have an equation of the form

$$x^2 + bx + c = 0 \in \mathbb{Q}[X], \quad \text{with } b, c \in \mathbb{Q}. \tag{2.2.a}$$

Let $e = b^2 - 4c \in \mathbb{Q}$. Then (2.2.a) implies that

$$(2x + b)^2 = e.$$

In particular $\sqrt{e} \in K$, and moreover

$$x \in \left\{ \frac{-b + \sqrt{e}}{2}, \frac{-b - \sqrt{e}}{2} \right\} \subset \mathbb{Q}(\sqrt{e}).$$

We deduce that $K = \mathbb{Q}(\sqrt{e})$. Writing $e = u/v$ with $u, v \in \mathbb{Z}$, the element $f = v^2 e$ belongs to $\mathbb{Z}$. Then f may be written as $f = dg^2$, where $g \in \mathbb{Z}$ and d is square-free. Then $d = (v/g)^2 e$, so that $\mathbb{Q}(\sqrt{e}) = \mathbb{Q}(\sqrt{d})$. Note that the case $d = 1$ is excluded, as then $\mathbb{Q}(\sqrt{d}) = \mathbb{Q}$ is not a quadratic field. □

Theorem 2.2.3. *Let K be a quadratic field, and write $K = \mathbb{Q}(\sqrt{d})$ where $d \in \mathbb{Z} \smallsetminus \{1\}$ is square-free (see Proposition 2.2.2), and in particular $d \neq 0 \mod 4$. Then a $\mathbb{Z}$-basis of the ring of integers $\mathcal{O}_K$ (see Definition 2.1.10) is given by*

$$\begin{cases} (1, \sqrt{d}) & \text{if } d \text{ is congruent to } 2 \text{ or } 3 \text{ modulo } 4, \\ \left(1, \dfrac{1 + \sqrt{d}}{2}\right) & \text{if } d \text{ is congruent to } 1 \text{ modulo } 4. \end{cases}$$

Proof. The $\mathbb{Q}$-algebra K is isomorphic to $\mathbb{Q}[X]/(X^2 - d)$. In particular, every element of K is of the form $a + b\sqrt{d}$, for unique elements $a, b \in \mathbb{Q}$. Moreover, the morphism of $\mathbb{Q}$-algebras $\mathbb{Q}[X]/(X^2 - d) \to \mathbb{Q}[X]/(X^2 - d)$ given by $X \mapsto -X$ yields a morphism of $\mathbb{Q}$-algebras

$$\sigma \colon K \to K, \quad a + b\sqrt{d} \mapsto a - b\sqrt{d} \quad (\text{where } a, b \in \mathbb{Q}).$$

It follows that $\mathbb{Q} \subset K$ is the subset of elements fixed by the endomorphism $\sigma \colon K \to K$. In particular for any $x \in K$, the elements $x + \sigma(x)$ and $x\sigma(x)$ belong to $\mathbb{Q}$. If $x \in \mathcal{O}_K$, then $\sigma(x) \in \mathcal{O}_K$ by Lemma 2.1.17, and therefore (by Proposition 2.1.8) the elements $x + \sigma(x)$ and $x\sigma(x)$ are integral over $\mathbb{Z}$. Since $\mathbb{Z}$ is integrally closed (in $\mathbb{Q}$) by Remark 2.1.12, we deduce that $x + \sigma(x) \in \mathbb{Z}$ and $x\sigma(x) \in \mathbb{Z}$. In other words, if $a, b \in \mathbb{Q}$ are the elements such that $x = a + b\sqrt{d}$, we have

$$2a \in \mathbb{Z} \quad \text{and} \quad a^2 - db^2 \in \mathbb{Z}. \tag{2.2.b}$$

Conversely, assume that $a, b \in \mathbb{Q}$ satisfy the conditions given in (2.2.b). Then the element $a + b\sqrt{d} \in K$ is a root of the monic polynomial

$$X^2 - 2aX + (a^2 - db^2) \in \mathbb{Z}[X],$$

hence belongs to $\mathcal{O}_K$. We have proved that, for any $a, b \in \mathbb{Q}$

$$a + b\sqrt{d} \in \mathcal{O}_K \iff \text{(2.2.b)}.$$

Now the condition (2.2.b) implies that $4db^2 \in \mathbb{Z}$. Writing $2b = f/g$ with $f, g \in \mathbb{Z}$ relatively prime, we have $df^2 \in g^2\mathbb{Z}$, and so $d \in g^2\mathbb{Z}$ (as f^2 is prime to g^2). As d is square-free, we must have $g^2 = 1$, which implies that $2b \in \mathbb{Z}$. Therefore we may write $a = u/2$ and $b = v/2$ with $u, v \in \mathbb{Z}$, and The condition (2.2.b) becomes

$$u^2 - dv^2 \in 4\mathbb{Z}. \tag{2.2.c}$$

If u is even, the condition (2.2.c) implies that v is also even (recall that d is not divisible by 4, being square-free); then we have $a, b \in \mathbb{Z}$. If u is odd, then $u^2 = 1 \mod 4$ and thus (2.2.c) implies that

$$dv^2 = 1 \mod 4. \tag{2.2.d}$$

Thus the integer v^2 is not divisible by 4, and as observed in (0.a) this implies that $v^2 = 1 \mod 4$. In particular v is odd, and moreover the relation (2.2.d) implies that $d = 1 \mod 4$.

Conversely, assume that $d = 1 \mod 4$. If $u, v \in \mathbb{Z}$ have the same parity, then $u^2 - dv^2 = u^2 - v^2$ is divisible by 4 (see (0.a)), and so (2.2.c) holds. We have proved that

$$\mathcal{O}_K = \begin{cases} \{a + b\sqrt{d}, \text{ where } a, b \in \mathbb{Z}\} & \text{if } d = 2, 3 \mod 4, \\ \left\{ \dfrac{u + v\sqrt{d}}{2}, \text{ where } u, v \in \mathbb{Z} \text{ and } u = v \mod 2 \right\} & \text{if } d = 1 \mod 4. \end{cases}$$

The system $(1, \sqrt{d})$, resp. $(1, (1+\sqrt{d})/2)$, is $\mathbb{Z}$-linearly independent in K (being $\mathbb{Q}$-linearly independent), and is contained in $\mathcal{O}_K$ when d is congruent to 2 or 3 modulo 4, resp. 1 modulo 4. If $u, v \in \mathbb{Z}$ have the same parity, then

$$\frac{u + v\sqrt{d}}{2} = \frac{u - v}{2} + v\frac{1 + \sqrt{d}}{2}$$

is a $\mathbb{Z}$-linear combination of 1 and $(1 + \sqrt{d})/2$. This concludes the proof of the statement. □

CHAPTER 3

Trace, norm and discriminant

1. The characteristic polynomial

In this section, we consider a ring B and a subring $A \subset B$. We assume that the A-module B is free of rank $n \in \mathbb{N}$, in other words that there exists an isomorphism of A-modules $B \simeq A^{\oplus n}$.

DEFINITION 3.1.1. Let $b \in B$. Consider the morphism of A-modules

$$l_b \colon B \to B, \quad x \mapsto bx.$$

The *characteristic polynomial* of b is the polynomial[1]

$$\chi_{B/A}(b) = \det(X \operatorname{id}_B - l_b) \in A[X].$$

Observe that $\chi_{B/A}(b)$ is a monic polynomial of degree n with coefficients in A.

LEMMA 3.1.2. *If $\alpha \colon B \xrightarrow{\sim} B'$ is an isomorphism of A-algebras, then for any $b \in B$ we have*

$$\chi_{B/A}(b) = \chi_{B'/A}(\alpha(b)).$$

PROOF. Indeed we have $l_{\alpha(b)} = \alpha \circ l_b \circ \alpha^{-1}$, and the lemma follows from a standard property of the determinant. □

We recall that a element x of a ring R is called nilpotent if there exists an integer $n \in \mathbb{N}$ such that $x^n = 0$.

PROPOSITION 3.1.3. *Assume that the ring A is a domain. If $b \in B$ is a nilpotent element, then $\chi_{B/A}(b) = X^n$.*

PROOF. Assume that $b^{k+1} = 0$. Let $\varphi = l_b$, so that $\varphi^{k+1} = 0$. We have

$$(X \operatorname{id}_B - \varphi)(X^k \operatorname{id}_B + \varphi x^{k-1} + \cdots + \varphi^k) = X^{k+1} \operatorname{id}_B .$$

Taking the determinants, we deduce that $\chi_{B/A}(b) = \det(X \operatorname{id}_B - \varphi)$ divides $\det(X^{k+1} \operatorname{id}_B) = X^{n(k+1)}$. We conclude the proof using Lemma 3.1.4 below. □

LEMMA 3.1.4. *Let A be a domain, and $q \in \mathbb{N}$. Then the only monic polynomials dividing X^n in $A[X]$ are the polynomials X^k for $k \leq q$.*

PROOF. Assume that $X^q = PQ$ with $P, Q \in A[X]$. Then we may write

$$P = X^m(p_r X^r + \cdots + p_0) \quad \text{and} \quad P = X^{m'}(q_s X^s + \cdots + q_0),$$

where $p_0, \ldots, p_r, q_0, \ldots, q_s \in A$, and moreover $p_0 \neq 0$ and $q_0 \neq 0$. Then the $(X^{m+m'})$-coefficient of PQ is $p_0 q_0$. If either P or Q is not a power of X (i.e. if $r + s > 0$), we must

[1] We commit a slight abuse of notation, and use the same notation of endomorphisms of the A-module B and the induced endomorphisms of the $A[X]$-module $B[X]$.

have $p_0 q_0 = 0$ (because $PQ = X^q = X^{m+m'+r+s}$). Since the ring A is a domain, this implies that $p_0 = 0$ or $q_0 = 0$, a contradiction. □

Lemma 3.1.5. *Let B_1, B_2 be rings such that $A \subset B_1$ and $A \subset B_2$. Assume that B_1, B_2 are free of respective ranks $n_1, n_2 \in \mathbb{N}$ as A-modules. Then the A-algebra $B_1 \times B_2$ is free of rank $n_1 + n_2$ as an A-module, and for any $b_1 \in B_2$ and $b_2 \in B_2$, we have*

$$\chi_{(B_1 \times B_2)/A}((b_1, b_2)) = \chi_{B_1/A}(b_1) \cdot \chi_{B_2/A}(b_2).$$

Proof. If $(e_1, \dots, e_{n_1})$ is an A-basis of B_1 and $(f_1, \dots, f_{n_2})$ an A-basis of B_2, then

$$((e_1, 0), \dots, (e_{n_1}, 0), (0, f_1), \dots, (0, f_{n_2})) \tag{3.1.a}$$

is an A-basis of $B_1 \times B_2$. Let $M_1 \in M_{n_1}(A), M_2 \in M_{n_2}(A)$ be the matrices of l_{b_1}, l_{b_2} in the above basis of B_1, B_2. Then the matrix of $l_{(b_1, b_2)}$ in the basis (3.1.a) of $B_1 \times B_2$ is the block matrix

$$M = \begin{pmatrix} M_1 & 0 \\ 0 & M_2 \end{pmatrix} \in M_{n_1+n_2}(A)$$

and the properties of determinant of block matrices show that, denoting by $I_k \in M_k(A)$ the identity matrix,

$$\det(XI_{n_1+n_2} - M) = \det(XI_{n_1} - M_1) \cdot \det(XI_{n_2} - M_2),$$

which gives the required formula. □

Proposition 3.1.6 (Cayley–Hamilton Theorem). *For any $b \in B$ we have*

$$\big(\chi_{B/A}(b)\big)(b) = 0.$$

Proof. Let $(e_1, \dots, e_n)$ be an A-basis of B. Let us write for $i = 1, \dots, n$

$$be_i = \sum_{j=1}^{n} b_{ij} e_j, \quad \text{with } b_{ij} \in A. \tag{3.1.b}$$

Then $(b_{ij}) \in M_n(A)$ is the matrix of the endomorphism l_b in the above A-basis of B. Let us consider the matrix (using the notation of (1.3.b))

$$N = (\delta_{ij} b - b_{ij}) \in M_n(B).$$

The equation (3.1.b) asserts that the column vector $(e_1, \dots, e_n) \in B^n$ belongs to the kernel of N. Since $(e_1, \dots, e_n)$ is an A-basis of B, the element 1 is an A-linear combination of the elements $e_1, \dots, e_n$, and in particular a B-linear combination of those. It thus follows from Lemma 2.1.5 that $\det N = 0 \in B$. On the other hand, we have

$$\chi_{B/A}(b) = \det(\delta_{ij} X - b_{ij}) \in A[X].$$

This formula also holds in $B[X]$ (here we use that the following fact: if $M \in M_n(A[X])$ has image $M' \in M_n(B[X])$, then $\det M' \in B[X]$ is the image of $\det M \in A[X]$). Evaluating at $b \in B$ shows that $\chi_{B/A}(b)(b) = \det N \in B$, and we have seen above that this element vanishes. □

Two particular coefficients of the characteristic polynomial will be especially significant:

DEFINITION 3.1.7. We define the *norm* and *trace* of an element $b \in B$ as the determinant and trace of the endomorphism l_b of the free A-module B of rank n (see Definition 3.1.1):

$$\mathrm{N}_{B/A}(b) = \det(l_b) \in A \quad \text{and} \quad \mathrm{Tr}_{B/A}(b) = \mathrm{Tr}(l_b) \in A.$$

LEMMA 3.1.8. *For $b \in B$, let us write*

$$\chi_{B/A}(b) = X^n + a_{n-1}X^{n-1} + \cdots + a_0 \in A[X],$$

where $a_0, \ldots, a_{n-1} \in A$. Then

$$\mathrm{N}_{B/A}(b) = (-1)^n a_0 \quad \textit{and} \quad \mathrm{Tr}_{B/A}(b) = -a_{n-1}.$$

PROOF. Let us choose a basis of the A-module B consisting of n elements of B, and denote by $b_{ij} \in A$ the coefficients of the matrix of the endomorphism l_b in that basis. Then (using the notation of (1.3.b))

$$\chi_{B/A}(b) = \det(\delta_{ij}X - b_{ij}) \in A[X].$$

Then we set $m_{ij} = \delta_{ij}X - b_{ij} \in A[X]$, and consider the formula (where $\mathfrak{S}_n$ denotes the symmetric group on n elements, and $\mathrm{sgn}\colon \mathfrak{S}_n \to \{1, -1\}$ is the signature morphism)

$$\det(m_{ij}) = \sum_{\sigma \in \mathfrak{S}_n} \mathrm{sgn}(\sigma) m_{1\sigma(1)} \cdots m_{n\sigma(n)} \in A[X]. \tag{3.1.c}$$

This polynomial has constant coefficient

$$\sum_{\sigma \in \mathfrak{S}_n} \mathrm{sgn}(\sigma)(-b_{1\sigma(1)}) \cdots (-b_{n\sigma(n)}) = (-1^n)\det(b_{ij}) \in A.$$

In the formula (3.1.c), the term $\mathrm{sgn}(\sigma)m_{1\sigma(1)} \cdots m_{n\sigma(n)}$ can contribute to the X^{n-1}-coefficient only when $\sigma(i) = i$ for at least $n-1$ values of $i \in \{1, \ldots, n\}$, in which case we must also have $\sigma(i) = i$ for the single remaining value of i, and so $\sigma = \mathrm{id}$. Therefore the X^{n-1}-coefficient of (3.1.c) coincides with the X^{n-1}-coefficient of the polynomial

$$\prod_{i=1}^{n} m_{ii} = \prod_{i=1}^{n} (X - b_{ii}) \in A[X],$$

and is thus equal to

$$\sum_{i=1}^{n} (-b_{ii}) = -\mathrm{Tr}(l_b) \in A. \qquad \square$$

PROPOSITION 3.1.9. *The following hold:*

(i) We have

$$\mathrm{Tr}_{B/A}(0) = 0 \quad \textit{and} \quad \mathrm{N}_{B/A}(1) = 1.$$

(ii) For any $x, y \in B$, we have

$$\mathrm{Tr}_{B/A}(x+y) = \mathrm{Tr}_{B/A}(x) + \mathrm{Tr}_{B/A}(y) \quad \textit{and} \quad \mathrm{N}_{B/A}(xy) = \mathrm{N}_{B/A}(x)\,\mathrm{N}_{B/A}(y).$$

(iii) For any $a \in A$, we have $\chi_{B/A}(a) = (X-a)^n$. In particular

$$\mathrm{Tr}_{B/A}(a) = na \quad \textit{and} \quad \mathrm{N}_{B/A}(a) = a^n.$$

PROOF. (i) and (ii) are clear from the definitions.

(iii) : This follows from the fact that, in any A-basis of B, the matrix of $l_a\colon B \to B$ is diagonal with coefficients $(a, \ldots, a)$. $\square$

Lemma 3.1.10. *For any $b \in B$, we have*

$$b \in B^\times \iff \mathrm{N}_{B/A}(b) \in A^\times.$$

Proof. It follows from Proposition 3.1.9 (i) and (ii) that $\mathrm{N}_{B/A}(b) \in A^\times$ when $b \in B^\times$. Conversely if $\mathrm{N}_{B/A}(b) \in A^\times$, the morphism of A-modules $l_b \colon B \to B$ has invertible determinant, hence is bijective. Its surjectivity yields an element $c \in B$ such that $bc = 1$, which shows that $b \in B^\times$. □

Remark 3.1.11. It follows from Proposition 3.1.9 and Lemma 3.1.10 that the norm map induces a group morphism

$$\mathrm{N}_{B/A} \colon B^\times \to A^\times.$$

2. The discriminant

In this section B will be a ring and $A \subset B$ a subring such that the A-module B is free of rank $n \in \mathbb{N}$.

Definition 3.2.1. The *discriminant* of a system $(x_1, \dots, x_n) \in B^n$ is defined as the element

$$\mathrm{D}_{B/A}(x_1, \dots, x_n) = \det(\mathrm{Tr}_{B/A}(x_i x_j)) \in A,$$

where (i, j) runs over $\{1, \dots, n\}^2$.

Lemma 3.2.2. *Assume that $(e_1, \dots, e_n)$ is an A-basis of B. Let $\varphi \colon B \to B$ be a morphism of A-modules. Then*

$$\mathrm{D}_{B/A}(\varphi(e_1), \dots, \varphi(e_n)) = (\det \varphi)^2 \cdot \mathrm{D}_{B/A}(e_1, \dots, e_n).$$

Proof. Let us denote by $a_{ij} \in A$ for $1 \leq i, j \leq n$ the coefficients of the matrix of φ in the basis $(e_1, \dots, e_n)$. Then

$$\mathrm{Tr}(\varphi(e_i)\varphi(e_j)) = \mathrm{Tr}\Big(\Big(\sum_{p=1}^n a_{pi} e_p\Big)\Big(\sum_{q=1}^n a_{qj} e_q\Big)\Big) = \sum_{p,q=1}^n a_{pi} a_{qj} \,\mathrm{Tr}(e_p e_q).$$

We thus have equalities between matrices in $M_n(A)$

$$(\mathrm{Tr}(\varphi(e_i)\varphi(e_j))) = (a_{pi}) \cdot (\mathrm{Tr}(e_p e_q)) \cdot {}^t(a_{qj}),$$

where ${}^tM$ denotes the transpose of the matrix M. Taking determinants yields the statement (as transposing a matrix does not change its determinant). □

Definition 3.2.3. The *discriminant ideal* $\mathfrak{D}_{B/A}$ is defined as the ideal of A generated by the elements $\mathrm{D}_{B/A}(x_1, \dots, x_n)$, where $(x_1, \dots, x_n)$ runs over B^n.

Lemma 3.2.4. *If $\alpha \colon B \xrightarrow{\sim} B'$ is an isomorphism of A-algebras, then $\mathfrak{D}_{B'/A} = \mathfrak{D}_{B/A}$.*

Proof. Consider a system $(x_1, \dots, x_n) \in B^n$. It follows from Lemma 3.1.2 that, for any $i, j \in \{1, \dots, n\}$

$$\mathrm{Tr}_{B/A}(x_i x_j) = \mathrm{Tr}_{B'/A}(\alpha(x_i x_j)) = \mathrm{Tr}_{B'/A}(\alpha(x_i)\alpha(x_j)).$$

Taking the determinants of the matrices whose coefficients are displayed in the above equation shows that

$$\mathrm{D}_{B/A}(x_1, \dots, x_n) = \mathrm{D}_{B'/A}(\alpha(x_1), \dots, \alpha(x_n)).$$

This implies that $\mathfrak{D}_{B/A} \subset \mathfrak{D}_{B'/A}$. Applying this reasoning to the inverse morphism $\alpha^{-1} \colon B' \to B$ shows that $\mathfrak{D}_{B/A} \subset \mathfrak{D}_{B'/A}$. □

Proposition 3.2.5. *Assume that $\mathfrak{D}_{B/A} \neq 0$ and that the ring A is a domain. Then a system $(x_1, \dots, x_n) \in B^n$ is an A-basis of B if and only if the element $\mathrm{D}_{B/A}(x_1, \dots, x_n)$ generates the ideal $\mathfrak{D}_{B/A}$ in A.*

Proof. Let $(e_1, \dots, e_n)$ be an A-basis of B. Then there exists an A-linear map $\varphi\colon B \to B$ such that $\varphi(e_i) = x_i$ for all $i \in \{1, \dots, n\}$, and by Lemma 3.2.2 we have

$$\mathrm{D}_{B/A}(x_1, \dots, x_n) = (\det \varphi)^2 \cdot \mathrm{D}_{B/A}(e_1, \dots, e_n). \tag{3.2.a}$$

As $(\det \varphi)^2 \in A$, this implies that the element $\mathrm{D}_{B/A}(e_1, \dots, e_n)$ generates the ideal $\mathfrak{D}_{B/A}$ in A, proving one implication.

Now let $d = \mathrm{D}_{B/A}(x_1, \dots, x_n)$, and assume that d generates the ideal $\mathfrak{D}_{B/A}$ in A. Then $\mathrm{D}_{B/A}(e_1, \dots, e_n) = ad$ for some $a \in A$, hence (3.2.a) yields $d = (\det \varphi)^2 ad$. Now $d \neq 0$ (because by the ideal $\mathfrak{D}_{B/A}$ is nonzero by assumption), and as A is assumed to be a domain, we deduce that $1 = (\det \varphi)^2 a$. Therefore the element $\det \varphi$ is invertible in A. Thus φ is an isomorphism of A-modules, and so $(x_1, \dots, x_n)$ is an A-basis of B, being the image under φ of an A-basis of B. □

The following complement is sometimes useful to study integers in number fields:

Lemma 3.2.6. *Assume that $A = \mathbb{Z}$, and let $(x_1, \dots, x_n) \in B^n$ be a system such that the integer $\mathrm{D}_{B/\mathbb{Z}}(x_1, \dots, x_n) \in \mathbb{Z}$ is square-free. Then $(x_1, \dots, x_n)$ is a $\mathbb{Z}$-basis of B.*

Proof. Indeed, let $(e_1, \dots, e_n)$ be a $\mathbb{Z}$-basis of B. Then there exists a morphism of $\mathbb{Z}$-modules $\varphi\colon B \to B$ such that $\varphi(e_i) = x_i$ for each $i \in \{1, \dots, n\}$. By Lemma 3.2.2 we have

$$\mathrm{D}_{B/\mathbb{Z}}(x_1, \dots, x_n) = \det(\varphi)^2 \cdot \mathrm{D}_{B/\mathbb{Z}}(e_1, \dots, e_n).$$

As this integer is assumed to be square-free, we must have $\det(\varphi) \in \{1, -1\} = \mathbb{Z}^\times$, and thus φ is an isomorphism. This implies that $(x_1, \dots, x_n)$ is a $\mathbb{Z}$-basis of B. □

Remark 3.2.7. Lemma 3.2.6 merely provides a sufficient condition for a given system to be a $\mathbb{Z}$-basis, which is not always necessary, as shown by Example 3.2.8 below.

Example 3.2.8. Let $K = \mathbb{Q}(\sqrt{d})$, with $d \in \mathbb{Z} \smallsetminus \{1\}$ square-free. We set $A = \mathbb{Z}$ and $B = \mathcal{O}_K$. Let us compute the discriminant d_K of the $\mathbb{Z}$-basis of $\mathcal{O}_K$ given by Theorem 2.2.3.

Assume that d is congruent to 2 or 3 modulo 4. Then a $\mathbb{Z}$-basis of $\mathcal{O}_K$ is given by $(x_1, x_2) = (1, \sqrt{d})$. We have

$$\mathrm{Tr}(l_1) = \mathrm{Tr}\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = 2, \quad \mathrm{Tr}(l_{\sqrt{d}}) = \mathrm{Tr}\begin{pmatrix} 0 & d \\ 1 & 0 \end{pmatrix} = 0, \quad \mathrm{Tr}(l_d) = \mathrm{Tr}\begin{pmatrix} d & 0 \\ 0 & d \end{pmatrix} = 2d,$$

so that

$$\mathrm{Tr}_{\mathcal{O}_K/\mathbb{Z}}(x_i x_j) = \begin{pmatrix} \mathrm{Tr}(l_1) & \mathrm{Tr}(l_{\sqrt{d}}) \\ \mathrm{Tr}(l_{\sqrt{d}}) & \mathrm{Tr}(l_d) \end{pmatrix} = \begin{pmatrix} 2 & 0 \\ 0 & 2d \end{pmatrix}.$$

Taking determinants we obtain $d_K = 4d$.

Assume now that $d = 1 \mod 4$, and let $e \in \mathbb{Z}$ be the integer such that $d - 1 = 4e$. Then a $\mathbb{Z}$-basis of $\mathcal{O}_K$ is given by $(x_1, x_2) = (1, \alpha)$, where $\alpha = (1 + \sqrt{d})/2$. We have

$$\alpha^2 = \frac{(1+\sqrt{d})^2}{4} = \frac{d-1}{4} + \frac{1+\sqrt{d}}{2} = e + \alpha$$

and thus

$$\alpha^3 = e\alpha + \alpha^2 = e + (e+1)\alpha.$$

We have

$$\mathrm{Tr}(l_1) = \mathrm{Tr}\begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix} = 2, \quad \mathrm{Tr}(l_\alpha) = \mathrm{Tr}\begin{pmatrix}0 & e\\ 1 & 1\end{pmatrix} = 1, \quad \mathrm{Tr}(l_{\alpha^2}) = \mathrm{Tr}\begin{pmatrix}e & e\\ 1 & e+1\end{pmatrix} = 2e+1,$$

hence

$$\mathrm{Tr}_{\mathcal{O}_K/\mathbb{Z}}(x_i x_j) = \begin{pmatrix}\mathrm{Tr}(l_1) & \mathrm{Tr}(l_\alpha)\\ \mathrm{Tr}(l_\alpha) & \mathrm{Tr}(l_{\alpha^2})\end{pmatrix} = \begin{pmatrix}2 & 1\\ 1 & 2e+1\end{pmatrix}.$$

Taking determinants yields $d_K = 4e + 1 = d$.

CHAPTER 4

Étale algebras

1. Separable field extensions

When k is a field, recall that a *k-algebra* is a ring A together with a ring morphism $\iota_A\colon k \to A$. A morphism of k-algebras $\varphi\colon A \to B$ is a ring morphism such that $\varphi \circ \iota_A = \iota_B$.

When a k-algebra F is a field, we say that F/k is a *field extension*. Note that in this case the ring morphism $k \to F$ is automatically injective, and so we will view k as a subfield of F.

Definition 4.1.1. A field extension F/k is called *finite*, or *of finite degree*, if the inclusion $k \subset F$ makes F a finite-dimensional k-vector space. The *degree* of the extension is $\dim_k L$, denoted $[L : k]$.

Remark 4.1.2. If the field extensions F/k and L/F are both finite, then so is L/k, and

$$[L : k] = [L : F][F : k].$$

Definition 4.1.3. Let F/k be a field extension. An element $x \in F$ is called *algebraic over k* if it is the root of a nonzero polynomial with coefficients in k. The extension F/k is called *algebraic* when all elements of F are algebraic over k.

Note that a field extension F/k is algebraic if and only if the ring F is integral over its subring k.

Remark 4.1.4. A finite field extension F/k is always algebraic. Indeed, if $x \in F$, then the family $x^i, i \in \mathbb{N}$ is linearly dependent over k (as $\dim_k F < \infty$), which provides a nonzero polynomial in $k[X]$ having x as a root. (Alternatively this follows from Example 2.1.14.) There exist algebraic extensions which are not finite.

Lemma 4.1.5. *Let $P \in k[X]$ be an irreducible polynomial, and set $F = k[X]/P$. Then F is a field and $[F : k] = \deg P$.*

Proof. Let $d = \deg P$, and $x \in F$ the class of X. A k-basis of F is given by $1, x, \ldots, x^{d-1}$, and so $\dim_k F = d$. As P is irreducible, it follows that the ring F is a domain. The ring extension $k \subset F$ is integral by Example 2.1.14, hence F is a field by Proposition 2.1.20. □

Definition 4.1.6. When F/k is a field extension and $x \in F$ is algebraic over k, the *minimal polynomial of x over k* is the unique monic generator of the ideal of polynomial P in $k[X]$ such that $P(x) = 0 \in F$.

Remark 4.1.7. Let F/k be a field extension, and $x \in F$ an algebraic element. Let $P \in k[X]$ be the minimal polynomial of x over k. Then $X \mapsto x$ induces an isomorphism of k-algebras $k[X]/P \simeq k[x]$. Since the ring $k[x]$ is a domain (being contained in the field

F), so is the ring $k[X]/P$, which implies that the polynomial P is irreducible. Thus by Lemma 4.1.5 the subalgebra $k[x] \subset F$ is a field. We will call the field extension $k[x]/k$ the subextension of F/k generated by x.

PROPOSITION 4.1.8. *Let k be a field and $P_1, \dots, P_n \in k[X]$ be monic polynomials. Then there exists a field extension L/k of finite degree such that each polynomial $P_1, \dots, P_n$ splits into linear factors in $L[X]$.*

PROOF. We proceed by induction on $d = (\deg P_1) + \cdots + (\deg P_n)$ (allowing k to vary). The proposition is clear if $d = 0$, so we assume that $d \geq 1$. Then $\deg P_j > 0$ for some $j \in \{1, \dots, n\}$, and we let Q be an irreducible factor of P_j. Consider k-algebra $E = k[Y]/Q(Y)$. Then E/k is a field extension of finite degree by Lemma 4.1.5. The polynomial P_j has a root in E, namely (the class of) Y. Thus $P_j = (X - Y)R_j$ in $E[X]$ for some polynomial $R_j \in E[X]$. Setting $R_i = P_i \in E[X]$ for every $i \in \{1, \dots, n\} \smallsetminus \{j\}$, we have

$$(\deg R_1) + \cdots + (\deg R_n) = d - 1,$$

and so by induction we may find a field extension L/E of finite degree where each R_i splits into linear factors. Then each P_i splits into linear in $L[X]$, completing the proof. □

PROPOSITION 4.1.9. *Let E/k be a field extension, and L/k a field extension of finite degree. Then there exist a field extension F/E of finite degree, and a morphism of k-algebras $L \to F$.*

PROOF. We proceed by induction on the degree $[L : k]$, the case $[L : k]$ being clear. Assume that $L \neq k$, and pick $x \in L \smallsetminus k$. Let K/k be the subextension of L/k generated by x. Then x is the root of an irreducible polynomial $P \in k[X]$ (its minimal polynomial over k, recall that the field extension L/k is assumed to be of finite degree), and the k-algebra K isomorphic to $k[X]/P$. If Q is any irreducible divisor of P in $E[X]$, then $E' = E[Y]/Q(Y)$ is a field extension of E having finite degree (Lemma 4.1.5), which admits a morphism of k-algebras $K \to E'$ (corresponding to $X \mapsto Y$). By induction, we find a field extension F/E' of finite degree and a morphism of K-algebras $L \to F$, concluding the proof. □

It is sometimes convenient to adopt a slightly different point of view:

COROLLARY 4.1.10. *Let $L_1/k, \dots, L_n/k$ be field extensions of finite degrees. Let E/k be a field extension. Then there exists a field extension F/E such that F/k contains $L_1/k, \dots, L_n/k$ as subextensions.*

PROOF. We proceed by induction on n, the case $n = 0$ being clear. If $n > 0$, we find by induction a field extension F'/E such that F'/k contains $L_1/k, \dots, L_{n-1}/k$ as subextensions. Since the extension L_n/k is of finite degree, Proposition 4.1.9 yields a field extension F/F' together with a morphism of k-algebras $L_n \to F$, or equivalently a field extension F/k containing F'/k and L_n/k. This proves the corollary. □

DEFINITION 4.1.11. Let k be a field. A polynomial $P \in k[X]$ is called *separable* if, for every field extension L/k, the polynomial $P \in L[X]$ has no multiple root in L.

A field extension F/k is called *separable* if every element of F is the root of an irreducible separable polynomial with coefficients in k. In particular, a separable extension is algebraic by definition.[1]

[1]There exist more sophisticated definitions of separability, which apply to non-algebraic extensions.

Note that an algebraic extension is separable if and only if the minimal polynomial of every element is separable.

REMARK 4.1.12. If F/k is a field extension of finite degree, and $P \in k[X]$ is a polynomial whose image in $F[X]$ splits into a product of pairwise distinct linear factors, then P is separable. Indeed, if L/k is a field extension, we find by Corollary 4.1.10 a field extension E containing F and L. Then P splits into a product of pairwise distinct linear factors in $E[X]$, hence has no multiple roots in E. Since $L \subset E$, we conclude that P has no multiple roots in L as well.

REMARK 4.1.13. It follows from the definition that any subextension of a separable extension is separable. In addition, if F/k is separable field extension and E/k a subextension of F/k, then the extension F/E is separable: indeed the minimal polynomial over E of an element of F divides its minimal polynomial over k, and so must be separable.

LEMMA 4.1.14. *An irreducible polynomial $P \in k[X]$ is separable if and only if its derivative $P' \in k[X]$ is nonzero.*

PROOF. First, let F/k be a field extension, and $a \in F$ be such that $P(a) = 0$. Write $P = (X-a)R$, with $R \in F[X]$. Then $P' = R+(X-a)R'$, and so $P'(a) = R(a)$. Therefore

$$a \text{ is a multiple root of } P \iff (P(a) = 0 \text{ and } P'(a) = 0). \tag{4.1.a}$$

Assume now that $P' \neq 0$. Let $Q \in k[X]$ be the greatest common divisor of P and P' in $k[X]$, that is the monic generator of the ideal generated by P and P' in $k[X]$. As P' is nonzero and $Q \mid P'$, we have $\deg Q \leq \deg P' < \deg P$. As P is irreducible and divisible by Q, we must have $Q = 1$. Therefore there exist $U, V \in k[X]$ such that $1 = UP + VP'$. If F/k is a field extension, and $a \in F$ a multiple root of P, then a is root of P' by (4.1.a), so that

$$1 = (UP + VP')(a) = U(a)P(a) + V(a)P'(a) = 0,$$

a contradiction which proves that P is separable.

Conversely assume that P is separable. As P is nonconstant (being irreducible), by Proposition 4.1.8 we may find a field extension F/k, and an element $a \in F$ such that $P(a) = 0$. Then $P'(a) \neq 0$ by (4.1.a), and in particular the polynomial $P' \in k[X]$ is nonzero. □

DEFINITION 4.1.15. A field k is called *perfect* if every finite field extension of k is separable. An equivalent condition is that every irreducible polynomial in $k[X]$ is separable.

PROPOSITION 4.1.16. *Every field of characteristic zero is perfect.*

PROOF. Let k be a field of characteristic zero, and let $P \in k[X]$ be an irreducible polynomial, of degree $n > 1$. Then we write

$$P = a_n X^n + \cdots + a_0, \quad \text{with } a_0, \ldots, a_n \in k,$$

and $a_n \neq 0$. Then

$$P' = n a_n X^{n-1} + \cdots + a_1.$$

As $n \neq 0$ in k (because k has characteristic zero), we deduce that $P' \neq 0$. The proposition thus follows from Lemma 4.1.14. □

PROPOSITION 4.1.17. *Every finite field is perfect.*

Proof. Let k be a finite field. Then k has characteristic p, when $p > 0$ is a prime number. Let us first recall that if A is any ring where $p = 0$, we have

$$(a+b)^p = a^p + b^p \quad \text{for any } a, b \in A. \tag{4.1.b}$$

(Observe that the binomial coefficients $\binom{p}{i}$ are all divisible by p when $1 < i < p$.)

Let $P \in k[X]$ be an irreducible polynomial such that $P' = 0$. If $a_m \in k$ is the X^m-th coefficient of P, then ma_m is the X^{m-1}-th coefficient of P'. When m is not divisible by p, we have $m \neq 0$ in k and thus $a_m = 0$. Therefore we may $P = B(X^p)$, for some $B \in k[Y]$. Let us write

$$B = b_r Y^r + \cdots + b_0, \quad \text{with } b_0, \dots, b_r \in k.$$

In view of (4.1.b) (applied to $A = k$), the Frobenius map $\phi\colon k \to k$ given by $x \mapsto x^p$ is a group morphism. As $x^p = 0$ implies $x = 0$ in the field k, the morphism ϕ is injective. But the set k is finite, hence the map ϕ must also be surjective. Thus we can find elements $c_0, \dots, c_r \in k$ such that $c_i^p = b_i$ for all $i = 0, \dots, r$. Consider the polynomial

$$C = c_r X^r + \cdots + c_0 \in k[X].$$

Then $C(X)^p = B(X^p) = P$ by (4.1.b) (applied in the ring $A = k[X]$), which contradicts the fact the P is irreducible.

We have proved that every irreducible polynomial in $k[X]$ has a nonzero derivative, and we deduce the proposition from Lemma 4.1.14. □

We now come to a crucial property of separable extensions:

Proposition 4.1.18. *Let F/k be a finite separable field extension, and set $n = [F : k]$. Then there exists a finite field extension ℓ/k and n pairwise distinct morphisms of k-algebras $\sigma_1, \dots, \sigma_n\colon F \to \ell$.*

Proof. We proceed by induction on the integer n. The case $n = 1$ is clear, so we assume that $n > 1$, or equivalently $F \neq k$. Since F/k contains no infinite increasing chain of subextensions (such chains are in particular chains of k-subspaces, and F is finite-dimensional over k), we may find a subextension $E \subset F$ and an element $x \in F \smallsetminus E$ such that $F = E[x]$ (recall from Remark 4.1.7 that $E[x]$ is a field). Let $P \in E[X]$ be the minimal polynomial of x over E. Since the field extension F/E is separable by Remark 4.1.13, the polynomial P is separable. Mapping X to x induces an isomorphism of E-algebras $E[X]/P \simeq F$. Recall that the extension E/k is separable (Remark 4.1.13), and its degree $m = [E : k]$ satisfies $m < [F : k]$ because $E \neq F$. Therefore by induction we may find a field extension ℓ'/k of finite degree, and m distinct morphisms of k-algebras $\sigma'_1, \dots, \sigma'_m\colon E \to \ell'$.

For each $i \in \{1, \dots, n\}$ the polynomial $\sigma'_i(P) \in \ell'[X]$ is separable, being the image of the separable polynomial P under the field extension ℓ'/k given by σ'_i. By Proposition 4.1.8, we may find a field extension ℓ/ℓ' of finite degree such that each polynomial $\sigma'_i(P) \in \ell'[X]$ splits into monic linear factors in $\ell[X]$, which are pairwise distinct since $\sigma'_i(P)$ is separable.

For each $i \in \{1, \dots, m\}$, the extensions of the composite $E \xrightarrow{\sigma'_i} \ell' \subset \ell$ to a morphism of k-algebras $F \to \ell$ are in bijection with the roots of $\sigma'_i(P)$ in ℓ (because $F \simeq E[X]/P$), of which there are exactly $\deg P = [F : k]$, because the polynomial $\sigma'_i(P)$ is separable over . We have thus found $m[F : k] = n$ morphisms of k-algebras $F \to \ell$, as required. □

We will need the following consequence later:

COROLLARY 4.1.19 (Primitive Element Theorem). *If F/k is a separable field extension of finite degree, there exists an element $x \in F$ such that $F = k[x]$.*

PROOF. When k is finite, the group $k^\times$ is cyclic by Proposition 1.3.5, and we may simply take x a generator of that group.

We now assume that k is infinite. Let $n = [F : k]$. By Proposition 4.1.18 we find a field extension ℓ/k of finite degree, and n distinct morphisms $\sigma_1, \dots, \sigma_n \colon F \to \ell$. For each pair $(i, j) \in \{1, \dots, n\}^2$, consider the k-subspace $V_{i,j} \subset F$ consisting of those elements $y \in F$ such that $\sigma_i(y) = \sigma_j(y)$. Since the morphisms $\sigma_1, \dots, \sigma_n$ are pairwise distinct, we have $V_{i,j} \neq F$ whenever $i \neq j$. By Lemma 4.1.20 below, we may find an element $x \in F$ which belongs to no $V_{i,j}$ with $i \neq j$. The elements $\sigma_i(x)$ for $i \in \{1, \dots, n\}$ are then pairwise distinct. Those are roots (in ℓ) of the minimal polynomial P of x over k. Letting $d = \deg P$, we thus have $d \geq n$. The elements $1, x, \dots, x^{d-1} \in F$ are linearly independent over k, hence $[k[x] : k] \geq d$. But $k[x] \subset F$, hence $[k[x] : k] \leq [F : k] = n$. We conclude that $d = n$, and $[k[x] : k] = [F : k]$, which implies that $k[x] = F$. □

LEMMA 4.1.20. *Let k be an infinite field, and V a k-vector space. If $V_1, \dots, V_n$ are k-subspaces of V such that $V = V_1 \cup \cdots \cup V_n$, then there exists $i \in \{1, \dots, n\}$ such that $V_i = V$.*

PROOF. We proceed by induction on n, the statement being clear if $n = 1$. Assume that $n > 1$. Assume $V_1 \neq V$ (otherwise the conclusion of the lemma holds), and pick $y \in V \smallsetminus V_1$. Let $x \in V_1$. Then the set

$$E = \{x + \lambda y | \lambda \in k \smallsetminus \{0\}\}$$

is in bijection with $k \smallsetminus \{0\}$ (as $y \neq 0$), and in particular is infinite. Since $y \notin V_1$, it follows that $E \cap V_1 = \varnothing$, and thus $E \subset V_2 \cup \cdots \cup V_n$, or equivalently

$$E = (E \cap V_2) \cup \cdots \cup (E \cap V_n).$$

As the set E is infinite, we may find an index $j \in \{2, \dots, n\}$ such that the set $E \cap V_j$ is infinite, and in particular contains two distinct elements. So there are $\lambda_1 \neq \lambda_2 \in k$ such that $x + \lambda_1 y \in V_j$ and $x + \lambda_2 y \in V_j$. This implies that

$$y = (\lambda_1 - \lambda_2)^{-1}((x + \lambda_1 y) - (x + \lambda_2 y))$$

belongs to V_j, and thus $x = (x + \lambda_1 y) - \lambda_1 y \in V_j$. We have proved that $V_1 \subset V_2 \cup \cdots \cup V_n$. Therefore $V = V_2 \cup \cdots \cup V_n$, and by induction we find $i \in \{2, \dots, n\}$ such that $V_i = V$. □

2. Étale algebras over a field

In this section k is a field. When X is any set, and F a field, then the set of maps $X \to F$ is naturally F-vector space; namely for any $f, g \colon X \to F$ and $\lambda \in F$, we define

$$f + \lambda g \colon X \to F, \quad x \mapsto f(x) + \lambda g(x).$$

LEMMA 4.2.1 (Dedekind). *Let A be a k-algebra, and ℓ/k a field extension. Let $\sigma_1, \dots, \sigma_n$ be pairwise distinct morphisms of k-algebras $A \to \ell$. Then the elements $\sigma_1, \dots, \sigma_n$ are ℓ-linearly independent, in the ℓ-vector space of maps $A \to \ell$.*

In particular $n \leq \dim_k A$ when A is finite-dimensional.

PROOF. Assume that

$$a_1\sigma_1 + \cdots + a_m\sigma_m = 0. \tag{4.2.a}$$

where $a_1, \dots, a_m \in \ell$ are not all zero. Pick such a relation, where $m \in \{1, \dots, n\}$ is minimal. In particular $a_m \neq 0$. As $\sigma_m \neq 0$ (because $\sigma_m(1) = 1 \in \ell$, which is nonzero since ℓ is a field), there exists $j \in \{1, \dots, m-1\}$ such that $a_j \neq 0$ (in particular $m > 1$). Since $\sigma_j \neq \sigma_m$, we may find $z \in A$ such that $\sigma_j(z) \neq \sigma_m(z)$. Since the morphisms $\sigma_1, \dots, \sigma_n$ are multiplicative, it follows from (4.2.a) (applied to zx for all $x \in A$) that

$$a_1\sigma_1(z)\sigma_1 + \cdots + a_m\sigma_m(z)\sigma_m = 0. \tag{4.2.b}$$

Subtracting $\sigma_m(z)$ times Equation (4.2.a) to (4.2.b) yields

$$a_1(\sigma_1(z) - \sigma_m(z))\sigma_1 + \cdots + a_{m-1}(\sigma_{m-1}(z) - \sigma_m(z))\sigma_{m-1} = 0.$$

Since $a_j(\sigma_j(z) - \sigma_m(z)) \neq 0$, we have found a contradiction with the minimality of m. □

Definition 4.2.2. A k-algebra A of finite dimension n is called *étale* if there exist a field extension ℓ/k and n distinct morphisms of k-algebras $\sigma_1, \dots, \sigma_n \colon A \to \ell$.

It is clear from the definition that any k-algebra isomorphic to an étale k-algebra is itself étale.

Lemma 4.2.3. *Let A be an étale k-algebra. Then there exist a field extension ℓ/k of finite degree, and n distinct morphisms of k-algebras $\sigma_1, \dots, \sigma_n \colon A \to \ell$.*

Proof. Let $\sigma_1, \dots, \sigma_n \colon A \to \ell$ be as in Definition 4.2.2, and let $e_1, \dots, e_n$ be a k-basis of A. Recall that the ring A is integral over k (see Example 2.1.14), hence the elements $\sigma_i(e_j) \in \ell$ are integral over k by Lemma 2.1.17. Therefore, by Corollary 2.1.7, the k-subalgebra ℓ' of ℓ generated by the elements $\sigma_i(e_j)$ for $i, j \in \{1, \dots, n\}$ is of finite dimension as a k-vector space. Since the ring ℓ' is contained in the field ℓ, it is a domain, and thus ℓ' is a field by Proposition 2.1.20. Since $\ell' \subset \ell$ contains the image of each morphism σ_i for $i \in \{1, \dots, n\}$, we may thus replace ℓ with ℓ'. □

Recall that a field F is called *algebraically closed* if the only algebraic field extension of F is F itself.

Lemma 4.2.4. *Let $\overline{k}/k$ be a field extension, with $\overline{k}$ algebraically closed. Then a k-algebra A of finite dimension n is étale if and only if there are exactly n morphisms of k-algebras $A \to \overline{k}$.*

Proof. Assume that A is étale, and pick a finite field extension ℓ/k and morphisms $\sigma_1, \dots, \sigma_n \colon A \to \ell$ (see Lemma 4.2.3). Then it follows from Proposition 4.1.9 that we may find a morphism of k-algebras $\ell \to \overline{k}'$, where $\overline{k}'/\overline{k}$ is a field extension of finite degree, and in particular an algebraic field extension. Since the field $\overline{k}$ is algebraically closed, we must have $\overline{k}' = \overline{k}$. We have thus n distinct morphisms $A \to \overline{k}$. By Dedekind's Lemma 4.2.1, there are no other such morphisms.

The converse follows from Definition 4.2.2, with $\ell = \overline{k}$. □

Proposition 4.2.5. *A finite separable field extension of k is an étale k-algebra.*

Proof. This is Proposition 4.1.18. □

Proposition 4.2.6. *Let $P \in k[X]$ be a nonzero polynomial, and consider the k-algebra $A = k[X]/P$. Then A is étale if and only if P is separable.*

PROOF. Let $n = \deg P = \dim_k A$, and denote by $x \in A$ the class of X.

Assume that P is separable. Then by Proposition 4.1.8 we may find a field extension ℓ/k such that P splits into linear factors in $\ell[X]$, and so has n distinct roots $\alpha_1, \dots, \alpha_n \in \ell$. This yields n distinct morphisms of k-algebras, given by $x \mapsto \alpha_i$ for $i = 1, \dots, n$. We have proved that A is étale.

Conversely, assume that A is étale. According to Lemma 4.2.3, we may find a finite field extension ℓ/k and n distinct morphisms of k-algebras $\sigma_1, \dots, \sigma_n \colon A \to \ell$. The elements $\sigma_1(x), \dots, \sigma_n(x) \in \ell$ are then n distinct roots of P. Let us consider now a field extension F/k. By Corollary 4.1.10 we may find a field extension E/k containing both F/k and ℓ/k. The polynomial P splits into a product of pairwise distinct monic linear factors in $E[X]$ (because it does so in $\ell[X]$), hence its roots in E are pairwise distinct in E, and thus so are its roots in F. We have proved that the polynomial P is separable. □

3. Extension of scalars

Let k be a field. When A is a k-algebra and ℓ/k a field extension, we recall that we may define an ℓ-algebra $A \otimes_k \ell$ (see exercises). Its elements are of the form

$$\sum_{i=1}^{m} a_i \otimes \lambda_i, \quad \text{where } a_i \in A, \lambda_i \in \ell.$$

The map $A \to A \otimes_k \ell$ given by $a \mapsto a \otimes 1$ is an injective morphism of k-algebra, and we will thus view A as a k-subalgebra of $A \otimes_k \ell$.

When A is finite-dimensional as a k-vector space, so is the ℓ-vector space $A \otimes_k \ell$, and

$$\dim_k A = \dim_\ell (A \otimes_k \ell). \tag{4.3.a}$$

This construction satisfies the following universal property: if C is an ℓ-algebra, every morphism of k-algebras $A \to C$ extends uniquely to a morphism of ℓ-algebras $A \otimes_k \ell \to C$.

If A, B are k-algebras, then we have a canonical isomorphism of ℓ-algebras

$$(A \times B) \otimes_k \ell \simeq (A \otimes_k \ell) \times (B \otimes_k \ell). \tag{4.3.b}$$

PROPOSITION 4.3.1. *Let A be an étale k-algebra, and consider the distinct morphisms of k-algebras $\sigma_1, \dots, \sigma_n \colon A \to \ell$, where ℓ/k is a field extension and $n = \dim_k A$ (see Definition 4.2.2). Then there exists an isomorphism of ℓ-algebras*

$$\sigma \colon A \otimes_k \ell \xrightarrow{\sim} \ell^n$$

mapping $x \otimes y$ to $(\sigma_1(x)y, \dots, \sigma_n(x)y)$.

PROOF. Let us write $A' = A \otimes_k \ell$. By the universal property mentioned above, the n distinct morphisms of k-algebras $\sigma_1, \dots, \sigma_n \colon A \to \ell$ extend uniquely to n distinct morphisms of ℓ-algebras $\sigma'_1, \dots, \sigma'_n \colon A' \to \ell$, and we set

$$\sigma = (\sigma'_1, \dots, \sigma'_n) \colon A' \to \ell^n.$$

For $i \in \{1, \dots, n\}$ and $x \in A, y \in \ell$, we have, by ℓ-linearity of σ'_i and the fact that σ'_i extends σ_i,

$$\sigma'_i(x \otimes y) = \sigma'_i(x)y = \sigma_i(x)y.$$

By Dedekind's Lemma 4.2.1, the elements $\sigma'_1, \dots, \sigma'_n$ are linearly independent in the ℓ-vector space $\mathrm{Hom}_\ell(A', \ell)$ of ℓ-linear forms $A' \to \ell$. This vector space has dimension $\dim_\ell A' = \dim_k A = n$ (see (4.3.a)), hence the family $\sigma'_1, \dots, \sigma'_n$ generates it.

Let now $a \in A'$ be such that $\sigma_i(a) = 0 \in \ell$ for all $i \in \{1, \dots, n\}$. If $a \neq 0$, then we may find an ℓ-linear form $\varphi\colon A' \to \ell$ such that $\varphi(a) \neq 0$ (take an ℓ-basis $(e_1, \dots, e_n)$ of A', pick $i \in \{1, \dots, n\}$ such that i-th coordinate of a is nonzero in that basis, and take for φ the linear form given by $\varphi(e_j) = \delta_{ij}$). We may then write φ as an ℓ-linear combination of $\sigma'_1, \dots, \sigma'_n$ (recall that those generate the ℓ-vector space $\mathrm{Hom}_\ell(A', \ell)$). This implies that $\varphi(a) = 0$, a contradiction. We have proved that σ is injective, hence bijective by dimensional reasons (see (4.3.a)). □

LEMMA 4.3.2. *Let A be a finite dimensional k-algebra, and ℓ/k a field extension.*

(i) For any $a \in A$, the characteristic polynomials (see Definition 3.1.1) satisfy

$$\chi_{A/k}(a) = \chi_{(A\otimes_k \ell)/\ell}(a \otimes 1) \in k \subset \ell.$$

(ii) If $(x_1, \dots, x_n) \in A^n$, the discriminant satisfy

$$\mathrm{D}_{A/k}(x_1, \dots, x_n) = \mathrm{D}_{(A\otimes_k \ell)/\ell}(x_1 \otimes 1, \dots, x_n \otimes 1) \in k \subset \ell.$$

(iii) We have

$$\mathfrak{D}_{A/k} = 0 \quad \Longleftrightarrow \quad \mathfrak{D}_{(A\otimes_k \ell)/\ell} = 0.$$

PROOF. We let $(e_1, \dots, e_n)$ be a k-basis of A. Then $(e_1 \otimes 1, \dots, e_n \otimes 1)$ is an ℓ-basis of $A \otimes_k \ell$ (exercise).

(i): The coefficients of the matrix of $l_{a\otimes 1}\colon A\otimes_k \ell \to A\otimes_k \ell$ in the basis $(e_1\otimes 1, \dots, e_n\otimes 1)$ are the images of those of the matrix of $l_a\colon A \to A$ in the basis $(e_1, \dots, e_n)$ under the inclusion $k \subset \ell$. It follows that the characteristic polynomial $\chi_{(A\otimes_k \ell)/\ell}(a\otimes 1)$ is the image of the characteristic polynomial $\chi_{A/k}(a)$ under the inclusion $k \subset \ell$.

(ii): Let us write $A' = A \otimes_k \ell$ and $x'_i = x_i \otimes 1$ for $i \in \{1, \dots, n\}$. From (i), we deduce that $\mathrm{Tr}_{A/k}(x_i x_j) = \mathrm{Tr}_{A'/\ell}(x'_i x'_j)$ for any $i, j \in \{1, \dots, n\}$. Therefore the matrix $(\mathrm{Tr}_{A'/\ell}(x'_i x'_j)) \in M_n(\ell)$ is the image of the matrix $(\mathrm{Tr}_{A/k}(x_i x_j)) \in M_n(k)$ under the inclusion $k \subset \ell$, hence its determinant $\mathrm{D}_{A'/\ell}(x'_1, \dots, x'_n) \in \ell$ is the image of the determinant $\mathrm{D}_{A/k}(x_1, \dots, x_n) \in k$ under the inclusion $k \subset \ell$.

(iii): It follows from Proposition 3.2.5 that

$$\mathrm{D}_{A/k}(e_1, \dots, e_n) \neq 0 \quad \Longleftrightarrow \quad \mathfrak{D}_{A/k} \neq 0,$$

and that

$$\mathrm{D}_{(A\otimes \ell)/\ell}(e_1 \otimes 1, \dots, e_n \otimes 1) \neq 0 \quad \Longleftrightarrow \quad \mathfrak{D}_{(A\otimes \ell)/\ell} \neq 0.$$

Therefore (iii) follows from (ii). □

We are now in position to prove certain formulas that will be very useful in order to perform computations in étale algebras (and in particular in separable field extensions).

PROPOSITION 4.3.3. *Let A be an étale k-algebra. In the notation of Definition 4.2.2, the characteristic polynomial of any $a \in A$ satisfies*

$$\chi_{A/k}(a) = \prod_{i=1}^{n} (X - \sigma_i(a)) \in k[X] \subset \ell[X].$$

In particular, in $k \subset \ell$

$$\mathrm{Tr}_{A/k}(a) = \sum_{i=1}^{n} \sigma_i(a) \quad \text{and} \quad \mathrm{N}_{A/k}(a) = \prod_{i=1}^{n} \sigma_i(a).$$

PROOF. Consider the isomorphism of ℓ-algebras $\sigma\colon A\otimes_k \ell \xrightarrow{\sim} \ell^n$ of Proposition 4.3.1. We have in $k\subset\ell$, by Lemma 4.3.2 (i) and Lemma 3.1.2

$$\chi_{A/k}(a)=\chi_{(A\otimes_k\ell)/\ell}(a\otimes 1)=\chi_{\ell^n/\ell}(\sigma(a\otimes 1))=\chi_{\ell^n/\ell}(\sigma_1(a),\dots,\sigma_n(a)).$$

Now in the canonical basis of ℓ^n, multiplication by the element $(\sigma_1(a),\dots,\sigma_n(a))$ is given by the diagonal matrix having coefficients $\sigma_1(a),\dots,\sigma_n(a)$, whose characteristic polynomial is

$$\prod_{i=1}^{n}(X-\sigma_i(a))\in\ell[X]. \qquad \square$$

PROPOSITION 4.3.4. *Let A be an étale k-algebra. In the notation of Definition 4.2.2, for any system $(x_1,\dots,x_n)\in A^n$, we have*

$$\mathrm{D}_{A/k}(x_1,\dots,x_n)=\det(\sigma_i(x_j))^2\in k\subset\ell.$$

PROOF. For any $i,j\in\{1,\dots,n\}$, we have by Proposition 4.3.3

$$\mathrm{Tr}_{A/k}(x_ix_j)=\sum_{p=1}^{n}\sigma_p(x_ix_j)=\sum_{p=1}^{n}\sigma_p(x_i)\sigma_p(x_j)\in\ell,$$

which coincides with the (i,j)-th coefficient of the matrix product $M\cdot{}^tM$ in $M_n(\ell)$, where M is the matrix whose (r,s)-th coefficient is $\sigma_r(x_s)\in\ell$, and ${}^tM$ its transpose. Thus

$$\begin{aligned}\mathrm{D}_{A/k}(x_1,\dots,x_n)&=\det(\mathrm{Tr}_{A/k}(x_ix_j))\\&=\det(M\cdot{}^tM)\\&=(\det M)\cdot(\det{}^tM)\\&=(\det M)^2\\&=\det(\sigma_i(x_j))^2.\end{aligned}\qquad\square$$

PROPOSITION 4.3.5. *Let $A=k[X]/P$, where $P\in k[X]$ is a monic separable polynomial. Let n be the degree of P, and $x\in A$ be the class of X. Then*

$$\mathrm{D}_{A/k}(1,x,\dots,x^{n-1})=(-1)^{\frac{n(n-1)}{2}}\,\mathrm{N}_{A/k}(P'(x))\in k,$$

where $P'\in k[X]$ is the derivative of P.

PROOF. Recall from Proposition 4.2.6 that the k-algebra A is étale. So we have n morphisms of k-algebras $\sigma_1,\dots,\sigma_n\colon A\to\ell$, where ℓ/k is a field extension. Let $\alpha_i=\sigma_i(x)$ for $i=1,\dots,n$. Then $\alpha_1,\dots,\alpha_n$ are n distinct roots of P in ℓ, hence

$$P=\prod_{i=1}^{n}(X-\alpha_i)\in\ell[X],$$

so that

$$P'=\sum_{i=1}^{n}\prod_{j\neq i}(X-\alpha_j)\in\ell[X],$$

and in particular, for any $i\in\{1,\dots,n\}$

$$P'(\alpha_i)=\prod_{j\neq i}(\alpha_i-\alpha_j)\in\ell[X]. \tag{4.3.c}$$

We now compute:

$$\begin{aligned}
\mathrm{D}_{A/k}(1, x, \dots, x^{n-1}) &= \det((\alpha_i)^{j-1})^2 && \text{by Proposition 4.3.4} \\
&= \Big(\prod_{j<i}(\alpha_i - \alpha_j)\Big)^2 && \text{(Vandermonde determinant)} \\
&= (-1)^{\frac{n(n-1)}{2}} \prod_{i \neq j}(\alpha_i - \alpha_j) && \text{as } \mathrm{card}\{(i,j) | 1 \leq i < j \leq n\} = \frac{n(n-1)}{2} \\
&= (-1)^{\frac{n(n-1)}{2}} \prod_{i=1}^{n} \prod_{j \neq i}(\alpha_i - \alpha_j) \\
&= (-1)^{\frac{n(n-1)}{2}} \prod_{i=1}^{n} P'(\alpha_i) && \text{by (4.3.c)} \\
&= (-1)^{\frac{n(n-1)}{2}} \prod_{i=1}^{n} \sigma_i(P'(x)) && \text{as } \sigma_i \text{ is a morphism of } k\text{-algebras} \\
&= (-1)^{\frac{n(n-1)}{2}} \mathrm{N}_{A/k}(P'(x)) && \text{by Proposition 4.3.3.} \qquad \square
\end{aligned}$$

4. The trace form

LEMMA 4.4.1. *Let A, B be k-algebras. Then A and B are étale if and only if $A \times B$ is étale.*

PROOF. Clearly A and B are finite-dimensional over k if and only if $A \times B$ is so. Let us assume that this is the case, and write $n = \dim_k A, m = \dim_k B$.

Assume that the k-algebras A, B are étale. Then by Lemma 4.2.3 there exist field extensions ℓ/k and ℓ'/k of finite degrees, as well as n morphisms of k-algebras $A \to \ell$ and m morphisms of k-algebras $B \to \ell'$. By Corollary 4.1.10, we may assume that $\ell = \ell'$ (upon enlarging ℓ). Composing with the projections $A \times B \to A$ and $A \times B \to B$, we obtain $n+m$ distinct morphisms of k-algebras $A \times B \to \ell$. This proves that the k-algebra $A \times B$ is étale.

Let now ℓ/k be a field extension, and $f\colon A \times B \to \ell$ a morphism of k-algebras. Then the image of f is a domain (being contained in the field ℓ). Thus $\ker f$ is a prime ideal of $A \times B$, hence a maximal ideal by Corollary 2.1.21. This implies that $\ker f = \mathfrak{m} \times B$ or $\ker f = A \times \mathfrak{m}'$, where $\mathfrak{m} \subset A$ or $\mathfrak{m}' \subset B$ is a maximal ideal (this follows from the fact that the ideals of $A \times B$ are precisely the subsets $I \times J$, where $I \subset A$ and $J \subset B$ are ideals). In particular the morphism f factors through exactly one of the projections $A \times B \to A$ or $A \times B \to B$.

Assume now that the k-algebra $A \times B$ is étale. Then we find a field extension ℓ/k and $m+n$ morphisms of k-algebras $A \times B \to \ell$. Let a, resp. b, the number of those morphisms which factor through the quotient $A \times B \to A$, resp. $A \times B \to B$. Then $a \leq n$ and $b \leq m$ by Dedekind's Lemma 4.2.1. We have just seen that $a + b = n + m$. We conclude that $a = n$ and $b = m$, showing that both A and B are étale k-algebras. $\square$

We recall that a element x of a ring A is called nilpotent if there exists an integer $n \in \mathbb{N}$ such that $x^n = 0$. A ring is called *reduced* its only nilpotent element is zero.

LEMMA 4.4.2. *Let A, B be rings. Then $A \times B$ is reduced if and only if both A and B are reduced.*

PROOF. Certainly an element $(a, b) \in A \times B$ is nilpotent if and only if both $a \in A$ and $b \in B$ are nilpotent. □

LEMMA 4.4.3. *In a reduced noetherian ring, the zero ideal is the intersection of a finite family of pairwise distinct prime ideals.*

PROOF. Let A be a ring. We know that the ideal 0 contains a product of prime ideals of A (Lemma 1.2.9), hence $0 = \mathfrak{p}_1 \cdots \mathfrak{p}_n$, for some prime ideals $\mathfrak{p}_1, \ldots, \mathfrak{p}_n$ of A (possibly not pairwise distinct). If $x \in \mathfrak{p}_1 \cap \cdots \cap \mathfrak{p}_n$, then $x^n \in \mathfrak{p}_1 \cdots \mathfrak{p}_n$, hence $x^n = 0$, and thus $x = 0$ as A is reduced. Thus $\mathfrak{p}_1 \cap \cdots \cap \mathfrak{p}_n = 0$, where, upon removing duplicates, we may now assume that $\mathfrak{p}_i \neq \mathfrak{p}_j$ when $i \neq j$. □

PROPOSITION 4.4.4. *Every reduced finite-dimensional k-algebra is a product of finite field extensions of k.*

PROOF. Let A be a reduced finite-dimensional k-algebra. Then A is noetherian by Example 1.2.3, hence by Lemma 4.4.3 we may write $0 = \mathfrak{p}_1 \cap \cdots \cap \mathfrak{p}_n$, where $\mathfrak{p}_1, \ldots, \mathfrak{p}_n$ are pairwise distinct prime ideals of A. Then $\mathfrak{p}_i + \mathfrak{p}_j = A$ for $i \neq j$ because $\mathfrak{p}_i$ is maximal by Corollary 2.1.21. We conclude using Lemma 1.1.5 that $A \simeq (A/\mathfrak{p}_1) \times \cdots \times (A/\mathfrak{p}_n)$, where each $A/\mathfrak{p}_i$ is a field extension of k (this is an isomorphism of A-algebras, hence in particular of k-algebras). These field extensions have finite degrees, being quotients of the finite-dimensional k-vector space A. □

When V is a k-vector space, we recall that a symmetric bilinear form $\varphi\colon V \times V \to k$ is called *nondegenerate* if the k-linear map

$$V \to \mathrm{Hom}_k(V, k), \quad x \mapsto (y \mapsto \varphi(x, y)) \tag{4.4.a}$$

is bijective.

LEMMA 4.4.5. *Let V be a finite-dimensional k-vector space, and $\varphi\colon V \times V \to k$ a nondegenerate symmetric bilinear form. Then for each k-basis $(y_1, \ldots, y_n)$ of V we may find a k-basis $(x_1, \ldots, x_n)$ of V such that $\varphi(x_i, y_j) = \delta_{ij}$ for all $i, j \in \{1, \ldots, n\}$ (we use the notation of* (1.3.b)*).*

PROOF. For each $i \in \{1, \ldots, n\}$, consider the linear form $y_i^* \in \mathrm{Hom}_k(V, k)$ given by $y_i^*(y_j) = \delta_{ij}$ for all $j \in \{1, \ldots, n\}$. Since the map (4.4.a) is surjective, we may find an element x_i mapping to y_i^* under (4.4.a), which means that $\varphi(x_i, y_i) = \delta_{ij}$ for all $j \in \{1, \ldots, n\}$. It remains to prove that the system $(x_1, \ldots, x_n)$ is a k-basis of V. Assume that

$$\sum_{i=1}^{n} \lambda_i x_i = 0 \in V, \quad \text{with } \lambda_1, \ldots, \lambda_n \in k.$$

Applying (4.4.a) yields

$$\sum_{i=1}^{n} \lambda_i y_i^* = 0 \in \mathrm{Hom}_k(V, k).$$

Evaluating at $y_j \in V$, for $j \in \{1, \ldots, n\}$, shows that $\lambda_j = 0$. We have proved that the system $(x_1, \ldots, x_n)$ is k-linearly independent, hence a k-basis by dimensional reasons. □

THEOREM 4.4.6. *Let A be a finite-dimensional k-algebra. Then the following conditions are equivalent:*

(i) the k-algebra A is étale,

(ii) there exists a field extension ℓ/k of finite degree such that $A \otimes_k \ell \simeq \ell^n$ as ℓ-algebras,
(iii) $\mathfrak{D}_{A/k} \neq 0$ (see Definition 3.2.3),
(iv) the symmetric bilinear form $A \times A \to k$ given by $(x, y) \mapsto \mathrm{Tr}_{A/k}(xy)$ is nondegenerate,
(v) for every field extension ℓ/k, then ring $A \otimes_k \ell$ is reduced,
(vi) A is isomorphic to a product of separable field extensions of k.

PROOF. (i) $\Rightarrow$ (ii) : This is Proposition 4.3.1.

(ii) $\Rightarrow$ (iii) : The discriminant of the canonical ℓ-basis of ℓ^n is 1, hence $\mathfrak{D}_{\ell^n/\ell} \neq 0$. In view of Lemma 3.2.4, the assumption (ii) thus implies that $\mathfrak{D}_{(A\otimes_k\ell)/\ell} \neq 0$. Using Lemma 4.3.2 (iii) we deduce that $\mathfrak{D}_{A/k} \neq 0$.

(iii) $\Leftrightarrow$ (iv) : Let $(e_1, \ldots, e_n)$ be a k-basis of A. Let $(e_1^*, \ldots, e_n^*) \in \mathrm{Hom}_k(A, k)$ be the dual basis, characterised by the equations $e_i^*(e_j) = \delta_{ij}$ for $i, j \in \{1, \ldots, n\}$ (we use the notation of (1.3.b)). Then in these basis, the matrix of the k-linear map $A \to \mathrm{Hom}_k(A, k)$ sending $x \in A$ to the linear form $y \mapsto \mathrm{Tr}_{A/k}(xy)$ is given by $(\mathrm{Tr}_{A/k}(e_ie_j))$, so that its determinant is the discriminant $\mathrm{D}_{A/k}(e_1, \ldots, e_n) \in k$. We thus see that $\mathrm{D}_{A/k}(e_1, \ldots, e_n)$ is nonzero if and only if the trace form given in (iv) is nondegenerate. But it follows from Proposition 3.2.5 that $\mathrm{D}_{A/k}(e_1, \ldots, e_n) \neq 0$ if and only if $\mathfrak{D}_{A/k} \neq 0$.

(iii) $\Rightarrow$ (v) : Let ℓ/k be a field extension, and consider the ℓ-algebra $A' = A \otimes_k \ell$. We have $\mathfrak{D}_{A/k} \neq 0$ by (iii), hence $\mathfrak{D}_{A'/\ell} \neq 0$ by Lemma 4.3.2 (iii). In view of the implication (iii) $\Rightarrow$ (iv) established above (applied to the ℓ-algebra A'), we deduce that the trace form $A' \times A' \to \ell$ is nondegenerate. Thus for every nonzero element $a \in A'$, we may find an element $b \in A'$ such that $\mathrm{Tr}_{A'/\ell}(ab) \neq 0 \in \ell$. As the trace of a nilpotent element is zero (see Proposition 3.1.3), the element $ab \in A'$ is not nilpotent, hence the element $a \in A'$ is not nilpotent. We have proved that the ring A' is reduced, as required.

(v) $\Rightarrow$ (vi) : By Proposition 4.4.4, the k-algebra A is isomorphic to a product of field extensions of k of finite degrees. It remains to prove that these are separable. Let K/k be one of these field extensions, and $x \in K$. Let $B = k[x] \subset K$. Then the k-algebra B is isomorphic to $k[X]/P$, where P is the minimal polynomial of x over k. For every field extension ℓ/k, the ring $\ell[X]/P \simeq B \otimes_k \ell$ is reduced, being contained[2] in $K \otimes_k \ell$, which is reduced because $A \otimes_k \ell$ is so (Lemma 4.4.2, in view of (4.3.b)). This implies that the polynomial $P \in k[X]$ is separable: indeed if $P = (X - a)Q \in \ell[X]$ where $Q \in \ell[X]$ and $a \in \ell$ are such that $Q(a) = 0$, then $P \mid Q^2$, hence the image of Q is a nonzero nilpotent element of $\ell[X]/P$.

(vi) $\Rightarrow$ (i) : This follows from Proposition 4.2.5 and Lemma 4.4.1. □

COROLLARY 4.4.7. *Let F/k be a field extension of finite degree. Then the k-algebra F is étale if and only if the field extension F/k is separable.*

PROOF. One implication has been proved in Proposition 4.2.5. So assume that the k-algebra F is étale. Then by Theorem 4.4.6 we have an isomorphism of k-algebras $F \simeq A = F_1 \times \cdots \times F_r$, where each F_i/k is a separable field extension. If $r \geq 2$, then A is not a domain, because

$$(1, 0, 0, \ldots, 0) \cdot (0, 1, 0, \ldots, 0) = 0 \in A.$$

As F is a domain, we must have $r = 1$. Thus $F \simeq F_1$ as a k-algebra, hence F is a separable extension of k. □

[2]here we use the following easy fact: if $R \to S$ is an injective morphism of k-algebras, then the induced morphism of ℓ-algebras $R \otimes_k \ell \to S \otimes_k \ell$ is injective.

PROPOSITION 4.4.8. *Assume that the field k is perfect, for instance of characteristic zero (Proposition 4.1.16) or finite (Proposition 4.1.17). Then a finite-dimensional k-algebra is étale if and only if it is reduced.*

PROOF. An étale k-algebra is in particular reduced by the criterion (v) in Theorem 4.4.6. Conversely, let A be a reduced finite-dimensional k-algebra. By Proposition 4.4.4, the k-algebra A is isomorphic to $F_1 \times \cdots \times F_r$, where $F_1, \ldots, F_r$ are finite field extensions of k. As k is perfect, each extension F_i/k is separable, hence each F_i is an étale k-algebra by Proposition 4.2.5. We conclude using Lemma 4.4.1 that the k-algebra $F_1 \times \cdots \times F_r$ is étale, and thus so is A. □

CHAPTER 5

The ring of integers

1. Integral closure in a separable extension

A fundamental property of the norm and trace functions is that they produce integers out of integers:

PROPOSITION 5.1.1. *Let A be a domain, with fraction field K. Let L/K be a finite separable extension, and $x \in L$ an element which is integral over A. Then the coefficients of the characteristic polynomial $\chi_{L/K}(x) \in K[X]$ are integral over A.*

PROOF. We apply Proposition 4.1.18 with $F/k = L/K$, and so find a field extension E/K $(= \ell/k)$ and n morphisms of K-algebras $\sigma_1, \dots \sigma_n \colon L \to E$. By Proposition 4.3.3 we have

$$\chi_{L/K}(x) = \prod_{i=1}^{n} (X - \sigma_i(x)) \in E[X]. \tag{5.1.a}$$

Let C be the integral closure of A in E. Then the elements $\sigma_1(x), \dots, \sigma_n(x) \in E$ are integral over A by Lemma 2.1.17, hence belong to C. Therefore the formula (5.1.a) implies that $\chi_{L/K}(x) \in C[X]$, as required. □

COROLLARY 5.1.2. *Let A be an integrally closed domain, with fraction field K. Let L/K be a finite separable extension, and B the integral closure of A in L. Then*

$$\mathrm{Tr}_{L/K}(B) \subset A \quad \textit{and} \quad \mathrm{N}_{L/K}(B) \subset A.$$

PROOF. This follows from Proposition 5.1.1, since the maps $\mathrm{Tr}_{L/K}$ and $\mathrm{N}_{L/K}$ are given by certain coefficients of the characteristic polynomial (Lemma 3.1.8). □

COROLLARY 5.1.3. *Let A be an integrally closed domain, with fraction field K. Let L/K be a finite separable extension, and B the integral closure of A in L. Let $b \in B$. Then*

$$b \in B^\times \iff \mathrm{N}_{L/K}(b) \in A^\times.$$

PROOF. Assume that $b \in B^\times$. Then by Corollary 5.1.2 we have $\mathrm{N}_{L/K}(b) \in A$ and $\mathrm{N}_{L/K}(b^{-1}) \in A$, and by Proposition 3.1.9

$$1 = \mathrm{N}_{L/K}(1) = \mathrm{N}_{L/K}(bb^{-1}) = \mathrm{N}_{L/K}(b)\,\mathrm{N}_{L/K}(b^{-1}).$$

In particular $\mathrm{N}_{L/K}(b) \in A^\times$.

Conversely, assume that $\mathrm{N}_{L/K}(b) \in A^\times$. Then by Proposition 5.1.1, we may write

$$\chi_{L/K}(b) = X^n + a_{n-1}X^{n-1} + \cdots + a_0, \quad \text{with } a_0, \dots, a_{n-1} \in A.$$

Recall that by Lemma 3.1.8 we have $a_0 = (-1)^n \mathrm{N}_{L/K}(b)$, and so $a_0 \in A^\times$. By the Cayley–Hamilton theorem (Proposition 3.1.6) we have

$$b^n + a_{n-1}b^{n-1} + \cdots + a_0 = 0 \in L.$$

Therefore

$$b(b^{n-1} + a_{n-1}b^{n-2} + \cdots + a_1) = -a_0 \in A^\times \subset B^\times,$$

so that $b \in B^\times$. □

Lemma 5.1.4. *Let A be an integrally closed domain, with fraction field K. Let L/K be a finite field extension, and B the integral closure of A in L. Then every element of L is of the form ba^{-1} with $b \in B$ and $a \in A \smallsetminus \{0\}$. In particular L is the fraction field of B.*

Proof. Let $x \in L$. Then x is algebraic over K, hence satisfies an equation of the form

$$a_m x^m + \cdots + a_0 = 0,$$

where $a_0, \ldots, a_m \in K$ are not all zero. Observe that $m > 0$. We may assume that $a_m \neq 0$. Multiplying with a (nonzero) common denominator of $a_0, \ldots, a_m$, we may assume that $a_0, \ldots, a_m \in A$. Multiplying with the nonzero element $a_m^{m-1} \in A$ and setting $y = a_m x \in K$, we obtain an equation

$$y^m + a_{m-1}y^{m-1} + a_m a_{m-2} y^{m-2} + \cdots + a_m^{m-1} a_0 = 0,$$

showing that the element $y \in L$ is integral over A, hence belongs to B. So $x = y(a_m)^{-1}$ is of the required form. □

Theorem 5.1.5. *Let A be an integrally closed domain, with fraction field K. Let L/K be a finite separable field extension, and B the integral closure of A in L. Then B contains a K-basis of L. Moreover there exists an A-submodule F of L, which is free of rank $[L : K]$ and which contains B.*

Proof. Let $n = [L : K]$, and $(e_1, \ldots, e_n)$ a K-basis of L. By Lemma 5.1.4, for each $i \in \{1, \ldots, n\}$ we may find a nonzero element $a_i \in A$ such that $x_i = a_i e_i \in B$. Then $(x_1, \ldots, x_n)$ is a K-basis $(x_1, \ldots, x_n)$ of L contained in B.

Recall that by Theorem 4.4.6 (and Proposition 4.2.5), the trace form $L \times L \to K$ is nondegenerate, hence by Lemma 4.4.5 we may find a K-basis $(y_1, \ldots, y_n)$ such that $\mathrm{Tr}_{L/K}(x_i y_j) = \delta_{ij}$ for all $i, j \in \{1, \ldots, n\}$ (we use the notation of (1.3.b)). Let $b \in B$, and write

$$b = b_1 y_1 + \cdots + b_n y_n, \quad \text{with } b_1, \ldots, b_n \in K.$$

Then for any $i \in \{1, \ldots, n\}$ we have $bx_i \in B$ (because $b \in B$ and $x_i \in B$), hence by Proposition 5.1.1 we have $\mathrm{Tr}_{L/K}(bx_i) \in A$. But by K-linearity of $\mathrm{Tr}_{L/K} \colon L \to K$ (see Proposition 3.1.9), we have

$$\mathrm{Tr}_{L/K}(bx_i) = \mathrm{Tr}_{L/K}\Big(\sum_{j=1}^{n} b_j x_i y_j\Big) = \sum_{j=1}^{n} b_j \,\mathrm{Tr}_{L/K}(x_i y_j) = b_i,$$

so that $b_i \in A$. It follows that the element b lies in the A-submodule F of L generated by the elements $y_1, \ldots, y_n$. We have proved that $B \subset F$. The system $(y_1, \ldots, y_n)$ is A-linearly independent in F, because its image in L is so (being K-linearly independent). Therefore the system $(y_1, \ldots, y_n)$ is an A-basis of F, and so the A-module F is free of rank n. □

Corollary 5.1.6. *Let A be a principal ideal domain, with fraction field K. Let L/K be a finite separable field extension, and B the integral closure of A in L. Then B is a free A-module of rank $[L : K]$.*

Proof. Let $n = [L : K]$. By Theorem 5.1.5, the A-module B is contained in a submodule F of L, which is free of rank n, and in addition the subset $B \subset L$ spans L as a K-vector space. By the implication (ii) $\Rightarrow$ (i) in Proposition 1.3.13 (applied with $V = L$) the A-module B is free of rank n. □

Example 5.1.7. Let K be a number field of degree $n = [K : \mathbb{Q}]$. Then the field extension $K/\mathbb{Q}$ is separable (Proposition 4.1.16), and the ring $\mathbb{Z}$ is a principal ideal domain. Thus by Corollary 5.1.6 the $\mathbb{Z}$-module $\mathcal{O}_K$ is free of rank n.

Lemma 5.1.8. *In the situation of Corollary 5.1.6, the following hold:*

(i) Let $(e_1, \dots, e_n)$ be an A-basis of B. Then $(e_1, \dots, e_n)$ is a K-basis of L.

(ii) For any $b \in B$, we have

$$\chi_{B/A}(b) = \chi_{L/K}(b) \in A[X] \subset K[X].$$

(iii) For any system $(x_1, \dots, x_n) \in B^n$, we have

$$\mathrm{D}_{B/A}(x_1, \dots, x_n) = \mathrm{D}_{L/K}(x_1, \dots, x_n) \in A \subset K.$$

Proof. (i): Assume that

$$\sum_{i=1}^{n} \lambda_i e_i = 0, \quad \text{with } \lambda_1, \dots, \lambda_n \in K.$$

Then we may find a nonzero element $a \in A$ such that $a\lambda_i \in A$ for each $i \in \{1, \dots, n\}$. The A-linear independence of $(e_1, \dots, e_n)$ implies that $a\lambda_i = 0$, and therefore $\lambda_i = 0$, for all $i \in \{1, \dots, n\}$. Thus the system $(e_1, \dots, e_n)$ is K-linearly independent in L, hence a K-basis of L since $\dim_K L = n$.

(ii): We pick an A-basis $(e_1, \dots, e_n)$ of B. The coefficients of the matrix of the K-linear map $l_b \colon L \to L$ in the K-basis $(e_1, \dots, e_n)$ are the images of those of the matrix of the A-linear map $l_b \colon B \to B$ in the A-basis $(e_1, \dots, e_n)$ under the inclusion $A \subset K$. Hence the characteristic polynomial of the former is the image of the characteristic polynomial of the latter under the inclusion $A[X] \subset K[X]$.

(iii)): By (ii), the coefficients of the matrix $(\mathrm{Tr}_{L/K}(x_i x_j))$ in $M_n(K)$ are the images of those of the matrix $(\mathrm{Tr}_{B/A}(x_i x_j))$ in $M_n(A)$. Taking determinants yields the statement. □

Definition 5.1.9. The *absolute discriminant* of a number field K is the integer

$$\mathrm{D}_{K/\mathbb{Q}}(x_1, \dots, x_n) = \mathrm{D}_{\mathcal{O}_K/\mathbb{Z}}(x_1, \dots, x_n) \in \mathbb{Z},$$

where $(x_1, \dots, x_n)$ is any $\mathbb{Z}$-basis of $\mathcal{O}_K$ (see Lemma 5.1.8). This integer does not depend on the choice of the basis by Lemma 3.2.2, because $\mathbb{Z}^\times = \{-1, 1\}$ and so the square of any invertible element of $\mathbb{Z}$ is 1.

Example 5.1.10. Consider the case of a quadratic field $K = \mathbb{Q}(\sqrt{d})$, with $d \in \mathbb{Z}$ square-free. Then Example 3.2.8 provides a computation of the absolute discriminant d_K of K:

$$d_K = \begin{cases} d & \text{if } d = 1 \mod 4 \\ 4d & \text{if } d = 2, 3 \mod 4. \end{cases}$$

2. Irreducibility of polynomials

The next proposition is a variant of the classical Gauss Lemma, which is sometimes referred to as "Dedekind's Prague Theorem":

Proposition 5.2.1. *Let A be an integrally closed domain with fraction field K. If $Q, R \in K[X]$ are monic polynomials such that $QR \in A[X]$, then $Q, R \in A[X]$.*

Proof. Let L/K be a field extension where $Q, R \in L[X]$ split into a product of linear factors (Proposition 4.1.8). Then we may write in $L[X]$

$$Q = \prod_{i=1}^{n}(X - \alpha_i) \quad \text{and} \quad R = \prod_{i=1}^{m}(X - \beta_i), \tag{5.2.a}$$

where $\alpha_1, \dots, \alpha_n, \beta_1, \dots, \beta_m \in L$ are the roots of Q, R (with repetitions allowed). These roots are then integral over A (being roots of the monic polynomial $P \in A[X]$), hence belong to the integral closure B of A in L. The formulas (5.2.a) then show that $Q, R \in B[X]$. Since A is integrally closed (in K), we have $B \cap K = A$. As $Q, R \in K[X]$, we conclude that $Q, R \in A[X] = B[X] \cap K[X] \subset L[X]$. □

Corollary 5.2.2. *Let A be an integrally closed domain with fraction field K. Let $P \in A[X]$ be a monic polynomial. Then the polynomial P is irreducible in $A[X]$ if and only if it is irreducible in $K[X]$.*

Proof. If P is irreducible in $K[X]$, it is so in $A[X]$. Indeed, if $P = QR$ with $Q, R \in A[X]$, then one of the polynomials Q, R has degree zero (because P is irreducible in $K[X]$), hence equals $u \in A \subset A[X]$. Since P is monic, it follows that u is a unit in A, hence in $A[X]$.

Conversely, assume that P is irreducible in $A[X]$. We assume that $P = QR$ with $Q, R \in K[X]$, and show that one of Q, R is a unit in $K[X]$. Let $q, r \in K$ be the leading coefficients of Q, R. Since the polynomial P is monic, we have $qr = 1$. Replacing Q with rQ, and R with qR, we may assume that the polynomials Q and R are monic. By Proposition 5.2.1 we have $Q, R \in A[X]$. Since P is irreducible in $A[X]$, one of the elements Q, R must be a unit in $A[X]$, and a fortiori also in $K[X]$. □

Corollary 5.2.3 (Eisenstein's criterion). *Let A be an integrally closed domain, and $\mathfrak{p}$ a prime ideal of A. Consider a monic polynomial*

$$P = X^n + a_{n-1}X^{n-1} + \cdots + a_0 \in A[X]$$

where $a_0, \dots, a_{n-1} \in A$. Assume that $a_i \in \mathfrak{p}$ for all $i = 0, \dots, n-1$, but that $a_0 \notin \mathfrak{p}^2$. Then P is irreducible in $K[X]$, where K is the fraction field of A.

Proof. By Corollary 5.2.2, it will suffice to prove that P is irreducible in $A[X]$. Let us write $P = FG$ in $A[X]$, with F, G monic. Consider the quotient ring $C = A/\mathfrak{p}$, and denote by $\overline{Q} \in C[X]$ the image of a polynomial in $Q \in A[X]$. In $C[X]$ we have $\overline{P} = X^n$ (by the assumption) and $\overline{P} = \overline{F} \cdot \overline{G}$. As the ring C is a domain, it follows from Lemma 3.1.4 that $\overline{F}$ and $\overline{G}$ are powers of X in $C[X]$. Thus $F - X^r \in \mathfrak{p}A[X]$ and $G - X^s \in \mathfrak{p}A[X]$, where $r = \deg F$ and $s = \deg G$. If F and G are both nonconstant, then $r > 0$ and $s > 0$, and so $F(0) \in \mathfrak{p}$ and $G(0) \in \mathfrak{p}$. Thus

$$a_0 = P(0) = F(0)G(0) \in \mathfrak{p}^2,$$

which contradicts the assumption. □

3. Cyclotomic fields

In this section p will be a prime number, and $\xi \in \mathbb{C}$ a primitive p-th root of unity. This means that $\xi^p = 1$ and $\xi \neq 1$. We investigate the *cyclotomic field* $K = \mathbb{Q}(\xi) \subset \mathbb{C}$, and its ring of integers $\mathcal{O}_K$.

Consider the *cyclotomic polynomial*

$$\Phi_p = X^{p-1} + \cdots + 1 \in \mathbb{Z}[X], \tag{5.3.a}$$

which satisfies the relation

$$X^p - 1 = (X-1)\Phi_p \in \mathbb{Z}[X]. \tag{5.3.b}$$

The image of Φ_p in $K[X]$ admits $\xi, \ldots, \xi^{p-1} \in K$ as roots and thus

$$\Phi_p = (X-\xi)\cdots(X-\xi^{p-1}) \in K[X]. \tag{5.3.c}$$

Lemma 5.3.1. *The polynomial Φ_p is irreducible in $\mathbb{Q}[X]$.*

Proof. Set $Y = X - 1 \in \mathbb{Z}[X]$. Then, in $\mathbb{Z}[X]$ we have

$$Y\Phi_p = X^p - 1 = (Y+1)^p - 1 = Y^p + \sum_{i=1}^{p-1} \binom{p}{i} Y^i.$$

Since Y is nonzero and $\mathbb{Z}[X]$ is a domain, we deduce that

$$\Phi_p = F(Y) \quad \text{where } F(T) = T^{p-1} + \sum_{i=1}^{p-1} \binom{p}{i} T^{i-1} \in \mathbb{Z}[T]. \tag{5.3.d}$$

Now that binomial coefficient $\binom{p}{i}$ is divisible by p for $i = 1, \ldots, p-1$ (classical exercise), and $\binom{p}{1} = p$ is not divisible by p^2. Therefore by Eisenstein's criterion (Corollary 5.2.3), the polynomial F is irreducible in $\mathbb{Q}[T]$. Since $\Phi_p \in \mathbb{Q}[X]$ is the image of $F \in \mathbb{Q}[T]$ under the ring isomorphism $\mathbb{Q}[T] \mapsto \mathbb{Q}[X]$ given by $T \mapsto X - 1$, this implies that Φ_p is irreducible in $\mathbb{Q}[X]$. □

Lemma 5.3.1 implies that the mapping $X \mapsto \xi$ induces an isomorphism of $\mathbb{Q}$-algebras

$$\mathbb{Q}[X]/\Phi_p \simeq K. \tag{5.3.e}$$

In particular K is a number field of degree $p-1$, and a $\mathbb{Q}$-basis of K is given by $1, \xi, \ldots, \xi^{p-2}$. It follows from (5.3.c) that we have morphisms of $\mathbb{Q}$-algebras

$$\sigma_i \colon K \to K, \quad \xi \mapsto \xi^i$$

for $i \in \{1, \ldots, p-1\}$. Those are pairwise distinct, and there are $p - 1 = [K : \mathbb{Q}]$ of them. (So in the notation of Definition 4.2.2, we have $n = p-1$, and $k = \mathbb{Q}$, $A = K$, $\ell = K$.)

Lemma 5.3.2. *We have*

(i) $\mathrm{Tr}_{K/\mathbb{Q}}(1) = p - 1$,

(ii) $\mathrm{Tr}_{K/\mathbb{Q}}(\xi^j) = -1$ *for* $j \in \{1, \ldots, p-1\}$,

Proof. Observe that for $j \in \{0, \ldots, p-1\}$ we have $\sigma_i(\xi^j) = \xi^{ij}$ for all $i \in \{1, \ldots, p-1\}$. Using the formula of Proposition 4.3.3, we have

$$\mathrm{Tr}_{K/\mathbb{Q}}(\xi^j) = \sum_{i=1}^{p-1} \sigma_i(\xi^j) = \sum_{i=1}^{p-1} \xi^{ij} = \Phi_p(\xi^j) - 1.$$

Now $\Phi_p(\xi^j) = 0$ when $j \in \{1, \dots, p-1\}$ (see (5.3.c)), while $\Phi_p(\xi^0) = \Phi_p(1) = p$. This yields (i) and (ii). (Alternatively (i) follows directly from Proposition 3.1.9 (iii).). □

Lemma 5.3.3. *We have*

$$\mathrm{N}_{K/\mathbb{Q}}(\xi) = (-1)^{p-1}.$$

Proof. By Proposition 4.3.3, we have

$$\mathrm{N}_{K/\mathbb{Q}}(\xi) = \prod_{i=1}^{p-1} \xi^i = \xi^{1+\cdots+(p-1)} = \xi^{\frac{p(p-1)}{2}}.$$

If p is odd, this equals $(\xi^p)^{(p-1)/2} = 1 = (-1)^{p-1}$. If $p = 2$, this equals $\xi = -1 = (-1)^{p-1}$. □

Lemma 5.3.4. *We have*

$$\mathrm{N}_{K/\mathbb{Q}}(1-\xi) = (1-\xi)\dots(1-\xi^{p-1}) = p.$$

Proof. We have

$$\begin{aligned} \mathrm{N}_{K/\mathbb{Q}}(1-\xi) &= (1-\xi)\dots(1-\xi^{p-1}) && \text{by Proposition 4.3.3} \\ &= \Phi_p(1) && \text{by (5.3.c)} \\ &= p && \text{by (5.3.a).} \end{aligned}$$ □

Lemma 5.3.5. *We have*

$$\mathbb{Z} \cap (1-\xi)\mathcal{O}_K = p\mathbb{Z}.$$

Proof. By Lemma 5.3.4 we have $p\mathbb{Z} \subset \mathbb{Z} \cap (1-\xi)\mathcal{O}_K$. If this inclusion were not an equality, we would have $\mathbb{Z} = \mathbb{Z} \cap (1-\xi)\mathcal{O}_K$ (as $p\mathbb{Z}$ is a maximal ideal of $\mathbb{Z}$). In particular $1 = (1-\xi)\alpha$ for some $\alpha \in \mathcal{O}_K$. Taking the norms yields, in view of Lemma 5.3.4

$$1 = \mathrm{N}_{K/\mathbb{Q}}(1) = \mathrm{N}_{K/\mathbb{Q}}(1-\xi) \cdot \mathrm{N}_{K/\mathbb{Q}}(\alpha) = p\,\mathrm{N}_{K/\mathbb{Q}}(\alpha).$$

This is a contraction, as $\mathrm{N}_{K/\mathbb{Q}}(\alpha) \in \mathbb{Z}$ by Corollary 5.1.2 (in view of Remark 2.1.12). □

Lemma 5.3.6. *We have*

$$\mathrm{Tr}_{K/\mathbb{Q}}((1-\xi)\mathcal{O}_K) \subset p\mathbb{Z}.$$

Proof. Let $y \in \mathcal{O}_K$. Then the elements $\sigma_i(y) \in \mathbb{C}$, for $i \in \{1, \dots, p-1\}$, are also integral over $\mathbb{Z}$ by Lemma 2.1.17, hence belong to $\mathcal{O}_K$. Thus

$$\begin{aligned} \mathrm{Tr}_{K/\mathbb{Q}}((1-\xi)y) &= \sum_{i=1}^{p-1} \sigma_i((1-\xi)y) \\ &= \sum_{i=1}^{p-1} (1-\xi^i)\sigma_i(y) \\ &= (1-\xi)\sum_{i=1}^{p-1} (\xi^{i-1} + \cdots + 1)\sigma_i(y) \end{aligned}$$

belongs to $(1-\xi)\mathcal{O}_K$. On the other hand $\mathrm{Tr}_{K/\mathbb{Q}}((1-\xi)y) \in \mathbb{Z}$ by Corollary 5.1.2, and we conclude using Lemma 5.3.5. □

Proposition 5.3.7. *For the number field $K = \mathbb{Q}(\xi)$, we have $\mathbb{Z}[\xi] = \mathcal{O}_K$, and $(1, \dots, \xi^{p-2})$ is a $\mathbb{Z}$-basis of $\mathbb{Z}[\xi]$.*

Proof. Since $\xi^{p-1} = -1 - \cdots - \xi^{p-2}$ (because $\Phi_p(\xi) = 0$), it follows that the family $1, \ldots, \xi^{p-2}$ generates the $\mathbb{Z}$-module $\mathbb{Z}[\xi]$. This family is $\mathbb{Z}$-linearly independent, because it is $\mathbb{Q}$-linearly independent in K. It remains to prove that $\mathbb{Z}[\xi] = \mathcal{O}_K$. It will suffice to show that $\mathcal{O}_K \subset \mathbb{Z}[\xi]$, since the other inclusion is clear.

For $j \in \mathbb{N}$, let $Q_j \subset K$ be the $\mathbb{Q}$-subspace generated by $1, \ldots, \xi^{j-1}$, and $Z_j \subset K$ the $\mathbb{Z}$-submodule generated by $1, \ldots, \xi^{j-1}$. We show by induction on $j \leq p-1$ that

$$Q_j \cap \mathcal{O}_K \subset Z_j.$$

The proposition then follows from the case $j = p-1$, since $Q_{p-1} = K$ and $Z_{p-1} = \mathbb{Z}[\xi]$.

The case $j = 0$ is trivial, since $Z_0 = 0 = Q_0$. Assume that $j \in \{1, \ldots, p-1\}$. Let $y \in Q_j \cap \mathcal{O}_K$, and write

$$y = a_0 + a_1\xi + \cdots + a_{j-1}\xi^{j-1},$$

with $a_0, \ldots, a_{j-1} \in \mathbb{Q}$. Then we have

$$(1-\xi)y = a_0(1-\xi) + \cdots + a_{j-1}(\xi^{j-1} - \xi^j).$$

Let us take the trace, having Lemma 5.3.2 in mind. This yields

$$\mathrm{Tr}_{K/\mathbb{Q}}((1-\xi)y) = a_0 p.$$

Since by assumption $y \in \mathcal{O}_K$, we have $a_0 p \in p\mathbb{Z}$ by Lemma 5.3.6, which implies that $a_0 \in \mathbb{Z}$. Now $\xi^{-1} = \xi^{p-1} \in \mathcal{O}_K$, and thus

$$\xi^{-1}(y - a_0) = a_1 + \cdots + a_{j-1}\xi^{j-2} \in Q_{j-1} \cap \mathcal{O}_K.$$

By induction, this element belongs to Z_{j-1}, hence

$$y \in a_0\mathbb{Z} + \xi Z_{j-1} \subset Z_j.$$

This concludes the inductive proof. □

Lemma 5.3.8. *The absolute discriminant d_K of the number field $K = \mathbb{Q}(\xi)$ is $(-1)^{\frac{(p-1)(p-2)}{2}} p^{p-2}$; in other words*

$$d_K = \begin{cases} 1 & \text{if } p = 2 \\ p^{p-2} & \text{if } p = 1 \mod 4 \\ -p^{p-2} & \text{if } p = 3 \mod 4. \end{cases}$$

Proof. Recall from (5.3.e) that the mapping $X \mapsto \xi$ induces an isomorphism of k-algebras $\mathbb{Q}[X]/\Phi_p \xrightarrow{\sim} K$. By Proposition 4.3.5 (in view of Lemma 3.2.4), we have

$$\mathrm{D}_{\mathcal{O}_K/\mathbb{Z}}(1, \xi, \ldots, \xi^{p-2}) = (-1)^{\frac{(p-1)(p-2)}{2}} \mathrm{N}_{K/\mathbb{Q}}(\Phi_p'(\xi)). \tag{5.3.f}$$

Taking the derivative of the formula (5.3.b), we have

$$pX^{p-1} = \Phi_p + (X-1)\Phi_p'.$$

Evaluating at $X = \xi$ yields, as $\Phi_p(\xi) = 0$,

$$p\xi^{p-1} = (\xi - 1)\Phi_p'(\xi). \tag{5.3.g}$$

Observe that, by Proposition 3.1.9 and Lemma 5.3.4, we have

$$\mathrm{N}_{K/\mathbb{Q}}(\xi - 1) = \mathrm{N}_{K/\mathbb{Q}}((-1)(1-\xi)) = (-1)^{p-1}\mathrm{N}_{K/\mathbb{Q}}(1-\xi) = (-1)^{p-1}p.$$

Now, by Lemma 5.3.3 and Proposition 3.1.9, we have

$$\mathrm{N}_{K/\mathbb{Q}}(\xi^{p-1}) = \mathrm{N}_{K/\mathbb{Q}}(\xi)^{p-1} = ((-1)^{p-1})^{p-1} = (-1)^{p-1}.$$

Taking norms in (5.3.g) thus yields (in view of Proposition 3.1.9)

$$p^{p-1}(-1)^{p-1} = (-1)^{p-1} p \, \mathrm{N}_{K/\mathbb{Q}}(\Phi_p'(\xi)),$$

and therefore

$$\mathrm{N}_{K/\mathbb{Q}}(\Phi_p'(\xi)) = p^{p-2}.$$

Plugging this equation into (5.3.f) yields the result. □

CHAPTER 6

Dedekind domains

In this chapter, we introduce Dedekind domains, which are generalisations of principal ideal domains. The ring of integers of a number field is often not a principal ideal domain, but it is always a Dedekind domain. In such rings, unique factorisation of elements into a product of irreducible ones does not necessarily hold; as a substitute we have a unique factorisation of ideals into a product of prime ideals.

1. Integral closure of a Dedekind domain

DEFINITION 6.1.1. An domain A is called a *Dedekind domain* if the following conditions are satisfied:

(a) the ring A is integrally closed,
(b) the ring A is noetherian,
(c) every nonzero prime ideal of A is maximal.

REMARK 6.1.2. In particular, every field is a Dedekind domain. In some references, the definition of a Dedekind domain explicitly excludes the case of fields. In any case, most statements involving Dedekind domains that we will formulate become vacuous or trivial in the case of fields.

REMARK 6.1.3. It follows from Lemma 1.2.10 that every nonzero ideal of a Dedekind domain is contained in only finitely many prime ideals. (Indeed, all such prime ideals are nonzero, hence maximal ideals; there are thus no inclusion relations between them.)

PROPOSITION 6.1.4. *Every principal ideal domain is a Dedekind domain.*

PROOF. Let A be a principal ideal domain. We know that the ring A is noetherian (Proposition 1.2.6) and integrally closed (Proposition 2.1.11). To conclude the proof, we let $\mathfrak{p}$ be a nonzero prime ideal of A, and prove that $\mathfrak{p}$ is a maximal ideal of A. We may write $\mathfrak{p} = aA$ for some nonzero element $a \in A$. If J is an ideal of A such that $\mathfrak{p} \subset J$, then $J = bA$ for some $b \in A$. Since $a \in J$, we may find $c \in A$ such that $a = bc$. Now since $bc \in \mathfrak{p}$ and the ideal $\mathfrak{p}$ is prime, we must have $c \in \mathfrak{p}$ or $b \in \mathfrak{p}$. If $b \in \mathfrak{p}$, then $\mathfrak{p} = J$. If $c \in \mathfrak{p}$, then $c = ad$ for some $d \in A$, so that $a = bc = abd$. Thus $a(1 - bd) = 0$, and since a is nonzero and A is a domain, we have $bd = 1$. Therefore $1 \in J$, and thus $J = A$. □

REMARK 6.1.5. In particular Proposition 6.1.4 implies that the ring $\mathbb{Z}$ is Dedekind domain.

THEOREM 6.1.6. *Let A be a Dedekind domain, with fraction field K. Let L/K be a finite separable field extension, and B the integral closure of A in L. Then B is a Dedekind domain with fraction field L, and finitely generated as an A-module.*

Proof. The fact that L is the fraction field of B was proved in Lemma 5.1.4. Thus, by construction the ring B is an integrally closed domain (see Remark 2.1.16). Since B is a submodule of a finitely generated A-module by Theorem 5.1.5, it follows from Corollary 1.2.5 that B is a finitely generated A-module. Moreover Corollary 1.2.5 implies that the A-module B is noetherian. In particular the ring B is noetherian (because ideals of B are in particular A-submodules of B).

Now let $\mathfrak{q}$ be a nonzero prime ideal of B. Set $\mathfrak{p} = \mathfrak{q} \cap A$. Then the ideal $\mathfrak{p}$ of A is prime by Lemma 1.1.2, and nonzero by Lemma 2.1.19. As A is a Dedekind domain, the ideal $\mathfrak{p}$ is maximal. Now the ring extension $A/\mathfrak{p} \subset B/\mathfrak{q}$ is integral (Lemma 2.1.18), and $A/\mathfrak{p}$ is a field. It then follows from Proposition 2.1.20 that $B/\mathfrak{q}$ is a field, or equivalently that $\mathfrak{q}$ is a maximal ideal of B. □

Corollary 6.1.7. *If K is a number field, then its ring of integers $\mathcal{O}_K$ is a Dedekind domain.*

2. Fractional ideals

Definition 6.2.1. Let A be a domain, with fraction field K. A *fractional ideal* of A is an A-submodule I of K such that there exists a nonzero element $d \in A$ satisfying $dI \subset A$. Such an element d will be called a *common denominator* of I.

Proposition 6.2.2. *Let A be a noetherian domain, with fraction field K, and I an A-submodule of K. Then I is a fractional ideal of A if and only if the A-module I is finitely generated.*

Proof. Assume that the A-module I is finitely generated, and let $a_1, \dots, a_n$ be a family of elements generating I as an A-module. For each $i \in \{1, \dots, n\}$ we may find an element d_i such that $d_i a_i \in A$. Then it is easy to verify that the product $d_1 \cdots d_n$ is a common denominator of I.

Conversely, assume that I is a fractional ideal of A. Let $d \in A$ be nonzero and such that $dI \subset A$. Then the ideal dI in the noetherian ring A is finitely generated, say by $a_1, \dots, a_n \in dI$. Then the elements $d^{-1}a_1, \dots, d^{-1}a_n \in K$ belong to I (if $x \in dI$, then $d^{-1}x \in I$), and they generate the A-module I. □

If I, J are A-submodules of K, the notation IJ refers to the A-submodule of K generated by the elements ij for $i \in I$ and $j \in J$. Observe that if I and J are fractional ideals, then so is IJ. This allows us to define the product

$$\prod_{i=1}^{n} I_i = I_1 \cdots I_n$$

of fractional ideals $I_1, \dots, I_n$, as well as the powers I^n for $n \in \mathbb{N}$ of a fractional ideal I.

Definition 6.2.3. We will denote by $\mathcal{F}(A)$ the set of nonzero fractional ideals of A. This set forms a commutative monoid, where the operation is given by the product of ideals, and the neutral element by the fractional ideal A itself.

3. Prime decomposition in Dedekind domains

In this section A will be a Dedekind domain with fraction field K.

Lemma 6.3.1. *If I, J are nonzero fractional ideals of A such that $IJ \subset I$, then $J \subset A$.*

PROOF. Let $x \in J$. Then $xI \subset I$, hence $x^n I \subset I$ for all $n \in \mathbb{N}$ by induction on n. Let i be a nonzero element of I, and $d \in A \smallsetminus \{0\}$ be such that $dI \subset A$. Then $dix^n \in dI \subset A$ for all $n \in \mathbb{N}$, hence the A-submodule $A[x] \subset K$ is a fractional ideal of A, with common denominator di. By Proposition 6.2.2, this A-module is finitely generated, so that $x \in K$ is integral over A by Proposition 2.1.6. As the ring A is integrally closed, we deduce that $x \in A$. □

PROPOSITION 6.3.2. *Every nonzero prime ideal of A is invertible in the monoid $\mathcal{F}(A)$.*

PROOF. Let $\mathfrak{p}$ be a nonzero prime ideal of A. Since A is a Dedekind domain, the ideal $\mathfrak{p}$ is maximal. Set

$$J = \{x \in K | x\mathfrak{p} \subset A\}. \tag{6.3.a}$$

Note that J is a fractional ideal of A: any nonzero element of $\mathfrak{p}$ provides a common denominator. Certainly $A \subset J$ and $\mathfrak{p}J \subset A$. Thus $\mathfrak{p} = \mathfrak{p}A \subset \mathfrak{p}J \subset A$. As $\mathfrak{p}$ is a maximal ideal in A, we have either $\mathfrak{p} = \mathfrak{p}J$, or $\mathfrak{p}J = A$. If $\mathfrak{p}J = A$, then J is the inverse of $\mathfrak{p}$, as required. To conclude the proof, we assume that $\mathfrak{p} = \mathfrak{p}J$ and come to a contradiction. It follows from

Since $\mathfrak{p}J \subset \mathfrak{p}$, we have $J \subset A$ by Lemma 6.3.1. Let us now choose a nonzero element $a \in \mathfrak{p}$. Then the ideal aA contains a product $\mathfrak{p}_1 \cdots \mathfrak{p}_n$ of nonzero prime ideals $\mathfrak{p}_1, \ldots, \mathfrak{p}_n$ by Lemma 1.2.9. We may assume that n is so chosen as to be minimal. Then $\mathfrak{p}_1 \cdots \mathfrak{p}_n \subset aA \subset \mathfrak{p}$, and so by Lemma 1.1.3 the ideal $\mathfrak{p}$ contains the ideal $\mathfrak{p}_i$ for some $i \in \{1, \ldots, n\}$. As $\mathfrak{p}_i$ is nonzero and A is a Dedekind domain, the ideal $\mathfrak{p}_i$ is maximal, and therefore $\mathfrak{p} = \mathfrak{p}_i$. Let

$$I = \prod_{j \neq i} \mathfrak{p}_j.$$

Then $I \not\subset aA$ by minimality of n. We may thus find an element $b \in I$ such that $b \notin aA$. As $\mathfrak{p}I = \mathfrak{p}_1 \cdots \mathfrak{p}_n \subset aA$, we have $b\mathfrak{p} \subset aA$, and so $a^{-1}b\mathfrak{p} \subset A$. By (6.3.a), this implies that $a^{-1}b \in J$. On the other hand, as $b \notin aA$, we have $a^{-1}b \notin A$. We conclude that $J \not\subset A$, which is the required contradiction. □

COROLLARY 6.3.3. *Let $\mathfrak{p}$ be a maximal ideal of A. Then for all $n \in \mathbb{N}$, we have $\mathfrak{p}^n \neq \mathfrak{p}^{n+1}$.*

PROOF. By Proposition 6.3.2, we find a fractional ideal I of A such that $\mathfrak{p}I = A$. If $\mathfrak{p}^n = \mathfrak{p}^{n+1}$, then $A = I^n\mathfrak{p}^n = I^n\mathfrak{p}^{n+1} = \mathfrak{p}$, a contradiction. □

LEMMA 6.3.4. *Every nonzero ideal of A is a product of nonzero prime ideals of A (possibly not pairwise distinct).*

PROOF. Consider the set Φ of nonzero ideals of A which cannot be written as products of nonzero prime ideals. To prove the statement, we assume that Φ is nonempty. Since the ring A is noetherian, the set Φ admits a maximal element J (for the inclusion of ideals). Then $J \neq A$ (because A is the product of the empty family of nonzero prime ideals). The family of ideals of A containing J and unequal to A is nonempty, hence admits a maximal element $\mathfrak{m}$, since the ring A is noetherian. Observe that $\mathfrak{m}$ is a maximal ideal of A. Thus by Proposition 6.3.2 the fractional ideal $\mathfrak{m}$ admit an inverse $\mathfrak{m}^{-1}$ in the monoid $\mathcal{F}(A)$. From the inclusion $J \subset \mathfrak{m}$, we deduce that $J\mathfrak{m}^{-1} \subset \mathfrak{m}\mathfrak{m}^{-1} = A$, so that $J\mathfrak{m}^{-1}$ is an ideal of A. From the inclusion $\mathfrak{m} \subset A$, we deduce that $A = \mathfrak{m}\mathfrak{m}^{-1} \subset \mathfrak{m}^{-1}$, and so $J \subset J\mathfrak{m}^{-1}$.

Next we claim that $J \neq J\mathfrak{m}^{-1}$. Indeed, assume that $J = J\mathfrak{m}^{-1}$. Then Lemma 6.3.1 implies that $\mathfrak{m}^{-1} \subset A$. Multiplying with $\mathfrak{m}$ yields $A \subset \mathfrak{m}$, a contradiction.

Thus $J \subsetneq J\mathfrak{m}^{-1}$. From the choice of J, it follows that the ideal $J\mathfrak{m}^{-1}$ can be written as a product of nonzero prime ideals. Multiplying with the nonzero prime ideal $\mathfrak{m}$ shows that the same is true for the ideal J, a contradiction. □

THEOREM 6.3.5. *Let A be a Dedekind domain and I a nonzero fractional ideal of A. Let us denote by P the set of nonzero prime ideals of A. Then there exist integers $n_\mathfrak{p} \in \mathbb{Z}$ for each $\mathfrak{p} \in P$ such that the set $\{\mathfrak{p} \in P | n_\mathfrak{p} \neq 0\}$ is finite, and*

$$I = \prod_{\mathfrak{p} \in P} \mathfrak{p}^{n_\mathfrak{p}}.$$

In addition, the integers $n_\mathfrak{p}$ are uniquely determined by the fractional ideal I, and are all positive if I is an ideal of A.

PROOF. By assumption, there exists a nonzero element $d \in A$ such that $dI \subset A$. By Lemma 6.3.4, we may write

$$dI = \prod_{\mathfrak{p} \in P} \mathfrak{p}^{m_\mathfrak{p}} \quad \text{and} \quad dA = \prod_{\mathfrak{p} \in P} \mathfrak{p}^{d_\mathfrak{p}}.$$

Thus

$$I = I \cdot \prod_{\mathfrak{p} \in P} \mathfrak{p}^{d_\mathfrak{p}} \cdot \prod_{\mathfrak{p} \in P} \mathfrak{p}^{-d_\mathfrak{p}} = I \cdot (dA) \cdot \prod_{\mathfrak{p} \in P} \mathfrak{p}^{-d_\mathfrak{p}} = (dI) \cdot \prod_{\mathfrak{p} \in P} \mathfrak{p}^{-d_\mathfrak{p}} = \prod_{\mathfrak{p} \in P} \mathfrak{p}^{m_\mathfrak{p} - d_\mathfrak{p}},$$

proving the "existence" part of the statement.

Let us now prove the "unicity" part. Let us assume that

$$\prod_{\mathfrak{p} \in P} \mathfrak{p}^{n_\mathfrak{p}} = \prod_{\mathfrak{p} \in P} \mathfrak{p}^{m_\mathfrak{p}}, \tag{6.3.b}$$

and prove that $n_\mathfrak{p} = m_\mathfrak{p}$ for all $\mathfrak{p} \in P$. Let $P_+ \subset P$ be the subset consisting of those $\mathfrak{p}$ such that $n_\mathfrak{p} > m_\mathfrak{p}$, and $P_- \subset P$ the subset consisting of those $\mathfrak{p}$ such that $n_\mathfrak{p} < m_\mathfrak{p}$. Then $P_+ \cap P_- = \varnothing$, hence multiplying (6.3.b) with the fractional ideal

$$\prod_{\mathfrak{p} \in P \smallsetminus P_+} \mathfrak{p}^{-n_\mathfrak{p}} \prod_{\mathfrak{p} \in P_+} \mathfrak{p}^{-m_\mathfrak{p}} = \prod_{\mathfrak{p} \in P_-} \mathfrak{p}^{-n_\mathfrak{p}} \prod_{\mathfrak{p} \in P \smallsetminus P_-} \mathfrak{p}^{-m_\mathfrak{p}}$$

yields an equality of ideals

$$\prod_{\mathfrak{p} \in P_+} \mathfrak{p}^{n_\mathfrak{p} - m_\mathfrak{p}} = \prod_{\mathfrak{p} \in P_-} \mathfrak{p}^{m_\mathfrak{p} - n_\mathfrak{p}}. \tag{6.3.c}$$

Assume that the set P_+ is nonempty. Then the set P_+ contains an element $\mathfrak{q}_+$, and the left hand side of (6.3.c) is contained in $\mathfrak{q}_+$. Therefore the ideal $\mathfrak{q}_+$ contains the right hand side of (6.3.c), and it follows from Lemma 1.1.3 that $\mathfrak{q}_+$ contains some ideal $\mathfrak{q}_- \in P_-$. But the ideal $\mathfrak{q}_-$ is maximal, which implies that $\mathfrak{q}_+ = \mathfrak{q}_-$. Therefore $P_+ \cap P_- \neq \varnothing$, a contradiction. We have proved that $P_+ = \varnothing$. An analog argument shows that $P_- = \varnothing$, which concludes the proof of the unicity.

The "positivity" part of the statement follows from Lemma 6.3.4. □

COROLLARY 6.3.6. *Let A be a Dedekind domain. The monoid $\mathcal{F}(A)$ of nonzero fractional ideals of A is an abelian group. As such, it is freely generated by the nonzero prime ideals of A.*

The next lemma will not be used, but may help clarify the situation:

LEMMA 6.3.7. *Let I a nonzero fractional ideal of A. Then the inverse of I in the group $\mathcal{F}(A)$ is given by*

$$I^{-1} = \{x \in K | xI \subset A\}.$$

PROOF. Let $J = \{x \in K | xI \subset A\}$. Then clearly $JI \subset A$. On the other hand, by Corollary 6.3.6 the fractional ideal I admits an inverse I^{-1}, which satisfies $I^{-1}I = A$. In particular every $x \in I^{-1}$ is such that $xI \in A$, and so $I^{-1} \subset J$. Therefore $A = I^{-1}I \subset JI$. We have proved that $JI = A$, hence $J = I^{-1}$. □

DEFINITION 6.3.8. Let A be a Dedekind domain, and I a nonzero fractional ideal of A. For each nonzero prime ideal $\mathfrak{p}$ of A, we will denote by $v_{\mathfrak{p}}(I) \in \mathbb{Z}$ the integer $n_{\mathfrak{p}}$ appearing in Theorem 6.3.5.

PROPOSITION 6.3.9. *Let I, J be nonzero fractional ideals of A. Then:*

(i) We have $v_{\mathfrak{p}}(IJ) = v_{\mathfrak{p}}(I) + v_{\mathfrak{p}}(J)$ for each nonzero prime ideal $\mathfrak{p}$ of A.

(ii) We have $J \subset I$ if and only if $v_{\mathfrak{p}}(I) \leq v_{\mathfrak{p}}(J)$ for each nonzero prime ideal $\mathfrak{p}$ of A.

PROOF. (i): This clear from the unicity in Theorem 6.3.5.

(ii): The relation $J \subset I$ implies by Corollary 6.3.6 that $I^{-1}J \subset I^{-1}I = A$. Therefore by (i), and the last words of Theorem 6.3.5, we have for each nonzero prime ideal $\mathfrak{p}$ of A

$$0 \leq v_{\mathfrak{p}}(I^{-1}J) = v_{\mathfrak{p}}(J) - v_{\mathfrak{p}}(I).$$

This proves one implication; the other one is easy. □

PROPOSITION 6.3.10. *Let I be a nonzero fractional ideal of A, and $\mathfrak{p}$ a nonzero prime ideal of A. Then the $(A/\mathfrak{p})$-vector space $I/I\mathfrak{p}$ has dimension one.*

PROOF. The $(A/\mathfrak{p})$-subspaces of $I/I\mathfrak{p}$ are its A-submodules, which are in bijection with the A-submodules of I containing $I\mathfrak{p}$, in other words the fractional ideals J of A such that $I\mathfrak{p} \subset J \subset I$ (note that any A-submodule of I is a fractional ideal). Multiplying by I^{-1}, we see that $\mathfrak{p} \subset I^{-1}J \subset A$ for such fractional ideals J. Since the ideal $\mathfrak{p}$ is maximal in A, this implies that $I^{-1}J = \mathfrak{p}$ or $I^{-1}J = A$, in other words that $J = I\mathfrak{p}$ or $J = I$. Therefore the $(A/\mathfrak{p})$-vector space $I/I\mathfrak{p}$ has exactly two subspaces, so it is of dimension one □

DEFINITION 6.3.11. Let A be a Dedekind domain, with fraction field K. A fractional ideal of A is called *principal* if it is of the form dA for some $d \in K$. The subset of nonzero principal fractional ideals forms a subgroup $\mathcal{P}(A)$ of $\mathcal{F}(A)$. The quotient group

$$\mathcal{C}(A) = \mathcal{F}(A)/\mathcal{P}(A)$$

is called the *ideal class group* of A.

The ideal class group measures the failure of the ring A from being principal:

PROPOSITION 6.3.12. *A Dedekind domain A is a principal ideal domain if and only if $\mathcal{C}(A) = 0$.*

PROOF. Clearly if $\mathcal{C}(A) = 0$, then each nonzero fractional ideal of A is principal, and in particular each ideal of A is principal.

Conversely, assume that A is a principal ideal domain. Let I be a nonzero fractional ideal of A. Pick a nonzero element $d \in A$ such that $dI \subset A$. Then $dI = aA$ for some $a \in A$, so that the fractional ideal $I = (ad^{-1})A$ is principal. Thus $\mathcal{C}(A) = 0$. □

PROPOSITION 6.3.13. *A Dedekind domain having only finitely many prime ideals is a principal ideal domain.*

PROOF. Let A be a Dedekind domain. By Lemma 6.3.4, it suffices to prove that each maximal ideal of A is principal. So let $\mathfrak{p}$ be a maximal ideal of A. As $\mathfrak{p} \neq \mathfrak{p}^2$ (Corollary 6.3.3), by prime avoidance (Lemma 1.1.4), we may pick $x \in \mathfrak{p}$ such that $x \notin (\mathfrak{p}^2 \cup \mathfrak{q}_1 \cup \cdots \cup \mathfrak{q}_n)$, where $\mathfrak{q}_1, \ldots \mathfrak{q}_n$ are the nonzero prime ideals of A different from $\mathfrak{p}$. Then the decomposition of the ideal xA given by Theorem 6.3.5 can only be $xA = \mathfrak{p}$. □

REMARK 6.3.14. Observe that the ring $\mathbb{Z}$ is an example of a principal ideal domain having infinitely many prime ideals.

4. The absolute norm

In this section, we let K be a number field of degree $n = [K : \mathbb{Q}]$, and $\mathcal{O}_K$ its ring of integers. For any $x \in \mathcal{O}_K$, recall that the norm $\mathrm{N}_{K/\mathbb{Q}}(x)$ is an element of $\mathbb{Z}$ by Proposition 5.1.1.

PROPOSITION 6.4.1. *Let $x \in \mathcal{O}_K \smallsetminus \{0\}$. Then*

$$|\,\mathrm{N}_{K/\mathbb{Q}}(x)| = \mathrm{card}(\mathcal{O}_K/x\mathcal{O}_K).$$

PROOF. Let us write $B = \mathcal{O}_K$ and $I = x\mathcal{O}_K$. Recall from Corollary 5.1.6 that the $\mathbb{Z}$-module B is free of rank $n = [K : \mathbb{Q}]$. Its submodule I is also free of rank n, because multiplication by x induces an isomorphism of $\mathbb{Z}$-modules $B \to I$. Therefore by Theorem 1.3.2 and its complement Proposition 1.3.13, we may find a $\mathbb{Z}$-basis $(e_1, \ldots, e_n)$ of B and integers $c_1, \ldots, c_n \in \mathbb{N} \smallsetminus \{0\}$ such that $(c_1e_1, \ldots, c_ne_n)$ is a $\mathbb{Z}$-basis of I. Then the $\mathbb{Z}$-module B/I is isomorphic to $(\mathbb{Z}/c_1\mathbb{Z}) \times \cdots \times (\mathbb{Z}/c_n\mathbb{Z})$, so that

$$\mathrm{card}(\mathcal{O}_K/x\mathcal{O}_K) = \mathrm{card}(B/I) = c_1 \cdots c_n. \tag{6.4.a}$$

We have three basis of the $\mathbb{Q}$-vector space K, given by $(e_1, \ldots, e_n)$, $(xe_1, \ldots, xe_n)$, and $(c_1e_1, \ldots, c_ne_n)$. We may thus define isomorphisms of $\mathbb{Q}$-vector spaces $u, v \colon K \to K$ by

$$u(e_i) = c_ie_i \quad \text{and} \quad v(c_ie_i) = xe_i \quad \text{for all } i = 1, \ldots, n.$$

Then the composite $v \circ u$ is multiplication by x, hence $\det(v \circ u) = \mathrm{N}_{K/\mathbb{Q}}(x)$. Since the matrix of u in the basis $(e_1, \ldots, e_n)$ is diagonal with values $(c_1, \ldots, c_n)$, we have $\det u = c_1 \cdots c_n$. To conclude the proof, in view of (6.4.a) and the fact that $\det(v \circ u) = (\det v)(\det u)$, it will suffice to show that $\det v \in \{-1, 1\}$.

Observe that $(c_1e_1, \ldots, c_ne_n)$ and $(xe_1, \ldots, xe_n)$ are both $\mathbb{Z}$-basis of I. Therefore the map $v \colon K \to K$ restricts to an isomorphism of $\mathbb{Z}$-modules $w \colon I \to I$. Its determinant $\det w$ is an invertible element of $\mathbb{Z}$, hence $\det w \in \{-1, 1\}$. Now any $\mathbb{Z}$-basis $\mathcal{B}$ of I maps to a $\mathbb{Q}$-basis $\mathcal{C}$ of K under the inclusion $I \subset K$, and the coefficients of the matrix of v in the basis $\mathcal{C}$ are the images of the coefficients of the matrix of w in the basis $\mathcal{B}$ under the inclusion $\mathbb{Z} \subset \mathbb{Q}$. We deduce that $\det v$ is the image of $\det w$ under the inclusion $\mathbb{Z} \subset \mathbb{Q}$, hence $\det v \in \{-1, 1\}$, as required. □

COROLLARY 6.4.2. *If I is a nonzero ideal of $\mathcal{O}_K$, then the group $\mathcal{O}_K/I$ is finite.*

PROOF. Indeed, let $x \in I \smallsetminus \{0\}$. Then $x\mathcal{O}_K \subset I$, and thus the group $\mathcal{O}_K/I$ is a quotient of $\mathcal{O}_K/x\mathcal{O}_K$. The latter is finite by Proposition 6.4.1, hence so is the former. □

DEFINITION 6.4.3. Let K be a number field, and I a nonzero ideal of $\mathcal{O}_K$. The *absolute norm* (or simply the *norm*) of I, denoted $\mathrm{N}(I)$, is defined as the integer $\mathrm{card}(\mathcal{O}_K/I)$ (which is finite by Corollary 6.4.2).

The following easy observation will be important:

LEMMA 6.4.4. *For any nonzero ideal I of $\mathcal{O}_K$, we have*

$$\mathrm{N}(I) \cdot \mathcal{O}_K \subset I.$$

PROOF. Let $m = \mathrm{N}(I)$. Then the finite group $\mathcal{O}_K/I$ has order m, and in particular $m(\mathcal{O}_K/I) = 0$, which means that $m\mathcal{O}_K \subset I$. □

PROPOSITION 6.4.5. *Let I, J be nonzero ideals of $\mathcal{O}_K$. Then*

$$\mathrm{N}(IJ) = \mathrm{N}(I)\,\mathrm{N}(J).$$

PROOF. In view of Theorem 6.3.5, we may assume that J is a maximal ideal of $\mathcal{O}_K$. The natural morphism $\mathcal{O}_K/IJ \to \mathcal{O}_K/I$ is surjective, and its kernel is I/IJ. Therefore every element of $\mathcal{O}_K/I$ admits exactly $\mathrm{card}(I/IJ)$ preimages in $\mathcal{O}_K/IJ$, so that

$$\mathrm{card}(\mathcal{O}_K/IJ) = \mathrm{card}(\mathcal{O}_K/I) \cdot \mathrm{card}(I/IJ). \tag{6.4.b}$$

By Proposition 6.3.10 the $(\mathcal{O}_K/J)$-vector space I/IJ has dimension one, hence $\mathrm{card}(I/IJ) = \mathrm{card}(\mathcal{O}_K/J)$. The proposition then follows from (6.4.b). □

CHAPTER 7

Localisation

In this section, we introduce a general tool — the localisation — which is very useful in commutative algebra, and review several notions discussed through the lens of this new tool. This will allow us to understand Dedekind domains as those domains which are "locally" principal ideal domains.

We will not discuss the most general situation of modules over rings, but restrict ourselves to the special case of submodules of the function field of a domain. This will permit to follow a somewhat more concrete approach to the process of localisation.

1. Localising inside the fraction field

In this section A is a domain with fraction field K.

DEFINITION 7.1.1. A subset $S \subset A$ is called *multiplicatively closed* if $1 \in S$, and for all $x, y \in S$ we have $xy \in S$.

For the rest of the section A will be a domain, and S a multiplicatively closed subset of A which does not contain zero.

DEFINITION 7.1.2. We define a subring

$$S^{-1}A = \left\{ \frac{a}{s}, \text{where } a \in A, s \in S \right\} \subset K.$$

More generally, when $M \subset K$ is an A-submodule, we define an $S^{-1}A$-module

$$S^{-1}M = M \cdot (S^{-1}A) = \left\{ \frac{m}{s}, \text{where } m \in A, s \in S \right\} \subset K.$$

Observe that $S^{-1}A$ is a domain which contains A, and that its fraction field is K. Note that $S^{-1}A = A$ when $S \subset A^\times$, and that $S^{-1}A = K$ when $S = A \smallsetminus \{0\}$.

LEMMA 7.1.3. *For every ideal J of $S^{-1}A$, we have $J = S^{-1}(J \cap A)$.*

PROOF. Since J is an ideal of $S^{-1}A$, we have

$$S^{-1}(J \cap A) = (J \cap A) \cdot (S^{-1}A) \subset J \cdot (S^{-1}A) = J.$$

Conversely, let $j \in J$. Since $j \in S^{-1}A$, we have $sj \in A$ for some $s \in S$. Thus $sj \in J \cap A$, so that $j \in S^{-1}(J \cap A)$. Therefore $J \subset S^{-1}(J \cap A)$. □

LEMMA 7.1.4. *Let I be an ideal of A. Then*

$$S^{-1}I = S^{-1}A \iff S \cap I \neq \varnothing.$$

PROOF. If $s \in S \cap I$, then $1 = s/s \in S^{-1}I$, and so $S^{-1}I = S^{-1}A$. Conversely assume that $S^{-1}I = S^{-1}A$. Then $1 = i/s$ for some $i \in I$ and $s \in S$. Thus $s = i \in S \cap I$. □

Lemma 7.1.5. *Let $\mathfrak{p}$ be a prime ideal of A such that $S \cap \mathfrak{p} = \varnothing$. Then for any ideal I of A, we have*

$$I \subset \mathfrak{p} \iff S^{-1}I \subset S^{-1}\mathfrak{p}.$$

Proof. $\Rightarrow$: This is clear.

$\Leftarrow$: Let $i \in I$. Then by assumption, we may find $s \in S$ such that $si \in \mathfrak{p}$. Since $\mathfrak{p}$ is a prime ideal and $s \notin \mathfrak{p}$, it follows that $i \in \mathfrak{p}$, as required. □

Proposition 7.1.6. *The following hold:*

(i) For every prime ideal $\mathfrak{p}$ of A such that $S \cap \mathfrak{p} = \varnothing$, the ideal $S^{-1}\mathfrak{p}$ of $S^{-1}A$ is prime, and satisfies $(S^{-1}\mathfrak{p}) \cap A = \mathfrak{p}$.

(ii) Each prime ideal of $S^{-1}A$ is of the form $S^{-1}\mathfrak{p}$, for a unique prime ideal $\mathfrak{p}$ of A. This prime ideal satisfies $S \cap \mathfrak{p} = \varnothing$.

Proof. (i): We have $S^{-1}\mathfrak{p} \neq S^{-1}A$ by Lemma 7.1.4. Let $x, y \in S^{-1}A$ be such that $xy \in S^{-1}\mathfrak{p}$. We may then find $s_1, s_2, t \in S$ such that $s_1 x, s_2 y \in A$, and $txy \in \mathfrak{p}$. Set $s = s_1 s_2 t$. Then $(sx)(sy) \in \mathfrak{p}$, hence, since $\mathfrak{p}$ is a prime ideal of A, we must have $sx \in \mathfrak{p}$ or $sy \in \mathfrak{p}$. This implies that $x \in S^{-1}\mathfrak{p}$ or $y \in S^{-1}\mathfrak{p}$. We have proved that $S^{-1}\mathfrak{p}$ is a prime ideal of $S^{-1}A$.

Let $I = (S^{-1}\mathfrak{p}) \cap A$. Then clearly $\mathfrak{p} \subset I$. Conversely

$$S^{-1}I = (S^{-1}A) \cdot I \subset (S^{-1}A) \cdot (S^{-1}\mathfrak{p}) = S^{-1}\mathfrak{p},$$

hence $I \subset \mathfrak{p}$ by Lemma 7.1.5.

(ii): Let $\mathfrak{q}$ be a prime ideal of $S^{-1}A$. Then $\mathfrak{p} = \mathfrak{q} \cap A$ is a prime ideal of A by Lemma 1.1.2. By Lemma 7.1.3, we have $\mathfrak{q} = S^{-1}\mathfrak{p}$.

Now let $\mathfrak{p}'$ be a prime ideal of A such that $S^{-1}\mathfrak{p}' = \mathfrak{q}$. As $\mathfrak{q} \neq S^{-1}A$ (because $\mathfrak{q}$ is assumed to be prime), we have $S \cap \mathfrak{p}' = \varnothing$ by Lemma 7.1.4. In particular, we have $S \cap \mathfrak{p} = \varnothing$. In addition, it follows from (i), applied to the prime ideal $\mathfrak{p}'$, that

$$\mathfrak{p} = \mathfrak{q} \cap A = (S^{-1}\mathfrak{p}') \cap A = \mathfrak{p}',$$

which completes the proof of (ii). □

Corollary 7.1.7. *The set of prime ideals $\mathfrak{q}$ of $S^{-1}A$ is in bijection with the set of prime ideals $\mathfrak{p}$ of A such that $S \cap \mathfrak{p} = \varnothing$. The mutually inverse maps are given by*

$$\mathfrak{q} \mapsto \mathfrak{q} \cap A \quad \text{and} \quad \mathfrak{p} \mapsto S^{-1}\mathfrak{p},$$

and are compatible with the orders given by the inclusion of ideals.

Lemma 7.1.8. *Let $I \subset A$ be an ideal and $\pi\colon A \to A/I$ the quotient map. Assume that $\pi(S) \subset (A/I)^\times$. Then the natural morphism of A-algebras*

$$A/I \to (S^{-1}A)/(S^{-1}I)$$

is an isomorphism.

Proof. Let $a \in A \cap S^{-1}I$. Then there exists $s \in S$ such that $sa \in I$. The assumption implies that we can find $t \in A$ and $i \in I$ such that $st = 1 + i$. We have

$$a = a(st - i) = (sa)t - ia \in I.$$

Thus $A \cap S^{-1}I \subset I$. As $I \subset A \cap S^{-1}I$, we have proved that $A \cap S^{-1}I = I$, which means that the morphism is injective.

Now consider an element $a/s \in S^{-1}A$. Then as above we find $t \in A$ and $i \in I$ such that $st = 1 + i$, and

$$ta - \frac{a}{s} = \frac{sta - a}{s} = \frac{ia}{s} \in S^{-1}I,$$

which proves that $ta \in A/I$ maps to a/s in $(S^{-1}A)/(S^{-1}I)$. This shows that the morphism is surjective. □

Proposition 7.1.9. *Let L/K be a field extension, and let B be the integral closure of A in L. Then $S^{-1}B$ is the integral closure of $S^{-1}A$ in L.*

Proof. Observe that the fraction field of B is naturally contained in L, hence so is its subring $S^{-1}B$. Every element of $S^{-1}B$ is of the form b/s with $b \in B$ and $s \in S$. Then b satisfies an equation of the form

$$b^n + a_{n-1}b^{n-1} + \cdots + a_0 = 0, \quad \text{with } a_0, \ldots, a_{n-1} \in A.$$

Dividing by s^n yields

$$\Big(\frac{b}{s}\Big)^n + \frac{a_{n-1}}{s}\Big(\frac{b}{s}\Big)^{n-1} + \cdots + \frac{a_0}{s^n} = 0,$$

which shows that the element b/s is integral over $S^{-1}A$.

Conversely, let $x \in L$ be integral over $S^{-1}A$. Then we may find $a_0, \ldots, a_{n-1} \in A$, $s_0, \ldots, s_{n-1} \in S$ such that

$$x^n + \frac{a_{n-1}}{s_{n-1}}x^{n-1} + \cdots + \frac{a_0}{s_0} = 0.$$

Set $s = s_0 \ldots s_{n-1} \in S$. Multiplying the above equation by s^n, we obtain

$$(sx)^n + \frac{sa_{n-1}}{s_{n-1}}(sx)^{n-1} + \cdots + \frac{s^n a_0}{s_0} = 0. \tag{7.1.a}$$

For each $i \in \{0, \ldots, n-1\}$, setting $t_i = s/s_i \in A \subset S^{-1}A$, we have

$$\frac{s^{n-i}a_i}{s_i} = a_i s^{n-1-i} t_i \in A \subset S^{-1}A.$$

Therefore the equation (7.1.a) has coefficients in $A \subset S^{-1}A$, which proves that sx is integral over A, hence $sx \in B$, and thus $x \in S^{-1}B$. □

Corollary 7.1.10. *If the domain A is integrally closed, then so is $S^{-1}A$.*

Lemma 7.1.11. *If the domain A is noetherian, then so is $S^{-1}A$.*

Proof. Consider a family of ideals J_n of $S^{-1}A$, for $n \in \mathbb{N}$, such that $J_n \subset J_{n+1}$ for all $n \in \mathbb{N}$. Then, as A is noetherian, we can find an integer s such that $J_n \cap A = J_s \cap A$ for all $n \geq s$. Thus $S^{-1}(J_n \cap A) = S^{-1}(J_s \cap A)$ for all $n \geq s$. By Lemma 7.1.3, this implies that $J_n = J_s$ for $n \geq s$, which proves that the ring $S^{-1}A$ is noetherian. □

Proposition 7.1.12. *If A is a Dedekind domain, then so is $S^{-1}A$.*

Proof. Then the domain $S^{-1}A$ is integrally closed by Proposition 7.1.9, and it is noetherian by Lemma 7.1.11. The fact that every nonzero prime ideal of A is maximal implies, by Corollary 7.1.7, that every nonzero prime ideal of $S^{-1}A$ is maximal. □

Definition 7.1.13. Let $\mathfrak{p}$ a prime ideal of A. Then the set $S = A \setminus \mathfrak{p}$ is multiplicatively closed and does not contain zero. The ring $S^{-1}A$ is called the *localisation of A at $\mathfrak{p}$*, and is denoted by $A_\mathfrak{p}$. If M is an A-submodule of K, we write $M_\mathfrak{p}$ instead of $S^{-1}M$.

A ring is called *local* if it possesses exactly one maximal ideal.

Lemma 7.1.14. *Let $\mathfrak{p}$ a prime ideal of A. Then the ring $A_\mathfrak{p}$ is local with maximal ideal $S^{-1}\mathfrak{p} = \mathfrak{p}A_\mathfrak{p}$.*

Proof. Let $S = A \setminus \mathfrak{p}$. Recall from Corollary 7.1.7 that the prime ideals of $S^{-1}A = A_\mathfrak{p}$ are of the form $S^{-1}\mathfrak{p}'$, where $S \cap \mathfrak{p}' = \varnothing$. As $S = A \setminus \mathfrak{p}$, this condition means that $\mathfrak{p}' \subset \mathfrak{p}$, so that $S^{-1}\mathfrak{p}' \subset S^{-1}\mathfrak{p}$. Therefore the prime ideal $S^{-1}\mathfrak{p}$ in $A_\mathfrak{p}$ contains every prime ideal of $A_\mathfrak{p}$; it is thus the unique maximal ideal $S^{-1}\mathfrak{p}$, and the ring $A_\mathfrak{p}$ is local. □

Proposition 7.1.15. *Let M be an A-submodule of K. Then*

$$M = \bigcap_\mathfrak{p} M_\mathfrak{p} \subset K,$$

where $\mathfrak{p}$ runs over the maximal ideals of A.

Proof. Let $M' = \bigcap_\mathfrak{p} M_\mathfrak{p}$. Certainly $M \subset M'$. Conversely, let $x \in M'$. The set

$$I = \{y \in A | xy \in M\}.$$

is an ideal of A. Assume that $I \neq A$. Then the ideal I is contained in some maximal ideal $\mathfrak{m}$ of A. But $x \in M_\mathfrak{m}$ by assumption, hence there exists $b \notin \mathfrak{m}$ such that $bx \in M$. This implies that $b \in I$, hence $b \in \mathfrak{m}$, a contradiction. Therefore we must have $I = A$. In particular $1 \in I$, so that $x \in M$, and thus $M = M'$. □

Corollary 7.1.16. *Let M, N be A-submodules of K. Then $M = N$ if and only if $M_\mathfrak{p} = N_\mathfrak{p}$ for all maximal ideals $\mathfrak{p}$ of A.*

2. Discrete valuation rings

Definition 7.2.1. Let A be a domain with fraction field K. The ring A is called a *discrete valuation ring* if there exists a surjective function $v\colon K \to \mathbb{Z} \cup \{\infty\}$ such that:

(I) $v(x) = \infty \iff x = 0$,
(II) $v(xy) = v(x) + v(y)$ for all $x, y \in K \setminus \{0\}$,
(III) $v(x + y) \geq \min(v(x), v(y))$ for all $x, y \in K \setminus \{0\}$,
(IV) $A = \{x \in K | v(a) \geq 0\}$.

Lemma 7.2.2. *Let A be a discrete valuation ring with fraction field K. Let $a \in K$. Then*

(i) If $a \neq 0$, then $v(a^{-1}) = -v(a)$.
(ii) We have $a \in A^\times$ if and only if $v(a) = 0$.

Proof. (i): We have $v(1) = v(1 \cdot 1) = v(1) + v(1)$ (by the axiom (II)), hence $v(1) = 0$. Thus, by the axiom (II) we deduce that $v(a) + v(a^{-1}) = v(1) = 0$.

(i): Since $v(0) = \infty$, we may assume that $a \neq 0$. Observe that $a \in A^\times$ if and only if $a, a^{-1} \in A$. By the axiom (IV) this holds if and only if $v(a) \geq 0$ and $v(a^{-1}) \geq 0$. Since $v(a) = -v(a^{-1})$ by (i), this is equivalent to the conditions $v(a) = v(a^{-1}) = 0$. □

Remark 7.2.3. A discrete valuation ring is never a field: indeed Lemma 7.2.2 prevents the map v from being surjective when A is a field. In certain alternative definitions of discrete valuations rings present in the literature, the surjectivity assumption for v is sometimes dropped, and thus discrete valuation rings are allowed to be fields.

DEFINITION 7.2.4. Let A be a discrete valuation ring. An element $\pi \in A$ such that $v(\pi) = 1$ is called a *uniformising parameter*. Observe that such an element always exists: indeed as $v\colon K \to \mathbb{Z} \cup \{\infty\}$ is surjective we may find $\pi \in K$ such that $v(\pi) = 1$, and the axiom (IV) ensures that $\pi \in A$.

As in the case of fields, it is easy to list the ideals of a discrete valuation ring:

PROPOSITION 7.2.5. *Let A be a discrete valuation ring, and π a uniformising parameter. Then every nonzero ideal of A is of the form $\pi^n A$ for some $n \in \mathbb{N}$.*

PROOF. Let I be a nonzero ideal of A. Let $n = \min(v(I)) \in \mathbb{N}$. Then for any $x \in I \smallsetminus \{0\}$, we have by the axiom (II) and Lemma 7.2.2 (i)

$$v(x\pi^{-n}) = v(x) - v(\pi^n) = v(x) - n. \tag{7.2.a}$$

Since $v(x) \geq n$ (by the choice of n), we deduce from (7.2.a) that $v(x\pi^{-n}) \geq 0$, so that $x\pi^{-n} \in A$ by the axiom (IV), and thus $x \in \pi^n A$. We have proved that $I \subset \pi^n A$.

Let now $x \in I$ be such that $v(x) = n$. Then (7.2.a) implies that $v(x\pi^{-n}) = 0$, hence $x\pi^{-n} \in A^\times$ by Lemma 7.2.2. In particular $\pi^n \in xA \subset I$. We have proved that $I = \pi^n A$. □

COROLLARY 7.2.6. *A discrete valuation ring is a principal ideal domain.*

COROLLARY 7.2.7. *A discrete valuation ring is local. Its maximal ideal is generated by any uniformising parameter.*

PROOF. Let A be a discrete valuation ring, and $\pi \in A$ a uniformising parameter. Certainly the ideal πA is the unique maximal element of the set $\{\pi^n A | n \in \mathbb{N} \smallsetminus \{0\}\}$, and the corollary follows from Proposition 7.2.5. □

PROPOSITION 7.2.8. *Let A be a ring. The following are equivalent:*

(i) A is a field or a discrete valuation ring,
(ii) A is a local principal ideal domain,
(iii) A is a local Dedekind domain.

PROOF. (i) ⇒ (ii) : A field is certainly a local principal ideal domain. Assume that A is a discrete valuation ring. The ring A is local by Corollary 7.2.7, and a principal ideal domain by Corollary 7.2.6.

(ii) ⇒ (iii) : This has been proved in Proposition 6.1.4.

(iii) ⇒ (i) : Let $\mathfrak{m}$ be the maximal ideal of the ring A, and K its fraction field. We assume that A is not a field, so that $\mathfrak{m}$ is nonzero. Observe that $\mathfrak{m}$ is then the unique nonzero prime ideal of A, and therefore by Theorem 6.3.5 every nonzero fractional ideal of A is of the form $\mathfrak{m}^k$ for a unique element $k \in \mathbb{Z}$. For $x \in K \smallsetminus \{0\}$, we define an integer $v(x) \in \mathbb{Z}$ by the condition $xA = \mathfrak{m}^{v(x)}$, and we set $v(0) = \infty$. Then clearly we have $v(xy) = v(x) + v(y)$ for all $x, y \in K \smallsetminus \{0\}$. Moreover for any nonzero $x \in K$ we have

$$v(x) \geq 0 \iff (xA = \mathfrak{m}^k \text{ for some } k \in \mathbb{N}) \iff xA \subset A \iff x \in A.$$

For $x, y \in K \smallsetminus \{0\}$, we have

$$\mathfrak{m}^{v(x+y)} = (x+y)A \subset xA + yA = \mathfrak{m}^{v(x)} + \mathfrak{m}^{v(y)} \subset \mathfrak{m}^{\min(v(x),v(y))},$$

and so $v(x+y) \geq \min(v(x), v(y))$.

As $\mathfrak{m} \neq 0$, we have $\mathfrak{m}^2 \neq \mathfrak{m}$ by Corollary 6.3.3. So we may pick an element $\pi \in \mathfrak{m} \smallsetminus \mathfrak{m}^2$. As $\pi A \subset \mathfrak{m}$ but $\pi A \not\subset \mathfrak{m}^2$, we must have $v(\pi) = 1$. The validity of the axiom (II) implies

that $v\colon K^\times \to \mathbb{Z}$ is a group morphism, which must thus be surjective. Therefore the ring A is a discrete valuation ring. □

Corollary 7.2.9. *In a discrete valuation ring, there are exactly two prime ideals.*

Proof. Let A be a discrete valuation ring. As A is a Dedekind domain by Proposition 7.2.8, every nonzero prime ideal of A is maximal. As A is local by Corollary 7.2.7, it follows that the number of prime ideals in A is at most two. If it is one, then the zero ideal is maximal, which means that A is a field, a case which is excluded (see Remark 7.2.3). □

Proposition 7.2.10. *Let A be a noetherian domain. Then A is a Dedekind domain if and only if the ring $A_\mathfrak{p}$ is a field or a discrete valuation ring for each maximal ideal $\mathfrak{p}$ of A.*

Proof. Assume that A is a Dedekind domain. For each maximal ideal $\mathfrak{p}$ of A, the ring $A_\mathfrak{p}$ is a local Dedekind domain by Lemma 7.1.14 and Proposition 7.1.12, and thus a field or a discrete valuation ring by Proposition 7.2.8.

Conversely, assume that $A_\mathfrak{p}$ is a field or discrete valuation ring for each maximal ideal $\mathfrak{p}$ of A. Let $\mathfrak{q}$ be a nonzero prime ideal of A. Pick a maximal ideal $\mathfrak{p}$ of A such that $\mathfrak{q} \subset \mathfrak{p}$ (Lemma 1.2.7). Then $\mathfrak{q}A_\mathfrak{p}$ is a nonzero prime ideal of $A_\mathfrak{p}$ by Proposition 7.1.6. Since $A_\mathfrak{p}$ is a Dedekind domain (Proposition 7.2.8), the ideal $\mathfrak{q}A_\mathfrak{p}$ is maximal in $A_\mathfrak{p}$, hence coincides with $\mathfrak{p}A_\mathfrak{p}$ by Lemma 7.1.14. As $(\mathfrak{q}A_\mathfrak{p}) \cap A = \mathfrak{q}$ and $(\mathfrak{p}A_\mathfrak{p}) \cap A = \mathfrak{p}$ (see Proposition 7.1.6), we deduce that $\mathfrak{p} = \mathfrak{q}$, and thus the ideal $\mathfrak{q}$ is maximal in A

Let now B be the integral closure of A in K. Then by Proposition 7.1.9 the ring $B_\mathfrak{p}$ is the integral closure of $A_\mathfrak{p}$ in K for each maximal ideal $\mathfrak{p}$ of A, and as $A_\mathfrak{p}$ is integrally closed (being a Dedekind domain by Proposition 7.2.8) we have $A_\mathfrak{p} = B_\mathfrak{p}$ in K. Therefore $A = B$ by Corollary 7.1.16. This proves that the domain A is integrally closed, and A is thus a Dedekind domain (recall that the ring A was assumed to be noetherian). □

CHAPTER 8

Lattices in real vector spaces

1. Discrete subgroups of $\mathbb{R}^n$

DEFINITION 8.1.1. A subset S of $\mathbb{R}^n$ is called *discrete* if its induced topology is discrete. This means that for every $s \in S$, there exists an open subset $U \subset \mathbb{R}^n$ such that $\{s\} = S \cap U$.

LEMMA 8.1.2. *Let S be a subset of $\mathbb{R}^n$. Then the following conditions are equivalent:*

(i) The subset $S \subset \mathbb{R}^n$ is closed and discrete.
(ii) For every bounded subset $B \subset \mathbb{R}^n$ the intersection $B \cap S$ is finite.

PROOF. (i) $\Rightarrow$ (ii): Enlarging B, we may assume that B is closed (observe that B is contained in some closed ball centered at the origin). Then B is compact, and so is $S \cap B$ (because S is closed). For each $s \in S$, pick an open subset $U_s \subset \mathbb{R}^n$ such that $S \cap U_s = \{s\}$. Then $S \cap B$ is contained in the union of the open subsets U_s for $s \in S$, hence by compactness we may find a finite subset $F \subset S$ such that $S \cap B$ is contained in the union of the subsets U_s for $s \in F$. Thus

$$S \cap B \subset \Big(\bigcup_{s \in F} U_s \Big) \cap S \cap B \subset \bigcup_{s \in F} (U_s \cap S) = \bigcup_{s \in F} \{s\} = F,$$

hence $S \cap B$ is finite.

(ii) $\Rightarrow$ (i): Let $s \in S$. Then s is contained in a bounded open subset V of $\mathbb{R}^n$ (e.g. some open ball centered in s). As $V \cap S$ is finite, we may write $(V \cap S) \smallsetminus \{s\} = F$ with F finite, and in particular closed in $\mathbb{R}^n$. The set $U = V \smallsetminus F$ is then open in $\mathbb{R}^n$, and satisfies $U \cap S = \{s\}$. We have proved that S is discrete.

For each $x \in \mathbb{R}^n$, pick a bounded open neighborhood U_x of x (e.g. some open ball centered in x). Then for each $x \in \mathbb{R}^n$, the set $U_x \cap S$ is finite by assumption, hence closed in $\mathbb{R}^n$. Thus $V_x = U_x \smallsetminus (U_x \cap S)$ is an open subset of $\mathbb{R}^n$. Therefore the subset

$$\mathbb{R}^n \smallsetminus S = \bigcup_{x \in \mathbb{R}^n} V_x$$

is open in $\mathbb{R}^n$, and so S is closed in $\mathbb{R}^n$. □

LEMMA 8.1.3. *Every discrete subgroup of $\mathbb{R}^n$ is closed.*

PROOF. Let H be a discrete subgroup of $\mathbb{R}^n$, and let g be an element of the closure of H in $\mathbb{R}^n$. Pick an open subset $U \subset \mathbb{R}^n$ such that $U \cap H = \{0\}$. Replacing U with $U \cap (-U)$, we may assume that $U = -U$. Then $g + U$ is an open neighborhood of g, and as g is in the closure of H, we must have

$$(g + U) \cap H \neq \varnothing.$$

Thus we may find an element $h \in H$ which can be written as $h = g + u$ with $u \in U$. Then $g \in h + (-U) = h + U$. Let $U^\circ = U \smallsetminus \{0\}$; this is an open subset of $\mathbb{R}^n$. Then $U^\circ \cap H = \varnothing$, and thus $(h+U^\circ) \cap H = \varnothing$. Therefore $h+U^\circ$ is an open subset of $\mathbb{R}^n$ which does not meet H, hence the subset $h + U^\circ$ does not meet the closure of H. In particular $g \notin h + U^\circ$. As $g \in h + U$, we must have $g = h$, and in particular $g \in H$. □

THEOREM 8.1.4. *Let H be a subgroup of $\mathbb{R}^n$. The following conditions are equivalent:*

(i) the subset $H \subset \mathbb{R}^n$ is discrete,
(ii) the subgroup $H \subset \mathbb{R}^n$ is generated by a set of $\mathbb{R}$-linearly independent vectors in $\mathbb{R}^n$.

PROOF. (ii) ⇒ (i) : Let $x_1, \dots, x_m$ be $\mathbb{R}$-linearly vectors in $\mathbb{R}^n$, and H the subgroup of $\mathbb{R}^n$ generated by these elements. Note that $m \leq n$. While proving that H is discrete, we may enlarge H (because a subset of a discrete subset is discrete). Therefore after completing the family $(x_1, \dots, x_m)$ into an $\mathbb{R}$-basis of $\mathbb{R}^n$, we may assume that $m = n$. Consider the $\mathbb{R}$-linear automorphism φ of $\mathbb{R}^n$ mapping the basis $(x_1, \dots, x_n)$ to the canonical basis $(c_1, \dots, c_n)$ of $\mathbb{R}^n$. For any $h \in H$, consider the open ball B_h centered at $\varphi(h)$ of radius 1 for the euclidean metric. Consider the open subset $U_h = \varphi^{-1}B_h$ of $\mathbb{R}^n$.

We claim that $U_h \cap H = \{h\}$, which will conclude the proof that the subset $H \subset \mathbb{R}^n$ is discrete. Indeed, let $x \in U_h$. Then

$$\varphi(x) = \varphi(h) + \sum_{i=1}^{n} \lambda_i c_i,$$

where $\lambda_1, \dots, \lambda_n \in \mathbb{R}$ are such that $\lambda_1^2 + \cdots + \lambda_n^2 < 1$, and in particular $\lambda_1, \dots, \lambda_n \notin \mathbb{Z}$. Since φ is injective and $c_i = \varphi(x_i)$ for $i \in \{1, \dots, n\}$, we deduce that

$$x - h = \sum_{i=1}^{n} \lambda_i x_i$$

If $x \neq h$, then there exists $j \in \{1, \dots, n\}$ such that $\lambda_j \neq 0$, and thus $\lambda_j \notin \mathbb{Z}$. Since every element of H is a $\mathbb{Z}$-linear combination of $(x_1, \dots, x_n)$, and $(x_1, \dots, x_n)$ is $\mathbb{R}$-linearly independent, this implies that $x - h \notin H$, or equivalently $x \notin H$. This proves the claim.

(i) ⇒ (ii) : Assume that the subset $H \subset \mathbb{R}^n$ is discrete. Choose a family of $\mathbb{R}$-linearly independent vectors $e_1, \dots, e_r \in H$, in such a way that r is maximum (note that in any case we have $r \leq n$). Consider the parallelotope

$$P = \Big\{ \sum_{i=1}^{r} \alpha_i e_i | 0 \leq \alpha_i \leq 1 \Big\} \subset \mathbb{R}^n.$$

Then P is bounded, hence $P \cap H$ is finite by Lemma 8.1.2 and Lemma 8.1.3. Let $x \in H$. By maximality of r, we may write

$$x = \sum_{i=1}^{r} \lambda_i e_i,$$

with $\lambda_1, \dots, \lambda_r \in \mathbb{R}$. For $j \in \mathbb{Z}$, set

$$x_j = jx - \sum_{i=1}^{r} \lfloor j\lambda_i \rfloor e_i \in H.$$

Here, for $\lambda \in \mathbb{R}$, we denote by $\lfloor \lambda \rfloor \in \mathbb{Z}$ the integer such that $\lfloor \lambda \rfloor \leq \lambda < \lfloor \lambda \rfloor + 1$. Then

$$x_j = \sum_{i=1}^{r} (j\lambda_i - \lfloor j\lambda_i \rfloor) e_i \in P \cap H. \tag{8.1.a}$$

Note that $e_i \in P \cap H$ for each $i \in \{1, \dots, r\}$. As

$$x = x_1 + \sum_{i=1}^{r} \lfloor \lambda_i \rfloor e_i,$$

it follows that the $\mathbb{Z}$-module H is generated by $P \cap H$, hence is finitely generated.

Now as $P \cap H$ is finite and $\mathbb{Z}$ infinite, we may find two distinct integers $j, k \in \mathbb{Z}$ such that $x_j = x_k$. Thus by (8.1.a), we obtain

$$j\lambda_i - \lfloor j\lambda_i \rfloor = k\lambda_i - \lfloor k\lambda_i \rfloor \quad \text{for all } i = 1, \dots, r,$$

hence, for all $i = 1, \dots, r$

$$\lambda_i = \frac{\lfloor j\lambda_i \rfloor - \lfloor k\lambda_i \rfloor}{j - k} \in \mathbb{Q}.$$

Therefore every element of H is a $\mathbb{Q}$-linear combination of $e_1, \dots, e_r$. Thus for every element $h \in H$, we may find a nonzero integer $d_h \in H$ such that $d_h \cdot h \in Z$, where $Z \subset \mathbb{R}^n$ is the $\mathbb{Z}$-submodule generated by the elements $e_1, \dots, e_r$. If $F \subset H$ is a finite subset which generates the $\mathbb{Z}$-module H (e.g. $F = P \cap H$), we may thus find a nonzero integer $d \in \mathbb{Z}$ such that $dh \in Z$ for every $h \in F$. Then $dH \subset Z$. Note that the family $(e_1, \dots, e_r)$ is a $\mathbb{Z}$-basis of Z, hence Z is a free $\mathbb{Z}$-module of rank r, so that by Theorem 1.3.2 the $\mathbb{Z}$-module $dH \subset Z$ is free of rank s, where $s \leq r$. The multiplication-by-d map induces an isomorphism of $\mathbb{Z}$-modules $H \xrightarrow{\sim} dH$, hence the $\mathbb{Z}$-module H is also free of rank s. Applying Theorem 1.3.2 and Proposition 1.3.13 to the inclusion $Z \subset H$, we deduce that $r \leq s$. We conclude that $r = s$, and therefore the $\mathbb{Z}$-module H is free of rank r.

Let $(f_1, \dots, f_r)$ be a $\mathbb{Z}$-basis of H. The inclusions $dH \subset Z \subset H$ show that Z and H generate the same $\mathbb{R}$-subspace V of $\mathbb{R}^n$. In other words the families $(e_1, \dots, e_r)$ and $(f_1, \dots, f_r)$ generate the $\mathbb{R}$-vector space V. Since they have the same number of elements, and the first family is $\mathbb{R}$-linearly independent, so is the second family. □

COROLLARY 8.1.5. *Every discrete subgroup of $\mathbb{R}^n$ is a free $\mathbb{Z}$-module of rank m, with $m \leq n$.*

PROOF. Let H be a discrete subgroup of $\mathbb{R}^n$. By Theorem 8.1.4 the group H is generated by a system of $\mathbb{R}$-linearly independent vectors of $\mathbb{R}^n$. Such system is in particular $\mathbb{Z}$-linearly independent, and is therefore a $\mathbb{Z}$-basis of H. The number of elements in this system is at most n (as is the case for any $\mathbb{R}$-linearly independent system in $\mathbb{R}^n$). □

EXAMPLE 8.1.6. The subgroup of $\mathbb{R}$ generated by 1 and $\sqrt{2}$ is free of rank two as a $\mathbb{Z}$-module. It follows from Corollary 8.1.5 that this subgroup is not discrete.

2. Minkowski's Theorem

DEFINITION 8.2.1. A subgroup of $\mathbb{R}^n$ is called a *lattice* if it is generated as a $\mathbb{Z}$-module by an $\mathbb{R}$-basis of $\mathbb{R}^n$.

Thus by Theorem 8.1.4 a lattice is always a discrete subgroup of $\mathbb{R}^n$. As a $\mathbb{Z}$-module a lattice is free of rank n.

For each $\mathbb{R}$-basis $e = (e_1, \dots, e_n)$ of $\mathbb{R}^n$, we consider the subset

$$P_e = \Big\{ \sum_{i=1}^{n} \alpha_i e_i | 0 \leq \alpha_i < 1 \Big\} \subset \mathbb{R}^n.$$

Remark 8.2.2. Let H be a lattice in $\mathbb{R}^n$. Then there exists an $\mathbb{R}$-basis $e = (e_1, \dots, e_n)$ of $\mathbb{R}^n$ such that e is a $\mathbb{Z}$-basis of H. The subset P_e is called a *fundamental domain* of H in this case. Note that every vector in $\mathbb{R}^n$ is congruent modulo H to a unique vector in P_e.

We will denote by μ the Lebesgue measure on $\mathbb{R}^n$. We will use the following properties of μ, where $S \subset \mathbb{R}^n$ is a measurable subset:

(1) ("invariance by translation") For any $t \in \mathbb{R}^n$, we have $\mu(S) = \mu(t + S)$.
(2) ("scaling") If $\varphi \colon \mathbb{R}^n \to \mathbb{R}^n$ is an $\mathbb{R}$-linear map, then $\mu(\varphi(S)) = |\det \varphi| \cdot \mu(S)$.
(3) ("σ-additivity") If S is the disjoint union of measurable subsets S_n for $n \in \mathbb{N}$, then

$$\mu(S) = \lim_{n \to \infty} \sum_{i=0}^{n} \mu(S_i) \in \mathbb{R} \cup \{\infty\}.$$

Lemma 8.2.3. *Let H be a lattice in $\mathbb{R}^n$, and $e = (e_1, \dots, e_n)$ an $\mathbb{R}$-basis of $\mathbb{R}^n$ which generates the $\mathbb{Z}$-module H. Then the subset $P_e \subset \mathbb{R}^n$ is measurable, and the number $\mu(P_e)$ does not depend on the choice of the basis e. It is given by*

$$\mu(P_e) = |\det(a_{ij})| \in \mathbb{R},$$

where $e_i = (a_{i1}, \dots, a_{in}) \in \mathbb{R}^n$, for $i = 1, \dots, n$.

Proof. The subset P_e is the intersection of the open subset $\{\sum_{i=1}^n \alpha_i e_i | -1 < \alpha_i < 1\}$ with the closed subset $\{\sum_{i=1}^n \alpha_i e_i | 0 \leq \alpha_i\}$, hence is measurable. Let $c = (c_1, \dots, c_n)$ be the canonical basis of $\mathbb{R}^n$, and consider the $\mathbb{R}$-linear automorphism φ of $\mathbb{R}^n$ given by mapping c_i to e_i for $i \in \{1, \dots, n\}$. The matrix of φ in the canonical basis c is (a_{ij}), so that by the property (2) of the Lebesgue measure recalled above, we have

$$\mu(P_e) = |\det \varphi| \cdot \mu(P_c) = |\det(a_{ij})|,$$

as $\mu(P_c) = 1$.

Now, let $f = (f_1, \dots, f_n)$ be another $\mathbb{R}$-basis of $\mathbb{R}^n$ which generates the $\mathbb{Z}$-module H, and consider the $\mathbb{R}$-linear automorphism ψ of $\mathbb{R}^n$ such that $\psi(e_i) = f_i$ for all $i \in \{1, \dots, n\}$. Then $\psi(P_e) = P_f$, and thus the property (2) above implies that

$$\mu(P_f) = |\det \psi| \cdot \mu(P_e). \tag{8.2.a}$$

Since e and f are both $\mathbb{Z}$-basis of H, there are elements $\alpha_{ij}, \beta_{ij} \in \mathbb{Z}$ for $i, j \in \{1, \dots, n\}$ such that, for all $j \in \{1, \dots, n\}$

$$f_j = \sum_{i=1}^{n} \alpha_{ij} e_i \quad \text{and} \quad e_j = \sum_{i=1}^{n} \beta_{ij} f_i.$$

In the basis e of $\mathbb{R}^n$, the matrix of ψ is (α_{ij}), while that of ψ^{-1} is (β_{ij}). Since these matrices belong to $M_n(\mathbb{Z}) \subset M_n(\mathbb{R})$, it follows that $\det \psi \in \mathbb{Z}^\times = \{1, -1\}$, hence (8.2.a) shows that $\mu(P_f) = \mu(P_e)$. □

DEFINITION 8.2.4. When H is a lattice in $\mathbb{R}^n$, its *volume* $v(H)$ is defined as the number $\mu(P_e) \in \mathbb{R}$, for any $\mathbb{R}$-basis e of $\mathbb{R}^n$ which generates the $\mathbb{Z}$-module H.

LEMMA 8.2.5. *Let $L \subset M$ be lattices in $\mathbb{R}^n$. Then the group M/L is finite, and*

$$v(L) = v(M) \cdot \mathrm{card}(M/L).$$

PROOF. Since the $\mathbb{Z}$-modules L, M are both free of rank n, it follows from Theorem 1.3.2 and its complement Proposition 1.3.13 that we may find a $\mathbb{Z}$-basis $(e_1, \dots, e_n)$ of M and nonzero integers $c_1, \dots, c_n \in \mathbb{N}$ such that $f = (c_1 e_1, \dots, c_n e_n)$ is a $\mathbb{Z}$-basis of L. Then $M/L \simeq (\mathbb{Z}/c_1\mathbb{Z}) \times \cdots \times (\mathbb{Z}/c_2\mathbb{Z})$ is finite, and

$$\mathrm{card}(M/L) = |c_1 \cdots c_n|.$$

Consider the $\mathbb{R}$-linear automorphism φ of $\mathbb{R}^n$ given by $\varphi(e_i) = c_i e_i$ for $i \in \{1, \dots, n\}$. Then by by the property (2) of the Lebesgue measure recalled above we have

$$v(L) = \mu(P_f) = |\det \varphi| \cdot \mu(P_e) = |c_1 \cdots c_n| \cdot v(M) = \mathrm{card}(M/L) \cdot v(M). \qquad \square$$

THEOREM 8.2.6 (Minkowski). *Let H be a lattice in $\mathbb{R}^n$ and $S \subset \mathbb{R}^n$ a measurable subset. Assume that $\mu(S) > v(H)$. Then there exist two distinct elements $x, y \in S$ such that $x - y \in H$.*

PROOF. Let e be an $\mathbb{R}$-basis of $\mathbb{R}^n$ which generates the $\mathbb{Z}$-module H. Recall from Remark 8.2.2 that $\mathbb{R}^n$ is the disjoint union of the subsets $h + P_e$ where h runs over H. Observe that the set H is countable, being in bijection with $\mathbb{Z}^n$. Pick a bijection $\mathbb{N} \xrightarrow{\sim} H$ and denote it by $i \mapsto h_i$. Then by σ-additivity (recalled in (3) above) we have

$$\mu(S) = \lim_{n \to \infty} \Big(\sum_{i=0}^{n} \mu(S \cap (h_i + P_e)) \Big) \in \mathbb{R} \cup \{\infty\}. \tag{8.2.b}$$

By invariance of the Lebesgue measure under translation (recalled in (1) above), we have for all $i \in \mathbb{N}$

$$\mu(S \cap (h_i + P_e)) = \mu((-h_i + S) \cap P_e). \tag{8.2.c}$$

If the conclusion of the theorem does not hold, then the subsets $-h_i + S \subset \mathbb{R}^n$ for $i \in \mathbb{N}$ are pairwise disjoint, so that by σ-additivity again

$$\mu(P_e) \geq \lim_{n \to \infty} \Big(\sum_{i=0}^{n} \mu((-h_i + S) \cap P_e) \Big) \in \mathbb{R} \cup \{\infty\}.$$

The left-hand side is $v(H)$ by definition, and the right-hand side is $\mu(S)$ by (8.2.b) and (8.2.c). Thus $v(H) \geq \mu(S)$, contradicting the assumption. $\square$

COROLLARY 8.2.7. *Let H be a lattice in $\mathbb{R}^n$, and $S \subset \mathbb{R}^n$ a measurable subset, which is convex and symmetric with respect to zero. Assume that one of the following conditions holds:*

(i) $\mu(S) > 2^n v(H)$,
(ii) $\mu(S) \geq 2^n v(H)$ *and S is compact.*

Then the subset $S \cap H \subset \mathbb{R}^n$ contains a nonzero vector.

Proof. Assume (i), and set $S' = 2^{-1}S \subset \mathbb{R}^n$. Then, by the property (2) of the Lebesgue measure,

$$\mu(S') = 2^{-n}\mu(S) > v(H),$$

hence by Theorem 8.2.6 there exist $x, y \in S'$ such that $x - y \in H \smallsetminus \{0\}$. Set $z = x - y$. Then $z \in H$, and

$$z = x - y = \frac{1}{2}(2x + (-2y))$$

belongs to S by symmetry and convexity. This proves the corollary in this case.

Assume (ii). We claim first that

$$S = \bigcap_{k \in \mathbb{N} \smallsetminus \{0\}} (1 + k^{-1})S. \tag{8.2.d}$$

Indeed, one inclusion is clear. Conversely, let us assume that $x \in (1 + k^{-1})S$ for all $k \in \mathbb{N} \smallsetminus \{0\}$ and prove that $x \in S$. If $x \notin S$, then as $\mathbb{R}^n \smallsetminus S$ is open (S being closed by assumption) we can find an element $\varepsilon > 0$ such that S does not meet the open ball centered in x of radius ε. As S is bounded, it is contained in an open ball centered at 0 of radius λ, for some $\lambda > 0$. Now pick an integer $\ell \geq \lambda/\varepsilon$. Then $x = (1 + \ell^{-1})y$ for some $y \in S$, hence $y - x = -\ell^{-1}y$, so that y belongs to the open ball centered at x of radius $\ell^{-1}\lambda$. Since $\ell^{-1}\lambda \leq \varepsilon$ and $y \in S$, we have obtained a contradiction, proving the claim (8.2.d).

For $k \in \mathbb{N} \smallsetminus \{0\}$, we have by the property (2) of the Lebesgue measure

$$\mu((1 + k^{-1})S) = (1 + k^{-1})^n \mu(S) > 2^n v(H),$$

hence it follows from (i) that the subset

$$U_k = (H \smallsetminus \{0\}) \cap (1 + k^{-1})S \subset \mathbb{R}^n$$

is nonempty. In addition the set U_k is finite, because H is a discrete subgroup and $(1 + k^{-1})S$ is bounded (by Lemma 8.1.2 and Lemma 8.1.3). Therefore the intersection

$$\bigcap_{k \in \mathbb{N} \smallsetminus \{0\}} U_k \subset \mathbb{R}^n$$

is nonempty, as every decreasing (for the inclusion relation) family of nonempty finite sets is stationary. Now

$$\begin{aligned}
\bigcap_{k \in \mathbb{N} \smallsetminus \{0\}} U_k &= \bigcap_{k \in \mathbb{N} \smallsetminus \{0\}} \Big((H \smallsetminus \{0\}) \cap (1 + k^{-1})S \Big) \\
&\subset (H \smallsetminus \{0\}) \cap \Big(\bigcap_{k \in \mathbb{N} \smallsetminus \{0\}} (1 + k^{-1})S \Big) \\
&= (H \smallsetminus \{0\}) \cap S,
\end{aligned}$$

where we have used (8.2.d) for the last equality. □

Remark 8.2.8. One may prove that a convex subset of $\mathbb{R}^n$ is automatically measurable.

CHAPTER 9

Ideal class group and units in number fields

1. The canonical embedding

When K is a number field of degree $n = [K : \mathbb{Q}]$, there are by Lemma 4.2.4 (in view of Proposition 4.2.5) exactly n morphisms of $\mathbb{Q}$-algebras $\sigma_1, \dots, \sigma_n \colon K \to \mathbb{C}$ (here we use the fact that the field $\mathbb{C}$ is algebraically closed). If $\iota \colon \mathbb{C} \to \mathbb{C}$ is the complex conjugation, then for every $i \in \{1, \dots, n\}$ there exists $j \in \{1, \dots, n\}$ such that $\iota \circ \sigma_i = \sigma_j$. We have $\sigma_i(K) \subset \mathbb{R}$ if and only if $\iota \circ \sigma_i = \sigma_i$. If $\sigma_i(K) \not\subset \mathbb{R}$, then there exists $j \neq i$ such that $\sigma_j = \iota \circ \sigma_i$. In particular the number of indices $i \in \{1, \dots, n\}$ such that $\sigma_i(K) \not\subset \mathbb{R}$ is even. Let us write

$$r_1 = \mathrm{card}\{i \in \{1, \dots, n\} | \sigma_i(K) \subset \mathbb{R}\},$$
$$2r_2 = \mathrm{card}\{i \in \{1, \dots, n\} | \sigma_i(K) \not\subset \mathbb{R}\},$$

so that

$$n = r_1 + 2r_2.$$

We reorder the σ_i's in such a way that $\sigma_1(K), \dots, \sigma_{r_1}(K) \subset \mathbb{R}$, and $\iota \circ \sigma_i = \sigma_{i+r_2}$ for $i \in \{r_1 + 1, \dots, r_1 + r_2\}$. This yields a ring morphism

$$\sigma \colon K \to \mathbb{R}^{r_1} \times \mathbb{C}^{r_2} \quad x \mapsto (\sigma_1(x), \dots, \sigma_{r_1+r_2}(x)).$$

Since K is a field and $\mathbb{R}^{r_1} \times \mathbb{C}^{r_2} \neq 0$ (as $n \geq 1$), it follows that the ring morphism σ is injective. We will often identify the group $\mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$ with $\mathbb{R}^n$ (note that this identification does not respect the ring structures).

Let d_K be the absolute discriminant of K (see Definition 5.1.9). Recall from Proposition 4.3.4 that we have

$$d_K = \det(\sigma_i(x_j))^2, \tag{9.1.a}$$

where $(x_1, \dots, x_n)$ is any $\mathbb{Z}$-basis of $\mathcal{O}_K$.

PROPOSITION 9.1.1. *Let E be a subgroup of K. Assume that E is free of rank n as a $\mathbb{Z}$-module, with basis $(x_1, \dots, x_n)$. Then $\sigma(E)$ is a lattice in $\mathbb{R}^n$, and its volume is*

$$v(\sigma(E)) = \frac{|\det(\sigma_i(x_j))|}{2^{r_2}}.$$

PROOF. For a given $j \in \{1, \dots, n\}$, the coordinates of the vector $\sigma(x_j)$ in the canonical basis of $\mathbb{R}^n$ are

$$(\sigma_1(x_j), \dots, \sigma_{r_1}(x_j), \Re(\sigma_{r_1+1}(x_j)), \Im(\sigma_{r_1+1}(x_j)), \dots, \Re(\sigma_{r_1+r_2}(x_j)), \Im(\sigma_{r_1+r_2}(x_j))), \tag{9.1.b}$$

where $\Re$ and $\Im$ denote the real and imaginary parts respectively. Consider the matrix $M \in M_n(\mathbb{R})$ whose j-th column is (9.1.b). We view $M \in M_n(\mathbb{C})$ via the embedding $\mathbb{R} \subset \mathbb{C}$, and denote by R_i the i-th row of M. Replacing R_i with $R_i + \mathrm{i}R_{i+1}$ (here i

denotes a complex root of -1) for $i \in \{r_1+1, r_1+3, \dots, r_1+2r_2-1\}$ shows that M has the same determinant as the matrix $M' \in M_n(\mathbb{C})$ whose j-th column is

$$(\sigma_1(x_j), \dots, \sigma_{r_1}(x_j), \sigma_{r_1+1}(x_j), \Im(\sigma_{r_1+1}(x_j)), \dots, \sigma_{r_1+r_2}(x_j), \Im(\sigma_{r_1+r_2}(x_j))). \tag{9.1.c}$$

Denote by R'_i the i-th row of M'. Replacing R'_i with $(-2\mathrm{i})R'_i + R'_{i-1}$ for $i \in \{r_1+2, r_1+4, \dots, r_1+2r_2\}$ shows that $(-2\mathrm{i})^{r_2} \det M' = \det M''$, where $M'' \in M_n(\mathbb{C})$ is the matrix whose j-th column is

$$(\sigma_1(x_j), \dots, \sigma_{r_1}(x_j), \sigma_{r_1+1}(x_j), \overline{\sigma_{r_1+1}(x_j)}, \dots, \sigma_{r_1+r_2}(x_j), \overline{\sigma_{r_1+r_2}(x_j)})),$$

where $z \mapsto \overline{z}$ denotes the complex conjugation. Since $\overline{\sigma_{r_1+j}(x_j)} = \sigma_{r_1+r_2+j}(x_j)$, it follows that the matrix M'' is obtained from the matrix $(\sigma_i(x_j))$ by permuting its rows. We conclude that

$$\det M = \pm(-2\mathrm{i})^{-r_2} \det(\sigma_i(x_j)). \tag{9.1.d}$$

Therefore by Proposition 4.3.4

$$(\det M)^2 = \pm 2^{-2r_2} \, \mathrm{D}_{K/\mathbb{Q}}(x_1, \dots, x_n),$$

which is nonzero by (3.2.5). We have proved that $M \in M_n(\mathbb{R})$ is invertible. It follows that the vectors $\sigma(x_1), \dots, \sigma(x_n) \in \mathbb{R}^n$ are $\mathbb{R}$-linearly independent (as those are the columns of M), so that $\sigma(E)$ is a lattice in $\mathbb{R}^n$. The formula for $v(\sigma(E))$ follows from Lemma 8.2.3 and (9.1.d). □

Proposition 9.1.2. *Let K be a number field, and d_K its absolute discriminant. Then*

$$v(\sigma(\mathcal{O}_K)) = \frac{\sqrt{|d_K|}}{2^{r_2}}.$$

If I is a nonzero ideal of $\mathcal{O}_K$, then $\sigma(I)$ is a lattice in $\mathbb{R}^n$, and we have

$$v(\sigma(I)) = \frac{\sqrt{|d_K|}}{2^{r_2}} N(I).$$

Proof. The $\mathbb{Z}$-module $\mathcal{O}_K$ is free of rank n by Corollary 5.1.6. Thus the first statement follows from (9.1.a) and Proposition 9.1.1.

By Theorem 1.3.2, we may find a $\mathbb{Z}$-basis $(x_1, \dots, x_n)$ of $\mathcal{O}_K$ and integers $c_1, \dots, c_s$ with $s \leq n$ and such that $(c_1 x_1, \dots, c_s x_s)$ is a $\mathbb{Z}$-basis of I. The quotient $\mathcal{O}_K/I$ is isomorphic to $(\mathbb{Z}/c_1\mathbb{Z}) \times \dots (\mathbb{Z}/c_s\mathbb{Z}) \times \mathbb{Z}^{n-s}$ and is finite by Corollary 6.4.2. This implies that $n = s$. Therefore by Proposition 9.1.1 the subgroup $\sigma(I) \subset \mathbb{R}^n$ is a lattice. Applying Lemma 8.2.5 to the inclusion of lattices $\sigma(I) \subset \sigma(\mathcal{O}_K)$ yields

$$v(\sigma(I)) = v(\mathcal{O}_K) \cdot \mathrm{card}(\sigma(\mathcal{O}_K)/\sigma(I)).$$

As the group morphism σ is injective, it induces an isomorphism $\mathcal{O}_K/I \simeq \sigma(\mathcal{O}_K)/\sigma(I)$, so that by the very definition of the absolute norm

$$\mathrm{card}(\sigma(\mathcal{O}_K)/\sigma(I)) = \mathrm{card}(\mathcal{O}_K/I) = N(I). \qquad \square$$

The above proposition will typically be combined with Minkowski's Theorem 8.2.6 to produce integers in $\mathcal{O}_K$ whose image under σ lies in certain subsets, as follows:

Corollary 9.1.3. *Let K be a number field, and d_K its absolute discriminant. Let B be a subset of $\mathbb{R}^n$, which is compact, convex, symmetric with respect to zero. If*

$$\mu(B) \geq 2^{n-r_2} \sqrt{|d_K|},$$

then there exists a nonzero element $x \in \mathcal{O}_K$ such that $\sigma(x) \in B$.

PROOF. This follows by combining Proposition 9.1.2 with Minkowski's Theorem (Corollary 8.2.7). □

2. Bounding the discriminant

Let $r_1, r_2 \in \mathbb{N}$. For every $t \in \mathbb{R}$ with $t > 0$, we consider the subset $B_t \subset \mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$ consisting of those elements $(y_1, \dots, y_{r_1}, z_1, \dots, z_{r_2})$ satisfying

$$(y_1, \dots, y_{r_1}, z_1, \dots, z_{r_2}) \in B_t \Longleftrightarrow \sum_{i=1}^{r_1} |y_i| + 2\sum_{i=1}^{r_2} |z_i| \le t. \tag{9.2.a}$$

LEMMA 9.2.1. *For $n = r_1 + 2r_2 > 0$ and $t > 0$, the measure of the subset B_t defined in* (9.2.a) *is*

$$\mu(B_t) = 2^{r_1}\Big(\frac{\pi}{2}\Big)^{r_2}\frac{t^n}{n!}.$$

PROOF. We argue by induction on r_1 and r_2. Let us set

$$V(r_1, r_2, t) = \mu(B_t).$$

When $r_1 = 1, r_2 = 0$, the subset $B_t \subset \mathbb{R}$ is $[-t, t]$, hence $V(1, 0, t) = 2t$. When $r_1 = 0, r_2 = 1$, the subset $B_t \subset \mathbb{C}$ is the disk $\{\rho e^{i\theta} | 0 \le \rho \le t/2\}$, hence $V(0, 1, t) = \frac{\pi t^2}{4}$. Thus the formula is correct in both these cases.

$r_1 \to r_1{+}1$: The subset $B_t \subset \mathbb{R}^{r_1+1} \times \mathbb{C}^{r_2}$ consists of those elements $(y, y_1, \dots, y_{r_1}, z_1, \dots, z_{r_2}) \in \mathbb{R} \times \mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$ verifying

$$|y| + \sum_{i=1}^{r_1} |y_i| + 2\sum_{i=1}^{r_2} |z_i| \le t.$$

Fubini's theorem yields

$$\begin{aligned} V(r_1 + 1, r_2, t) &= \int_{-t}^{t} V(r_1, r_2, t - |y|)\, dy \\ &= \int_{-t}^{t} 2^{r_1}\Big(\frac{\pi}{2}\Big)^{r_2}\frac{(t - |y|)^n}{n!}\, dy \\ &= 2\int_{0}^{t} 2^{r_1}\Big(\frac{\pi}{2}\Big)^{r_2}\frac{(t - y)^n}{n!}\, dy \\ &= 2\int_{0}^{t} 2^{r_1}\Big(\frac{\pi}{2}\Big)^{r_2}\frac{x^n}{n!}\, dx \qquad \text{(setting } x = t - y\text{)} \\ &= 2^{r_1+1}\Big(\frac{\pi}{2}\Big)^{r_2}\frac{t^{n+1}}{(n+1)!}, \end{aligned}$$

as required.

$r_2 \to r_2{+}1$: The subset $B_t \subset \mathbb{R}^{r_1} \times \mathbb{C}^{r_2+1}$ consists of those elements $(y_1, \dots, y_{r_1}, z_1, \dots, z_{r_2}, z) \in \mathbb{R}^{r_1} \times \mathbb{C}^{r_2} \times \mathbb{C}$ verifying

$$\sum_{i=1}^{r_1} |y_i| + 2\sum_{i=1}^{r_2} |z_i| + 2|z| \le t.$$

Denoting by $d\mu(z)$ is the Lebesgue measure on $\mathbb{C}$, Fubini's theorem now yields

$$\begin{aligned}
V(r_1, r_2+1) &= \int_{|z|\le t/2} V(r_1, r_2, t-2|z|)d\mu(z) \\
&= \int_{|z|\le t/2} 2^{r_1}\Big(\frac{\pi}{2}\Big)^{r_2}\frac{(t-2|z|)^n}{n!}\,d\mu(z) \\
&= \int_{\rho=0}^{t/2}\int_{\theta=0}^{2\pi} 2^{r_1}\Big(\frac{\pi}{2}\Big)^{r_2}\frac{(t-2\rho)^n}{n!}\rho\,d\rho\,d\theta \qquad \text{(setting } z=\rho e^{i\theta}\text{)} \\
&= 2^{r_1}\Big(\frac{\pi}{2}\Big)^{r_2}\frac{2\pi}{n!}\int_{\rho=0}^{t/2}(t-2\rho)^n\rho\,d\rho \\
&= 2^{r_1}\Big(\frac{\pi}{2}\Big)^{r_2}\frac{2\pi}{n!}\int_{x=0}^{t}x^n\frac{t-x}{2}\frac{dx}{2} \qquad \text{(setting } x=t-2\rho\text{)} \\
&= 2^{r_1}\Big(\frac{\pi}{2}\Big)^{r_2+1}\frac{1}{n!}\Big(\int_{x=0}^{t}tx^n\,dx-\int_{x=0}^{t}x^{n+1}\,dx\Big) \\
&= 2^{r_1}\Big(\frac{\pi}{2}\Big)^{r_2+1}\frac{1}{n!}\Big(\frac{t^{n+2}}{n+1}-\frac{t^{n+2}}{n+2}\Big) \\
&= 2^{r_1}\Big(\frac{\pi}{2}\Big)^{r_2+1}\frac{t^{n+2}}{(n+2)!},
\end{aligned}$$

as required. □

Lemma 9.2.2 (Arithmetic mean versus geometric mean). *Let $n \in \mathbb{N}\smallsetminus\{0\}$, and $a_1,\dots,a_n>0$ be real numbers. Then*

$$a_1\cdots a_n \le \Big(\frac{a_1+\cdots+a_n}{n}\Big)^n$$

Proof. Let $g=(a_1\cdots a_n)^{-1/n}\in\mathbb{R}$ with $g>0$. Replacing a_i with ga_i for all $i\in\{1,\dots,n\}$, we may assume that $a_1\cdots a_n=1$. Then it suffices to prove that

$$n \le a_1+\cdots+a_n \quad \text{when } a_1\cdots a_n=1.$$

This is done by induction on n. The case $n=1$ is clear. Assume that $n>1$. Upon reordering the elements $a_1,\dots,a_n$, we may assume that $a_{n-1}\le 1$ and $a_n\ge 1$. Then

$$0\le (a_n-1)(1-a_{n-1}) = a_{n-1}+a_n-a_na_{n-1}-1,$$

so that

$$a_na_{n-1}\le a_{n-1}+a_n-1. \tag{9.2.b}$$

Then applying the induction hypothesis to $a_1,\dots,a_{n-2},a_{n-1}a_n$ yields

$$n-1\le a_1+\cdots+a_{n-2}+a_{n-1}a_n.$$

Combining with (9.2.b) yields the result. □

Proposition 9.2.3. *Let K be a number field, and n, r_1, r_2 as in §9.1. Let d_K be the absolute discriminant of K (Definition 5.1.9). Let I be a nonzero ideal of $\mathcal{O}_K$. Then I contains a nonzero element x such that*

$$|\,\mathrm{N}_{K/\mathbb{Q}}(x)| \le \Big(\frac{4}{\pi}\Big)^{r_2}\frac{n!}{n^n}\sqrt{|d_K|}\cdot\mathrm{N}(I).$$

Proof. For $t \in \mathbb{R}$ with $t > 0$, consider the subset B_t defined in (9.2.a), and the canonical embedding $\sigma\colon K \to \mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$ (see §9.1). Setting

$$t = \Big(\frac{2^{n-r_1}}{\pi^{r_2}} n! \sqrt{|d_K|} \cdot \mathrm{N}(I)\Big)^{1/n} \tag{9.2.c}$$

we have by Lemma 9.2.1

$$\mu(B_t) = 2^{n-r_2}\sqrt{|d_K|} \cdot \mathrm{N}(I),$$

so that by Proposition 9.1.2

$$\mu(B_t) = 2^n v(\sigma(I)).$$

Then by Corollary 8.2.7 we may find a nonzero element $x \in I$ such that $\sigma(x) \in B_t$ (the subset B_t is closed and bounded, hence compact). By Proposition 4.3.3 (in view of Proposition 4.2.5), we have

$$\mathrm{N}_{K/\mathbb{Q}}(x) = \prod_{i=1}^{r_1} \sigma_i(x) \cdot \prod_{r_1+1}^{r_1+r_2} \sigma_i(x) \cdot \prod_{i=r_1+r_2+1}^{r_1+2r_2} \overline{\sigma_i(x)},$$

where $z \mapsto \overline{z}$ is the complex conjugation, so that

$$|\,\mathrm{N}_{K/\mathbb{Q}}(x)| = \prod_{i=1}^{r_1} |\sigma_i(x)| \cdot \prod_{r_1+1}^{r_1+r_2} |\sigma_i(x)|^2.$$

Using the inequality of Lemma 9.2.2 we have

$$|\,\mathrm{N}_{K/\mathbb{Q}}(x)| \leq \Big(\frac{1}{n}\sum_{i=1}^{r_1} |\sigma_i(x)| + \frac{2}{n}\sum_{r_1+1}^{r_1+r_2} |\sigma_i(x)|\Big)^n \leq \frac{t^n}{n^n},$$

where the last inequality follows from the fact that $\sigma(x) \in B_t$. Combining this inequality with (9.2.c), we obtain the statement. □

Corollary 9.2.4. *Let K be a number field, and n, r_2 as in §9.1. Let d_K be the absolute discriminant of K. Then every class in the ideal class group $\mathcal{C}(\mathcal{O}_K)$ (see Definition 6.3.11) contains a nonzero ideal $I \subset \mathcal{O}_K$ such that*

$$\mathrm{N}(I) \leq \Big(\frac{4}{\pi}\Big)^{r_2} \frac{n!}{n^n}\sqrt{|d_K|}.$$

Proof. Let us fix a class $\alpha \in \mathcal{C}(\mathcal{O}_K)$. Let J be a nonzero fractional ideal in the class α. After multiplying J with an element of $K^\times$ (which does not change the fact that its class is α), we may assume that $J^{-1} \subset \mathcal{O}_K$, i.e. J^{-1} is an ideal. Applying Proposition 9.2.3, we find a nonzero element $x \in J^{-1}$ such that

$$|\,\mathrm{N}_{K/\mathbb{Q}}(x)| \leq \Big(\frac{4}{\pi}\Big)^{r_2} \frac{n!}{n^n}\sqrt{|d_K|}\,\mathrm{N}(J^{-1}). \tag{9.2.d}$$

Observe that $xJ \subset J^{-1}J = A$, hence $I = xJ$ is a nonzero ideal of $\mathcal{O}_K$. In addition I lies in the same class as J, namely α. By multiplicativity of the absolute norms (Proposition 6.4.5) and Proposition 6.4.1, we have, as $x\mathcal{O}_K = IJ^{-1}$

$$\mathrm{N}(I)\,\mathrm{N}(J^{-1}) = \mathrm{N}(IJ^{-1}) = \mathrm{N}(x\mathcal{O}_K) = |\,\mathrm{N}_{K/\mathbb{Q}}(x)| \tag{9.2.e}$$

Combining (9.2.d) with (9.2.e), and dividing by $\mathrm{N}(J^{-1})$ (which is nonzero, being by definition the cardinality of a group) yields the result. □

COROLLARY 9.2.5. *Let K be a number field of degree n and absolute discriminant d_K. If $n \geq 2$, then*

$$|d_K| \geq \frac{\pi}{3}\Big(\frac{3\pi}{4}\Big)^{n-1},$$

and $n/\log|d_K|$ is bounded by a constant independent of K.

PROOF. Let us apply Corollary 9.2.4 to the trivial class (the class of the ideal $\mathcal{O}_K$). This yields a nonzero ideal I of $\mathcal{O}_K$ such that

$$\mathrm{N}(I) \leq \Big(\frac{4}{\pi}\Big)^{r_2}\frac{n!}{n^n}\sqrt{|d_K|}.$$

As $\mathrm{N}(I) = \mathrm{card}(\mathcal{O}_K/I) \geq 1$, we deduce that

$$\sqrt{|d_K|} \geq \Big(\frac{\pi}{4}\Big)^{r_2}\frac{n^n}{n!}.$$

Since $2r_2 \leq n$ and $\pi \leq 4$ (see Lemma 9.2.6 below), we have $|d_K| \geq a_n$, where

$$a_n = \Big(\frac{\pi}{4}\Big)^{n}\frac{n^{2n}}{(n!)^2}.$$

We have $a_2 = \pi^2/4$, and using the binomial formula

$$\frac{a_{n+1}}{a_n} = \frac{\pi}{4}\Big(1+\frac{1}{n}\Big)^{2n} = \frac{\pi}{4}\Big(1+2+\sum_{i=2}^{2n}\binom{2n}{i}\frac{1}{n^i}\Big) \geq \frac{3\pi}{4}.$$

Therefore

$$a_n \geq a_2\Big(\frac{3\pi}{4}\Big)^{n-2} = \frac{\pi^2}{4}\Big(\frac{3\pi}{4}\Big)^{n-2} = \frac{\pi}{3}\Big(\frac{3\pi}{4}\Big)^{n-1},$$

as required for the first statement. The second follows by taking logarithms. □

LEMMA 9.2.6. *We have $3 < \pi < 4$.*

PROOF. For instance, observe that

$$\frac{1}{2} = \int_0^{1/2} dt < \int_0^{1/2}\frac{dt}{\sqrt{1-t^2}} = \arcsin\Big(\frac{1}{2}\Big) - \arcsin(0) = \frac{\pi}{6},$$

and that

$$1 > \int_0^1 \frac{dt}{1+t^2} = \arctan(1) - \arctan(0) = \frac{\pi}{4}.$$ □

3. Discriminant and ideal class group

PROPOSITION 9.3.1. *Let $K = \mathbb{Q}(\sqrt{d})$ be a quadratic field, where*

$$d \in \{2, 3, 5, 13, -1, -2, -3, -7\}.$$

Then the ring $\mathcal{O}_K$ is a principal ideal domain.

PROOF. Let us assume that $K = \mathbb{Q}(\sqrt{d})$, where $d \in \mathbb{Z} \smallsetminus \{1\}$ is an arbitrary square-free integer. By Corollary 9.2.4 every class in $\mathcal{C}(\mathcal{O}_K)$ contains a nonzero ideal I such that

$$\mathrm{N}(I) \leq \Big(\frac{4}{\pi}\Big)^{r_2}\frac{n!}{n^n}\sqrt{|d_K|} = \Big(\frac{4}{\pi}\Big)^{r_2}\frac{\sqrt{|d_K|}}{2},$$

where d_K is the absolute discriminant of K, namely (see Example 5.1.10)

$$d_K = \begin{cases} d & \text{if } d = 1 \mod 4 \\ 4d & \text{if } d = 2, 3 \mod 4. \end{cases}$$

Assume that K is real, i.e. $d > 0$. Then $r_2 = 0$, and

$$\frac{\sqrt{|d_K|}}{2} < 2$$

when $d_K \leq 15$. For $d = 1 \mod 4$, this holds when $d \in \{5, 13\}$. For $d = 2, 3 \mod 4$, this holds when $d_K = 4d \in \{8, 12\}$, that is $d \in \{2, 3\}$.

Assume now that K is imaginary, i.e. $d < 0$. Then $r_2 = 1$. If

$$-d_K \leq 9,$$

then, as $\pi > 3$ (see Lemma 9.2.6)

$$\mathrm{N}(I) \leq \left(\frac{4}{\pi}\right)^{r_2} \frac{\sqrt{|d_K|}}{2} < \frac{2\sqrt{-d_K}}{3} \leq 2.$$

This is achieved for $d \in \{-3, -7\}$ when $d = 1 \mod 4$, and for $d \in \{-1, -2\}$ when $d = 2, 3 \mod 4$.

Therefore for the values of d indicated in the statement of the proposition, we have proved that every nonzero fractional ideal of $\mathcal{O}_K$ has the same class in $\mathcal{C}(\mathcal{O}_K)$ as a nonzero ideal I of $\mathcal{O}_K$ satisfying

$$\mathrm{N}(I) < 2.$$

We must thus have $\mathrm{N}(I) = 1$, which means that $\mathcal{O}_K/I = 0$, and thus $I = \mathcal{O}_K$. Therefore the group $\mathcal{C}(\mathcal{O}_K)$ possesses a single element (the class of $\mathcal{O}_K$), which implies by Proposition 6.3.12 that $\mathcal{O}_K$ is a principal ideal domain. □

Remark 9.3.2. The list figuring in Proposition 9.3.1 is far from exhaustive.

Theorem 9.3.3 (Hermite–Minkowski). *Let K be a number field with absolute discriminant d_K. If $K \neq \mathbb{Q}$, then $d_K \notin \{1, -1\}$.*

Proof. This follows from Corollary 9.2.5, as $\pi/3 > 1$ and $3\pi/4 > 1$ by Lemma 9.2.6. □

Lemma 9.3.4. *Let K be a number field. Then for each nonzero integer $q \in \mathbb{Z}$, there are only finitely many nonzero ideals I of $\mathcal{O}_K$ such that $\mathrm{N}(I) = q$.*

Proof. If I is a nonzero ideal of $\mathcal{O}_K$ such that $\mathrm{N}(I) = q$, then by Lemma 6.4.4 the ideal I is among the ideals containing $q\mathcal{O}_K$, and there are only finitely many such ideals because $\mathcal{O}_K/q\mathcal{O}_K$ is finite (recall that $\mathrm{card}(\mathcal{O}_K/q\mathcal{O}_K) = |\mathrm{N}_{K/\mathbb{Q}}(q)| < \infty$ by Proposition 6.4.1). □

Theorem 9.3.5 (Dirichlet). *For every number field K, the ideal class group $\mathcal{C}(\mathcal{O}_K)$ is finite.*

Proof. By Corollary 9.2.4 the set $\mathcal{C}(\mathcal{O}_K)$ is the set of classes of nonzero ideals I of $\mathcal{O}_K$ satisfying $\mathrm{N}(I) \leq \alpha$, where

$$\alpha = \left(\frac{4}{\pi}\right)^{r_2} \frac{n!}{n^n} \sqrt{|d_K|} \in \mathbb{R}.$$

It follows from Lemma 9.3.4, applied to each of the finitely many integers q such that $1 \leq q \leq \alpha$, that there are only finitely such nonzero ideals I, and thus only finitely many classes in $\mathcal{O}_K$. □

We will use the fact the "the coefficients of a polynomial are polynomial in its roots", so let us formalise this statement. Let $n \in \mathbb{N}$. We will introduce polynomials

$$F_{0,n}, \dots, F_{n,n} \in \mathbb{Z}[Y_1, \dots, Y_n],$$

which are, up to sign, the so-called elementary symmetric functions. Let us set $R = \mathbb{Z}[Y_1, \dots, Y_n]$, and consider the polynomial

$$(X - Y_1) \cdots (X - Y_n) \in R[X].$$

We then define $F_{0,n}, \dots, F_{n,n} \in R$ as its coefficients, so that

$$(X - Y_1) \cdots (X - Y_n) = F_{n,n}X^n + \cdots + F_{0,n} \in \mathbb{Z}[X, Y_1, \dots, Y_n]. \tag{9.3.a}$$

THEOREM 9.3.6 (Hermite). *The field $\mathbb{C}$ contains only finitely many number fields of given absolute discriminant.*

PROOF. We know by Corollary 9.2.5 that the degree of a number field of given absolute discriminant is bounded. Hence it will suffice to prove that $\mathbb{C}$ contains only finitely many of number fields of given degree n and discriminant d. Since for a given n, there are only finitely many pairs $(r_1, r_2) \in \mathbb{N}^2$ such that $n = r_1 + 2r_2$, we may fix the integers r_1, r_2, d and show that $\mathbb{C}$ contains only finitely many number fields admitting exactly r_1 real embeddings and $2r_2$ complex nonreal embeddings, and having discriminant d.

So we consider a number field K of degree n and discriminant $d_K = d$, and use the notation above (at this point we do not choose a particular embedding $K \subset \mathbb{C}$). We consider the subset $B \subset \mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$ of elements $(y_1, \dots, y_{r_1}, z_1, \dots, z_{r_2})$ such that (as usual $\overline{u} \in \mathbb{C}$ denotes the complex conjugate of $u \in \mathbb{C}$)

$$\text{if } r_1 > 0\text{:} \begin{cases} |y_1| \leq 2^{n-1}\left(\frac{\pi}{2}\right)^{-r_2}\sqrt{|d_K|}, \\ |y_i| \leq \frac{1}{2} \text{ for } i = 2, \dots, r_1, \\ |z_i| \leq \frac{1}{2} \text{ for } i = 1, \dots, r_2. \end{cases} \qquad \text{if } r_1 = 0\text{:} \begin{cases} |z_1 - \overline{z_1}| \leq 2^n\left(\frac{\pi}{2}\right)^{1-r_2}\sqrt{|d_K|}, \\ |z_1 + \overline{z_1}| \leq 1, \\ |z_i| \leq \frac{1}{2} \text{ for } i = 2, \dots, r_2. \end{cases}$$

The subset B is compact, convex, symmetric with respect to 0. If $r_1 > 0$, we have

$$\mu(B) = \left(2^n\left(\frac{\pi}{2}\right)^{-r_2}\sqrt{|d_K|}\right) \cdot (1)^{r_1 - 1} \cdot \left(\frac{\pi}{4}\right)^{r_2} = 2^{n-r_2}\sqrt{|d_K|}.$$

(Note that B is the product of r_1 intervals and r_2 disks.) If $r_1 = 0$, writing $z_1 = x + iy$ with $x, y \in \mathbb{R}$ we have $|z_1 - \overline{z_1}| = 2|y|$ and $|z_1 + \overline{z_1}| = 2|x|$, so that

$$\mu(B) = \left(2^n\left(\frac{\pi}{2}\right)^{2-r_2}\sqrt{|d_K|}\right) \cdot (1) \cdot \left(\frac{\pi}{4}\right)^{r_2 - 2} = 2^{n-r_2}\sqrt{|d_K|}.$$

In any case, by Corollary 9.1.3 we find a nonzero element $x \in \mathcal{O}_K$ such that $\sigma(x) \in B$.

Next, we claim that

$$\sigma_i(x) \neq \sigma_1(x) \quad \text{for all } i = 2, \dots, n. \tag{9.3.b}$$

Indeed, recall that $\mathrm{N}_{K/\mathbb{Q}}(x) \in \mathbb{Q} \smallsetminus \{0\}$ by Lemma 3.1.10, and that $\mathrm{N}_{K/\mathbb{Q}}(x) \in \mathbb{Z}$ by Corollary 5.1.2, so that $|\mathrm{N}_{K/\mathbb{Q}}(x)| \geq 1$ (alternatively this follows from Proposition 6.4.1). Thus, by Proposition 4.3.3 (and Proposition 4.2.5) we have

$$\prod_{i=1}^{n} |\sigma_i(x)| = |\mathrm{N}_{K/\mathbb{Q}}(x)| \geq 1. \tag{9.3.c}$$

If $r_1 > 0$, we have $|\sigma_i(x)| \leq \frac{1}{2}$ for $i = 2, \dots, n$ (because $\sigma(x) \in B$), so that $|\sigma_1(x)| \geq 1$ by (9.3.c), from which (9.3.b) follows.

If $r_1 = 0$, note that $|\sigma_{j+r_2}(x)| = |\overline{\sigma_j(x)}| = |\sigma_j(x)|$ for $j = 1, \dots, r_2$. Thus we have $|\sigma_i(x)| \leq \frac{1}{2}$ for $i \in \{1, \dots, n\} \smallsetminus \{1, r_2 + 1\}$ (because $\sigma(x) \in B$), so that $|\sigma_1(x)| = |\sigma_{r_2+1}(x)| \geq 1$. In particular $\sigma_1(x) \neq \sigma_i(x)$ when $i \notin \{1, r_2 + 1\}$. Moreover the condition $|\sigma_1(x) + \overline{\sigma_1(x)}| \leq 1$ (as $\sigma(x) \in B$) together with the fact that $|\sigma_1(x)| \geq 1$ implies that $\sigma_1(x) \notin \mathbb{R}$, so that $\sigma_1(x) \neq \overline{\sigma_1(x)} = \sigma_{r_2+1}(x)$. We have established (9.3.b) also in this case.

Let us now prove that $\mathbb{Q}(x) = K$. Assume that $[K : \mathbb{Q}(x)] > 1$. As the field extension $K/\mathbb{Q}(x)$ is separable (see Proposition 4.1.16), by Lemma 4.2.4 (in view of Proposition 4.2.5) each morphism of $\mathbb{Q}$-algebra $\mathbb{Q}(x) \to \mathbb{C}$ admits at least two distinct extensions to a morphism of $\mathbb{Q}$-algebras $K \to \mathbb{C}$. In particular $\sigma_1|_{\mathbb{Q}(x)} \colon \mathbb{Q}(x) \to \mathbb{C}$ extends to a morphism of $\mathbb{Q}$-algebras $\alpha \colon K \to \mathbb{C}$ which is not σ_1. Since $\{\sigma_1, \dots, \sigma_n\}$ is the set of morphisms of $\mathbb{Q}$-algebras $K \to \mathbb{C}$, we find an index $i \in \{2, \dots, n\}$ such that $\alpha = \sigma_i$. As $\alpha|_{\mathbb{Q}(x)} = \sigma_1$, we have $\sigma_i(x) = \alpha(x) = \sigma_1(x)$, a contradiction with (9.3.b), proving that $K = \mathbb{Q}(x)$.

We now consider the polynomials $F_{j,n} \in \mathbb{Z}[Y_1, \dots, Y_n]$ defined in (9.3.a). By the definition of B, for $i \in \{1, \dots, n\}$ the elements $\sigma_i(x) \in \mathbb{C}$ are bounded (by this we mean that the real numbers $|\sigma_i(x)|$ are bounded), hence so are the elements

$$F_{j,n}(\sigma_1(x), \dots, \sigma_n(x)) \in \mathbb{C}, \quad \text{for } j = 0, \dots, n. \tag{9.3.d}$$

We emphasize that we obtain a uniform bound, which depends only on the integers r_1, r_2, and not on the particular number field K having the given invariants r_1, r_2. But the elements (9.3.d) coincide with the coefficients of the characteristic polynomial $\chi_{K/\mathbb{Q}}(x)$ by Proposition 4.3.3, and therefore by Proposition 5.1.1 belong to $\mathbb{Z}$. Thus the characteristic polynomial $\chi_{K/\mathbb{Q}}(x) \in \mathbb{Q}[X]$ can take only finitely many values.

Now if $K \subset \mathbb{C}$, then $x \in \mathbb{C}$ is among the roots of the polynomial $\chi_{K/\mathbb{Q}}(x) \in \mathbb{C}[X]$, by the Cayley–Hamilton theorem (Proposition 3.1.6). Therefore there are only finitely many possibilities for the element $x \in \mathbb{C}$, hence also for $K = \mathbb{Q}(x) \subset \mathbb{C}$. □

Remark 9.3.7. Since every number field admits an embedding into $\mathbb{C}$, it follows from Theorem 9.3.6 that there are only finitely many isomorphism classes of number fields of given absolute discriminant.

4. Dirichlet's unit Theorem

We recall that an element $x \in K$ is called a *root of unity* if there exists an integer $q \in \mathbb{N} \smallsetminus \{0\}$ such that $x^q = 1$.

Theorem 9.4.1 (Dirichlet). *Let K be a number field. Consider the integers r_1, r_2 defined in §1, and set $r = r_1 + r_2 - 1$. Let $G \subset K^\times$ be the subgroup of roots of unity in K. Then the group G is finite and cyclic, and there exists a group isomorphism*

$$(\mathcal{O}_K)^\times \simeq \mathbb{Z}^r \times G.$$

Remark 9.4.2. Theorem 9.4.1 shows that there exist units $u_1, \dots, u_r \in (\mathcal{O}_K)^\times$ such that each unit of $(\mathcal{O}_K)^\times$ can be written in a unique way as

$$\xi u_1^{n_1} \cdots u_r^{n_r}, \text{ where } n_1, \dots, n_r \in \mathbb{Z}, \text{ and } \xi \in K \text{ is a root of unity.}$$

Such a system $(u_1, \dots, u_r)$ is called a *fundamental system of units* of K.

The proof of Theorem 9.4.1 is somewhat long, so we first establish a few facts. We use the injective ring morphisms

$$\sigma_1, \dots, \sigma_{r_1} \colon K \to \mathbb{R} \quad \text{and} \quad \sigma_{r_1+1}, \dots, \sigma_{r_1+r_2} \colon K \to \mathbb{C}$$

described at the beginning of §1 to define the map, called the *logarithmic embedding*:

$$L \colon K^\times \to \mathbb{R}^{r_1+r_2}, \quad x \mapsto (\log|\sigma_1(x)|, \dots, \log|\sigma_{r_1+r_2}(x)|).$$

Observe that L is a group morphism.

LEMMA 9.4.3. *For any bounded subset B of $\mathbb{R}^{r_1+r_2}$, the set $(\mathcal{O}_K)^\times \cap L^{-1}B$ is finite.*

PROOF. Let $C = (\mathcal{O}_K)^\times \cap L^{-1}B$. As B is bounded, so is $\log|\sigma_i(C)|$, and thus also $|\sigma_i(C)|$, for each $i \in \{1, \dots, r_1 + r_2\}$. Therefore the elements $\sigma_i(x) \in \mathbb{C}$, for $x \in C$, are bounded. Let us consider the polynomials $F_{j,n} \in \mathbb{Z}[Y_1, \dots, Y_n]$ defined in (9.3.a), so that by Proposition 4.3.3, the coefficients of the characteristic polynomial $\chi_{K/\mathbb{Q}}(x)$ are the elements

$$F_{j,n}(\sigma_1(x), \dots, \sigma_n(x)) \in \mathbb{C}, \quad \text{for } j = 0, \dots, n. \tag{9.4.a}$$

As x runs over C, the elements (9.4.a) are bounded, and belong to $\mathbb{Z}$ by Proposition 5.1.1. Therefore the set of polynomials $\chi_{K/\mathbb{Q}}(x) \in \mathbb{Z}[X]$, where x runs over C, is finite. Since $x \in K$ is among the finitely many roots of $\chi_{K/\mathbb{Q}}(x)$ in K (by the Cayley–Hamilton theorem, see Proposition 3.1.6), we deduce that the set C is finite. □

LEMMA 9.4.4. *The group G of roots of unity in $K^\times$ coincides with $(\mathcal{O}_K)^\times \cap \ker L$, and is finite and cyclic.*

PROOF. Taking $B = \{0\}$ in Lemma 9.4.3, we deduce that the group $H = (\mathcal{O}_K)^\times \cap \ker L$ is finite. Being a subgroup of $(\mathcal{O}_K)^\times$, we see using Proposition 1.3.5 that H is a finite cyclic group. Each element of H has finite order (because H is finite), hence is a root of unity, so that $H \subset G$. Conversely let $x \in K$ be a root of unity, and $q \in \mathbb{N} \smallsetminus \{0\}$ be such that $x^q = 1$. Then x is a root of the monic polynomial $X^q - 1$, and is thus integral over $\mathbb{Z}$, so that $x \in (\mathcal{O}_K)^\times$. Moreover, for any $i \in \{1, \dots, r_1 + r_2\}$, we have $\sigma_i(x)^q = 1$, hence $|\sigma_i(x)|^q = 1$, which implies $q \log|\sigma_i(x)| = 0$, and thus $\log|\sigma_i(x)| = 0$. We conclude that $L(x) = 0$. It follows that $G \subset H$, so that $G = H$. □

We now consider the $\mathbb{R}$-subspace

$$W = \Big\{(y_1, \dots, y_{r_1+r_2}) \mid \sum_{i=1}^{r_1} y_i + 2 \sum_{i=r_1+1}^{r_1+r_2} y_i = 0\Big\} \subset \mathbb{R}^{r_1+r_2}, \tag{9.4.b}$$

and set

$$r = \dim_{\mathbb{R}} W = r_1 + r_2 - 1.$$

LEMMA 9.4.5. *We have $L((\mathcal{O}_K)^\times) \subset W$.*

PROOF. For $x \in (\mathcal{O}_K)^\times$, we have by Proposition 4.3.3 (and Proposition 4.2.5)

$$\mathrm{N}_{K/\mathbb{Q}}(x) = \prod_{i=1}^{n} \sigma_i(x) = \prod_{i=1}^{r_1} \sigma_i(x) \prod_{i=r_1+1}^{r_1+r_2} \sigma_i(x)\overline{\sigma_i(x)},$$

where $y \mapsto \overline{y}$ denotes the complex conjugation. By Corollary 5.1.3, we have $\mathrm{N}_{K/\mathbb{Q}}(x) \in \mathbb{Z}^\times = \{1, -1\}$. Taking absolute values and then logarithms, we obtain

$$0 = \sum_{i=1}^{r_1} \log|\sigma_i(x)| + \sum_{i=r_1+1}^{r_1+r_2} \big(\log|\sigma_i(x)| + \log|\overline{\sigma_i(x)}|\big) = \sum_{i=1}^{r_1} \log|\sigma_i(x)| + 2\sum_{i=r_1+1}^{r_1+r_2} \log|\sigma_i(x)|,$$

which shows that $L(x) \in W$. □

Lemma 9.4.6. *Let s be the dimension of the $\mathbb{R}$-subspace generated by $L((\mathcal{O}_K)^\times)$ in $\mathbb{R}^{r_1+r_2}$. Then $s \leq r$, and there exists a group isomorphism*

$$(\mathcal{O}_K)^\times \simeq \mathbb{Z}^s \times G.$$

Proof. By Lemma 9.4.3, for every compact subset B of $\mathbb{R}^{r_1+r_2}$ the intersection $L((\mathcal{O}_K)^\times) \cap B$ is finite, being the image of $(\mathcal{O}_K)^\times \cap L^{-1}B$. Therefore by Lemma 8.1.2 the subgroup $L((\mathcal{O}_K)^\times) \subset \mathbb{R}^{r_1+r_2}$ is discrete, hence by Theorem 8.1.4 it is generated by a system $(e_1, \dots, e_s)$ of $\mathbb{R}$-linearly independent vectors in $\mathbb{R}^{r_1+r_2}$ (note that s is then the dimension of the $\mathbb{R}$-subspace generated by $L((\mathcal{O}_K)^\times)$). We have $e_1, \dots, e_s \in W$ by Lemma 9.4.5, and as $\dim_{\mathbb{R}} W = r$, we have $s \leq r$. Thus the $\mathbb{Z}$-module $L((\mathcal{O}_K)^\times)$ is free of rank $s \leq r$, a $\mathbb{Z}$-basis being given by $(e_1, \dots, e_s)$. Pick elements $f_1, \dots, f_s \in (\mathcal{O}_K)^\times$ such that $L(f_i) = e_i$ for $i = 1, \dots, s$. For $x \in (\mathcal{O}_K)^\times$, denote by $(x_1, \dots, x_s) \in \mathbb{Z}^s$ the coordinates of $L(x)$ in the basis $(e_1, \dots, e_s)$. Then the element

$$y = x \prod_{i=1}^{s} f_i^{-x_i} \in (\mathcal{O}_K)^\times$$

maps to $0 \in \mathbb{R}^{r_1+r_2}$ under L, hence belongs to $G = \ker L$. It is clear that the maps $x \mapsto x_i$ and $x \mapsto y$ define group morphisms $(\mathcal{O}_K)^\times \to \mathbb{Z}$ and $(\mathcal{O}_K)^\times \to G$. We thus obtain a group morphism

$$(\mathcal{O}_K)^\times \to \mathbb{Z}^s \times G, \quad x \mapsto (x_1, \dots, x_s, y).$$

Conversely, we define a group morphism

$$\mathbb{Z}^s \times G \to (\mathcal{O}_K)^\times, \quad (a_1, \dots, a_s, g) \mapsto g \prod_{i=1}^{s} f_i^{a_i},$$

and it is easy to verify that these two morphisms are mutually inverse. □

To conclude the proof of Theorem 9.4.1, in view of Lemma 9.4.6, it will suffice to show that $L((\mathcal{O}_K)^\times) \subset W$ contains an $\mathbb{R}$-basis of W. Thus, we let $f\colon W \to \mathbb{R}$ be a nonzero $\mathbb{R}$-linear form, and find a unit $u \in (\mathcal{O}_K)^\times$ such that $f(L(u)) \neq 0$. Consider the projection

$$\pi\colon \mathbb{R}^{r+1} \to \mathbb{R}^r, \quad (y_1, \dots, y_{r+1}) \mapsto (y_1, \dots, y_r).$$

Then the formula (9.4.b) defining the hyperplane W shows that π induces an isomorphism $W \xrightarrow{\sim} \mathbb{R}^r$: the inverse is given by

$$(y_1, \dots, y_r) \mapsto \Big(y_1, \dots, y_r, -\frac{1}{2}\Big(\sum_{i=1}^{r_1} y_i + 2\sum_{i=r_1+1}^{r} y_i\Big)\Big)$$

In particular, there exist $c_1, \dots, c_r \in \mathbb{R}$ such that for all $y = (y_1, \dots, y_{r+1}) \in W \subset \mathbb{R}^{r+1}$, we have

$$f(y) = c_1 y_1 + \cdots + c_r y_r. \tag{9.4.c}$$

Let us now set

$$\alpha = \Big(\frac{2}{\pi}\Big)^{r_2}\sqrt{|d_K|} \in \mathbb{R}, \quad \text{and} \quad \beta = 1 + \Big(\sum_{i=1}^{r} |c_i|\Big)\log\alpha \in \mathbb{R}.$$

LEMMA 9.4.7. *For each family $\lambda = (\lambda_1, \dots, \lambda_r) \in \mathbb{R}^r$ such that $\lambda_i > 0$ for all $i \in \{1, \dots, r\}$, there exists a nonzero element $x_\lambda \in \mathcal{O}_K$ such that*

$$|\,\mathrm{N}_{K/\mathbb{Q}}(x_\lambda)| \leq \alpha \tag{9.4.d}$$

and

$$\Big|f(L(x_\lambda)) - \sum_{i=1}^{r} c_i \log\lambda_i\Big| < \beta \tag{9.4.e}$$

PROOF. Assume given a system $\lambda = (\lambda_1, \dots, \lambda_r) \in \mathbb{R}^r$. We define a real number $\lambda_{r+1} > 0$ by the requirement that

$$\prod_{i=1}^{r_1} \lambda_i \prod_{i=r_1+1}^{r+1} \lambda_i^2 = \alpha.$$

The subset $B \subset \mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$ consisting of those $(y_1, \dots, y_{r_1}, z_1, \dots, z_{r_2})$ such that

$$|y_i| \leq \lambda_i \text{ for } i = 1, \dots, r_1 \text{ and } |z_j| \leq \lambda_{r_1+j} \text{ for } j = 1, \dots, r_2$$

is compact, convex, and symmetric with respect to the origin. It is a product of r_1 intervals and r_2 disks, whose measure is

$$\mu(B) = \prod_{i=1}^{r_1} 2\lambda_i \prod_{i=1}^{r_2} \pi\lambda_{r_1+i}^2 = 2^{r_1}\pi^{r_2}\alpha = 2^{n-r_2}\sqrt{|d_K|}$$

It then follows form Corollary 9.1.3 that there exists a nonzero element $x_\lambda \in \mathcal{O}_K$ such that $\sigma(x_\lambda) \in B$. This means that

$$|\sigma_i(x_\lambda)| \leq \lambda_i \quad \text{for } i = 1, \dots, n,$$

where we write $\lambda_{j+r_2} = \lambda_j$ for $j = r_1 + 1, \dots, r_1 + r_2$. As x_λ is a nonzero element of $\mathcal{O}_K$, we have $\mathrm{N}_{K/\mathbb{Q}}(x_\lambda) \in \mathbb{Z} \smallsetminus \{0\}$ by Lemma 3.1.10 and Corollary 5.1.2. Thus, by the formula for the norm (see Proposition 4.3.3 and Proposition 4.2.5)

$$1 \leq |\,\mathrm{N}_{K/\mathbb{Q}}(x_\lambda)| = \prod_{i=1}^{n} |\sigma_i(x_\lambda)| \leq \prod_{i=1}^{n} \lambda_i = \prod_{i=1}^{r_1} \lambda_i \prod_{i=r_1+1}^{r+1} \lambda_i^2 = \alpha,$$

so that, for each $i \in \{1, \dots, n\}$

$$|\sigma_i(x_\lambda)| = |\,\mathrm{N}_{K/\mathbb{Q}}(x_\lambda)| \cdot \prod_{j\neq i} |\sigma_j(x_\lambda)|^{-1} \geq \prod_{j\neq i} \lambda_j^{-1} = \lambda_i\alpha^{-1}.$$

We have proved that $\lambda_i\alpha^{-1} \leq |\sigma_i(x_\lambda)| \leq \lambda_i$ for all $i \in \{1, \dots, n\}$, and thus

$$0 \leq \log\lambda_i - \log|\sigma_i(x_\lambda)| \leq \log\alpha. \tag{9.4.f}$$

Coming back to the expression (9.4.c), we have

$$\begin{aligned}\Big|f(L(x_\lambda)) - \sum_{i=1}^{r} c_i \log \lambda_i\Big| &= \Big|\sum_{i=1}^{r} c_i(\log|\sigma_i(x_\lambda)| - \log\lambda_i)\Big| \\ &\le \sum_{i=1}^{r} |c_i| \cdot \Big|\log|\sigma_i(x_\lambda)| - \log\lambda_i\Big| \\ &\le \Big(\sum_{i=1}^{r} |c_i|\Big)\log\alpha \qquad \text{by (9.4.f)} \\ &< \beta. \end{aligned}$$

□

For each $h \in \mathbb{N} \smallsetminus \{0\}$, let us pick real numbers $\lambda_{1,h}, \dots, \lambda_{r,h} > 0$ satisfying

$$\sum_{i=1}^{r} c_i \log \lambda_{i,h} = 2\beta h.$$

(This is possible because the linear form $f\colon W \to \mathbb{R}$ is nonzero, and thus surjective.) Let us set, for all $h \in \mathbb{N} \smallsetminus \{0\}$

$$\lambda(h) = (\lambda_{1,h}, \dots, \lambda_{r,h}) \in \mathbb{R}^r.$$

Lemma 9.4.8. *The real numbers $f(L(x_{\lambda(h)}))$ are pairwise distinct for $h \in \mathbb{N} \smallsetminus \{0\}$.*

Proof. The equation (9.4.e) yields

$$|f(L(x_{\lambda(h)})) - 2\beta h| < \beta$$

and therefore

$$(2h-1)\beta < f(L(x_{\lambda(h)})) < (2h+1)\beta,$$

from which the lemma follows. □

Now, for every $h \in \mathbb{N} \smallsetminus \{0\}$, we have by Proposition 6.4.1 and (9.4.d)

$$\mathrm{N}(x_{\lambda(h)}\mathcal{O}_K) = |\,\mathrm{N}_{K/\mathbb{Q}}(x_{\lambda(h)})| \le \alpha$$

so that by Lemma 9.3.4 the set of ideals in $\mathcal{O}_K$

$$\{x_{\lambda(h)}\mathcal{O}_K | h \in \mathbb{N} \smallsetminus \{0\}\}$$

is finite. We may thus find $h, k \in \mathbb{N} \smallsetminus \{0\}$ such that $h \neq k$ and $x_{\lambda(h)}\mathcal{O}_K = x_{\lambda(k)}\mathcal{O}_K$. This means that there exists a unit $u \in (\mathcal{O}_K)^\times$ such that $x_{\lambda(k)} = u x_{\lambda(h)}$. We then have

$$f(L(u)) = f(L(x_{\lambda(k)})) - f(L(x_{\lambda(h)})) \in \mathbb{R},$$

which is nonzero by Lemma 9.4.8. We have thus found an element $L(u) \in L((\mathcal{O}_K)^\times)$, satisfying $f(L(u)) \neq 0$, which completes the proof of Theorem 9.4.1 (cf. the discussion just below the proof of Lemma 9.4.6).

CHAPTER 10

Decomposition of prime ideals in extensions

1. Prime ideals under extensions

We fix a Dedekind domain A with fraction field K. We let L/K be a finite separable extension of degree $n = [L : K]$, and let B be the integral closure of A in L. We recall that B is a Dedekind domain (Theorem 6.1.6).

Let $\mathfrak{p}$ be a nonzero prime ideal of A. Then $B\mathfrak{p}$ is an ideal of the Dedekind domain B, hence by Theorem 6.3.5 we may write

$$B\mathfrak{p} = \prod_{i=1}^{r} \mathfrak{q}_i^{e_i} \tag{10.1.a}$$

where $\mathfrak{q}_1, \dots, \mathfrak{q}_r$ are maximal ideals of B, and $e_1, \dots, e_r \in \mathbb{N} \smallsetminus \{0\}$.

Definition 10.1.1. We say that a prime ideal $\mathfrak{q}$ of B *lies over* $\mathfrak{p}$ if $\mathfrak{q} \cap A = \mathfrak{p}$.

Lemma 10.1.2. *The prime ideals of $\mathcal{O}_K$ lying over $\mathfrak{p}$ are $\mathfrak{q}_1, \dots, \mathfrak{q}_r$. Those are precisely the prime ideals of B containing $\mathfrak{p}$.*

Proof. Let us first observe that $\mathfrak{p} = \mathfrak{q} \cap A \iff \mathfrak{p} \subset \mathfrak{q}$. The relation $\Rightarrow$ is clear; conversely if $\mathfrak{p} \subset \mathfrak{q}$, then $\mathfrak{p} \subset \mathfrak{q} \cap A$. As $\mathfrak{q} \cap A$ is a prime ideal (Lemma 1.1.2) which is nonzero (Lemma 2.1.19), and A a Dedekind domain, it follows that $\mathfrak{p} = \mathfrak{q} \cap A$. Therefore the prime ideals $\mathfrak{q}$ of B such that $\mathfrak{p} = \mathfrak{q} \cap A$ are precisely those containing $\mathfrak{p}B$. In view of the decomposition (10.1.a), those are precisely $\mathfrak{q}_1, \dots, \mathfrak{q}_r$ by Proposition 6.3.9 (ii). □

Definition 10.1.3. In the above situation, the integer e_i is called the *ramification index* of $\mathfrak{q}_i$ over A. The integer

$$f_i = [B/\mathfrak{q}_i : A/\mathfrak{p}]$$

is called the *residual degree* of $\mathfrak{q}_i$ over A. When $\mathfrak{q}$ is a prime ideal of B lying over $\mathfrak{p}$, there is by Lemma 10.1.2 a unique i such that $\mathfrak{q} = \mathfrak{q}_i$. We will then write $e_\mathfrak{q}, f_\mathfrak{q}$ instead of e_i, f_i.

The following observation will permit to "localise" at the prime ideal $\mathfrak{p}$:

Lemma 10.1.4. *In the above situation, let $S = A \smallsetminus \mathfrak{p}$. Then the natural ring morphisms*

$$A/\mathfrak{p} \to (S^{-1}A)/(S^{-1}\mathfrak{p}) \quad \textit{and} \quad B/\mathfrak{p}B \to (S^{-1}B)/(\mathfrak{p}S^{-1}B)$$

are isomorphisms.

Proof. The first isomorphism follows directly from Lemma 7.1.8, because $A/\mathfrak{p}$ is a field (recall that $\mathfrak{p}$ is a maximal ideal of A). So will the second one, if we prove that $\pi(S) \subset (B/\mathfrak{p}B)^\times$, where $\pi\colon B \to B/\mathfrak{p}B$ is the quotient map.

So let $s \in S$. If $\pi(s) \notin (B/\mathfrak{p}B)^\times$, then $\pi(s)$ is contained in some maximal ideal $\mathfrak{m}$ of $B/\mathfrak{p}B$ (Lemma 1.2.7). Let $\mathfrak{q} = \pi^{-1}\mathfrak{m}$. Since π is surjective, it induces a ring isomorphism $B/\mathfrak{q} \simeq A/\mathfrak{m}$, hence $B/\mathfrak{q}$ is a field, so that $\mathfrak{q}$ is a maximal ideal of B. In addition $\mathfrak{q} = \pi^{-1}\mathfrak{m}$ contains $\mathfrak{p} = \pi^{-1}\{0\}$, hence $\mathfrak{q}$ lies over $\mathfrak{p}$. The element s belongs to $\mathfrak{q}$ (since $s \in \mathfrak{m}$), hence $s \in \mathfrak{q} \cap A = \mathfrak{p}$ by Lemma 10.1.2, contradicting that fact that $s \in S = A \smallsetminus \mathfrak{p}$. □

Proposition 10.1.5. *In the situation above, we have an isomorphism of B-algebras*

$$B/B\mathfrak{p} \simeq \prod_{i=1}^{r} B/\mathfrak{q}_i^{e_i}.$$

Proof. Let $i \in \{1, \dots, r\}$. Let $\mathfrak{q}$ be a prime ideal of B containing $\mathfrak{q}_i^{e_i}$. If $x \in \mathfrak{q}_i$, then $x^{e_i} \in \mathfrak{q}$, hence $x \in \mathfrak{q}$ because the ideal $\mathfrak{q}$ of B is prime. Thus $\mathfrak{q}_i \subset \mathfrak{q}$, hence $\mathfrak{q}_i = \mathfrak{q}$ by maximality of $\mathfrak{q}_i$. Thus $\mathfrak{q}_i$ is the only prime ideal of B containing $\mathfrak{q}_i^{e_i}$. Since for $i \neq j$ we have $\mathfrak{q}_i \neq \mathfrak{q}_j$, it follows that $\mathfrak{q}_i^{e_i} + \mathfrak{q}_j^{e_j} = B$. Therefore, in view of (10.1.a), the statement follows from the Chinese remainder theorem (Lemma 1.1.5). □

We will need the following easy lemma:

Lemma 10.1.6. *Let R be a ring and I an ideal of R. If M is a free R-module of rank $n \in \mathbb{N}$, then M/IM is a free (R/I)-module of rank n.*

Proof. Let $(e_1, \dots, e_n)$ be an R-basis of M, and denote by $(f_1, \dots, f_n)$ its image in M/IM. Then the elements $f_1, \dots, f_n$ certainly generate the (R/I)-module M/IM. Assume that $\lambda_1, \dots, \lambda_n \in R/I$ are such that

$$\sum_{i=1}^{n} \lambda_i f_i = 0 \in M/IM.$$

Pick preimages $r_1, \dots, r_n \in R$ of $\lambda_1, \dots, \lambda_n \in R/I$. Then

$$\sum_{i=1}^{n} r_i e_i \in IM.$$

Now the group IM is generated by the sets $Ie_1, \dots, Ie_n$, hence we may find $y_1, \dots, y_n \in I$ such that

$$\sum_{i=1}^{n} r_i e_i = \sum_{i=1}^{n} y_i e_i \in M.$$

Since $(e_1, \dots, e_n)$ is an R-basis of M, it follows that $r_i = y_i$ for $i \in \{1, \dots, n\}$, and in particular $r_1, \dots, r_n \in I$, and finally $\lambda_1 = \cdots = \lambda_n = 0$. We have proved that the system $(f_1, \dots, f_n) \in (M/IM)^n$ is (R/I)-linearly independent. □

Lemma 10.1.7. *Let $\mathfrak{q}$ be a nonzero prime ideal of B, and $s \in \mathbb{N} \smallsetminus \{0\}$ such that $\mathfrak{p}B \subset \mathfrak{q}^s$. Then*

$$\dim_{A/\mathfrak{p}}(B/\mathfrak{q}^s) = s \cdot \dim_{A/\mathfrak{p}}(B/\mathfrak{q}).$$

Proof. Let us write $k = A/\mathfrak{p}$. We proceed by induction on s, the case $s = 1$ being clear. Assume that $s > 1$. Consider the k-vector space $V = B/\mathfrak{q}^s$ and its subspace $U = \mathfrak{q}^{s-1}/\mathfrak{q}^s$. Then $\dim_k V = \dim_k U + \dim_k(V/U)$. Observe that $V/U \simeq B/\mathfrak{q}^{s-1}$ as k-vector space, so that $\dim_k(V/U) = (s-1) \cdot \dim_k(B/\mathfrak{q})$ by the induction hypothesis. Thus

$$\dim_k(B/\mathfrak{q}^s) = \dim_k(\mathfrak{q}^{s-1}/\mathfrak{q}^s) + (s-1) \cdot \dim_k(B/\mathfrak{q}). \tag{10.1.b}$$

But $\dim_{B/\mathfrak{q}}(\mathfrak{q}^{s-1}/\mathfrak{q}^s) = 1$ by Proposition 6.3.10 (applied in the Dedekind domain B), hence $\dim_k(\mathfrak{q}^{s-1}/\mathfrak{q}^s) = \dim_k(B/\mathfrak{q})$. Therefore the formula (10.1.b) becomes $\dim_k(B/\mathfrak{q}^s) = s \cdot \dim_k(B/\mathfrak{q})$, as required. □

Theorem 10.1.8. *In the above situation, we have*

$$n = \dim_{A/\mathfrak{p}}(B/\mathfrak{p}B) = \sum_{i=1}^{r} e_i f_i.$$

Proof. Proposition 10.1.5 implies that

$$\dim_{A/\mathfrak{p}}(B/\mathfrak{p}B) = \sum_{i=1}^{r} \dim_{A/\mathfrak{p}}(B/\mathfrak{q}_i^{e_i}).$$

Now by Lemma 10.1.7, we have for any $i \in \{1, \dots, r\}$

$$\dim_{A/\mathfrak{p}}(B/\mathfrak{q}_i^{e_i}) = e_i \cdot \dim_{A/\mathfrak{p}}(B/\mathfrak{q}) = e_i f_i.$$

This proves the second equality.

To prove the first equality, let us localise at the multiplicative set $S = A \setminus \mathfrak{p}$. We set $A' = S^{-1}A = A_{\mathfrak{p}}$ and $\mathfrak{p}' = S^{-1}\mathfrak{p}$, as well as $B' = S^{-1}B$. Recall from Proposition 7.1.12 that A' is a Dedekind domain with fraction field K, and from Proposition 7.1.9 that B' is the integral closure of A' in L. The ring A' is local (Lemma 7.1.14), and a Dedekind domain, hence by Proposition 7.2.8 it is a principal ideal domain. Therefore by Corollary 5.1.6 the A'-module B' is free of rank n. As observed in Lemma 10.1.6, this implies that the $(A'/\mathfrak{p}')$-module $B'/\mathfrak{p}'B'$ is free of rank n. Thus

$$n = \dim_{A'/\mathfrak{p}'}(B'/\mathfrak{p}'B') = \sum_{i=1}^{r} e_i f_i. \tag{10.1.c}$$

Finally it follows from Lemma 10.1.4 that

$$\dim_{A/\mathfrak{p}}(B/\mathfrak{p}B) = \dim_{A'/\mathfrak{p}'}(B'/\mathfrak{p}B').$$ □

Remark 10.1.9. It follows from Theorem 10.1.8 that $r \geq 1$, so that $B\mathfrak{p}$ is contained in some prime ideal of B. This fact is in fact a consequence of the integrality of the extension $A \subset B$ alone (by the so-called "going-up" theorem).

2. Discriminant and ramification

In this section A is a Dedekind domain with fraction field K. We consider a finite separable field extension L/K of degree $n = [L : K]$, and let B be the integral closure of A in L.

Definition 10.2.1. We say that a nonzero prime ideal $\mathfrak{p}$ of A *does not ramify* in B if the $(A/\mathfrak{p})$-algebra $B/\mathfrak{p}B$ is étale. Otherwise, we say that $\mathfrak{p}$ *ramifies* in B. When $A = \mathbb{Z}$ and so L is a number field, we say that a prime number p ramifies (resp. does not ramify) in L if the ideal $p\mathbb{Z}$ ramifies (resp. does not ramifies) in $B = \mathcal{O}_L$.

Proposition 10.2.2. *A nonzero prime ideal $\mathfrak{p}$ of A does not ramify in B if and only if, for every prime ideal $\mathfrak{q}$ of B lying over $\mathfrak{p}$, the following two conditions are satisfied:*

(1) the field extension $A/\mathfrak{p} \subset B/\mathfrak{q}$ is separable,

(2) $e_{\mathfrak{q}} = 1$.

Proof. Recall from §10.1 that we have an isomorphism of B-algebras

$$B/\mathfrak{p}B \simeq (B/\mathfrak{q}_1^{e_1}) \times \cdots \times (B/\mathfrak{q}_r^{e_r}),$$

where $\mathfrak{q}_1, \ldots, \mathfrak{q}_r$ are the prime ideals $\mathfrak{q}$ of B lying over $\mathfrak{p}$. By Lemma 4.4.1, the prime $\mathfrak{p}$ does not ramify in B if and only if each $(A/\mathfrak{p})$-algebra $B/\mathfrak{q}_i^{e_i}$ is étale, for $i \in \{1, \ldots, r\}$.

So let us fix $i \in \{1, \ldots, r\}$. If $e_i \geq 2$, we may find by Corollary 6.3.3 and element $y \in \mathfrak{q}_i \smallsetminus (\mathfrak{q}_i^{e_i})$. Then the image of y in $B/\mathfrak{q}_i^{e_i}$ is nilpotent and nonzero, so that the ring $B/\mathfrak{q}_i^{e_i}$ is not reduced. Since an étale algebra is reduced (Theorem 4.4.6), we must have $e_i = 1$ when $\mathfrak{p}$ does not ramify in B. In addition $A/\mathfrak{p} \subset B/\mathfrak{q}_i$ is a field extension of finite degree f_i, which is separable if and only the $(A/\mathfrak{p})$-algebra $B/\mathfrak{q}_i$ is étale (Corollary 4.4.7). □

Corollary 10.2.3. *Let F/K be a finite separable field extension containing L/K as a subextension, and C the integral closure of A in F. Let $\mathfrak{p}$ be a nonzero prime ideal of A which does not ramify in C. Then $\mathfrak{p}$ does not ramify in B.*

Proof. It follows from Proposition 2.1.15 that C is the integral closure of B in L. Assume that $\mathfrak{q}$ is a prime ideal of B satisfying $\mathfrak{q} \cap A = \mathfrak{p}$. By Remark 10.1.9, there exists a prime ideal $\mathfrak{a}$ of C such that $\mathfrak{a} \cap B = \mathfrak{q}$. By assumption the field extension $A/\mathfrak{p} \subset C/\mathfrak{a}$ is separable, hence so is its subextension $A/\mathfrak{p} \subset B/\mathfrak{q}$. Moreover if e is the ramification index of $\mathfrak{q}$ over A, we have

$$C\mathfrak{p} = C(B\mathfrak{p}) \subset C(\mathfrak{q}^e) = (\mathfrak{q}C)^e \subset \mathfrak{a}^e,$$

which implies that $e = 1$, as $\mathfrak{p}$ does not ramify in C. □

Remark 10.2.4. Assume that L is a number field. Set $K = \mathbb{Q}$ and $A = \mathbb{Z}$, so that $B = \mathcal{O}_L$. Then any prime ideal $\mathfrak{p}$ of A is of the form $p\mathbb{Z}$ for a prime number p, and thus $A/\mathfrak{p}$ is the finite field with p elements. Therefore $A/\mathfrak{p}$ is perfect by Proposition 4.1.17, and thus the field extension $A/\mathfrak{p} \subset B/\mathfrak{q}$ is automatically separable. In conclusion, a prime number p ramifies in $\mathcal{O}_L$ if and only if for some prime ideal $\mathfrak{q}$ of $\mathcal{O}_L$ lying over $p\mathbb{Z}$ the ramification index $e_{\mathfrak{q}}$ is unequal to 1.

Definition 10.2.5. The *discriminant ideal* is the ideal $\mathfrak{D}_{B/A}$ of A generated by the discriminants $\mathrm{D}_{L/K}(x_1, \ldots, x_n)$ of the systems $(x_1, \ldots, x_n) \in B^n$ (recall that those belong to $A \subset K$ by Proposition 5.1.1).

Remark 10.2.6. It follows from Lemma 5.1.8 (iii) that this definition is compatible with the existing definition of the discriminant ideal $\mathfrak{D}_{B/A}$ given in Definition 3.2.3 when the A-module B is free of rank n.

Lemma 10.2.7. *The discriminant ideal $\mathfrak{D}_{B/A}$ is nonzero.*

Proof. Recall from Theorem 5.1.5 that B contains a K-basis $(e_1, \ldots, e_n)$ of L. Moreover, as the field extension L/K is separable we have $\mathfrak{D}_{L/K} \neq 0$ by Theorem 4.4.6 (and Proposition 4.2.5). Then by Proposition 3.2.5 we have $\mathrm{D}_{L/K}(e_1, \ldots, e_n) \neq 0$, so that $\mathfrak{D}_{B/A} \neq 0$. □

Lemma 10.2.8. *Let $S \subset A$ be a multiplicatively closed subset which does not contain zero. Then $S^{-1}\,\mathfrak{D}_{B/A} = \mathfrak{D}_{(S^{-1}B)/(S^{-1}A)}$.*

Proof. First observe that for any system $(u_1, \ldots, u_n) \in L^n$ and $\lambda \in K$, we have

$$\det(\mathrm{Tr}_{L/K}(\lambda u_i \cdot \lambda u_j)) = \lambda^{2n} \det(\mathrm{Tr}_{L/K}(u_i u_j)),$$

so that

$$\mathrm{D}_{L/K}(\lambda u_1, \dots, \lambda u_n) = \lambda^{2n} \mathrm{D}_{L/K}(u_1, \dots, u_n) \tag{10.2.a}$$

Consider now a system $(y_1, \dots, y_n) \in (S^{-1}B)^n$. Then we may find an element $s \in S$ such that $sy_i \in B$ for all $i \in \{1, \dots, n\}$. By (10.2.a) we have $s^{2n} \mathrm{D}_{L/K}(y_1, \dots, y_n) = \mathrm{D}_{L/K}(sy_1, \dots, sy_n)$, which belongs to A by Proposition 5.1.1, hence $\mathrm{D}_{L/K}(y_1, \dots, y_n)$ belongs to $S^{-1}A$. This proves that $\mathfrak{D}_{(S^{-1}B)/(S^{-1}A)} \subset S^{-1}\mathfrak{D}_{B/A}$.

Conversely, let $(x_1, \dots, x_n) \in B^n$ be a system, and $s \in S$. Then, by (10.2.a) we have

$$\frac{\mathrm{D}_{L/K}(x_1, \dots, x_n)}{s} = s^{2n-1} \mathrm{D}_{L/K}\Big(\frac{x_1}{s}, \dots, \frac{x_n}{s}\Big),$$

and this element belongs to $\mathfrak{D}_{(S^{-1}B)/(S^{-1}A)}$. Thus $S^{-1}\mathfrak{D}_{B/A} \subset \mathfrak{D}_{(S^{-1}B)/(S^{-1}A)}$. □

Lemma 10.2.9. *Assume that the A-module B is free of rank n. Let I be an ideal of A. Then the ideal $\mathfrak{D}_{(B/IB)/(A/I)}$ is the image of $\mathfrak{D}_{B/A}$ under the quotient map $A \to A/I$.*

Proof. Recall from Lemma 10.1.6 that the (A/I)-module B/IB is free of rank n. Consider a system $(b_1, \dots, b_n) \in B^n$, and its image $(c_1, \dots, c_n) \in (B/IB)^n$. Then the coefficients of the matrix $(\mathrm{Tr}_{(B/IB)/(A/I)}(c_i c_j)) \in M_n(A/I)$ are the images of those of the matrix $(\mathrm{Tr}_{B/A}(b_i b_j)) \in M_n(A)$. Taking determinants shows that $\mathrm{D}_{(B/IB)/(A/I)}(c_1, \dots, c_n) \in A/I$ is the image of $\mathrm{D}_{(B/IB)/(A/I)}(b_1, \dots, b_n) \in A$. Thus the ideal $\mathfrak{D}_{B/A}$ contains the image of $\mathfrak{D}_{(B/IB)/(A/I)}$. The other inclusion follows from the fact that any system in $(B/IB)^n$ is the image of some system in B^n. □

Theorem 10.2.10. *Let $\mathfrak{p}$ be a nonzero prime ideal of A. Then $\mathfrak{p}$ ramifies in B if and only if $\mathfrak{D}_{B/A} \subset \mathfrak{p}$.*

Proof. The subset $S = A \smallsetminus \mathfrak{p}$ of A (and thus also of B) is multiplicatively closed and does not contain zero. Set $A' = S^{-1}A$, $B' = S^{-1}B$, $\mathfrak{p}' = S^{-1}\mathfrak{p}$. Recall from Lemma 10.1.4 that we have natural isomorphisms

$$A/\mathfrak{p} \simeq A'/\mathfrak{p}' \quad \text{and} \quad B/\mathfrak{p}B \simeq B'/\mathfrak{p}'B'.$$

In addition $A' = A_{\mathfrak{p}}$ is principal ideal domain (Proposition 7.2.8), so that the A'-module B' is free of rank n (Corollary 5.1.6). Now by the characterisation of étale algebras given in Theorem 4.4.6, it follows that the prime ideal $\mathfrak{p}$ ramifies in B if and only if

$$\mathfrak{D}_{(B/\mathfrak{p}B)/(A/\mathfrak{p})} = \mathfrak{D}_{(B'/\mathfrak{p}'B')/(A'/\mathfrak{p}')} = 0,$$

which by Lemma 10.2.9 is equivalent to $\mathfrak{D}_{B'/A'} \subset \mathfrak{p}'$, which is in turn equivalent to $S^{-1}\mathfrak{D}_{B/A} \subset S^{-1}\mathfrak{p}$ by Lemma 10.2.8. But this last condition is equivalent to $\mathfrak{D}_{B/A} \subset \mathfrak{p}$ by Lemma 7.1.5. □

Remark 10.2.11. When $A = \mathbb{Z}$ and so L is a number field, recall from Proposition 3.2.5 that the ideal $\mathfrak{D}_{\mathcal{O}_L/\mathbb{Z}}$ is generated by the absolute discriminant d_L (see Definition 5.1.9). Thus it follows from Theorem 10.2.10 that the prime numbers ramifying in L are precisely the prime divisors of the absolute discriminant d_L. In particular, Hermite–Minkowski's Theorem 9.3.3 implies that there is always at least one prime number which ramifies in L, when $L \neq \mathbb{Q}$.

Corollary 10.2.12. *The set of nonzero prime ideals of A ramifying in B is finite.*

Proof. Since $\mathfrak{D}_{B/A} \neq 0$ by Lemma 10.2.7, the corollary follows from Theorem 10.2.10 and Remark 6.1.3. □

3. Cyclotomic fields

Let p be an odd prime number, and $\xi \in \mathbb{C}$ is a primitive p-th root of unity. Consider the cyclotomic field $K = \mathbb{Q}(\xi) \subset \mathbb{C}$, which is a number field of degree $p-1$ (see §5.3).

Proposition 10.3.1. *The only prime number which ramifies in K is p.*

Proof. Recall that p is assumed to be odd. The absolute discriminant of K is $(-1)^{p-1}p^{p-2}$ by Lemma 5.3.8, hence the statement follows from Theorem 10.2.10. □

Proposition 10.3.2. *The ideal $(1-\xi)\mathcal{O}_K$ is prime in $\mathcal{O}_K$, and*

$$p\mathcal{O}_K = \big((1-\xi)\mathcal{O}_K\big)^{p-1}.$$

Proof. Recall from Lemma 5.3.4 that $p\mathcal{O}_K = (1-\xi)\cdots(1-\xi^{p-1})\mathcal{O}_K$. For any $i \in \{1,\dots,p-1\}$, we have $(1-\xi^i) = (1-\xi)(1+\xi+\cdots+\xi^{i-1}) \in (1-\xi)\mathcal{O}_K$. It follows that $p\mathcal{O}_K \subset ((1-\xi)\mathcal{O}_K)^{p-1}$, so that

$$p\mathcal{O}_K = I \cdot \big((1-\xi)\mathcal{O}_K\big)^{p-1}, \tag{10.3.a}$$

where I is a nonzero ideal of the Dedekind domain $\mathcal{O}_K$. Recall from Lemma 6.3.4 that the nonzero ideal $(1-\xi)\mathcal{O}_K$ may be written as a product $\mathfrak{a}_1\cdots\mathfrak{a}_m$ where $\mathfrak{a}_1,\dots,\mathfrak{a}_m$ are prime ideals of $\mathcal{O}_K$ (possibly not pairwise distinct). Since $(1-\xi)\mathcal{O}_K \neq \mathcal{O}_K$ (for instance by Lemma 5.3.5), we have $m \geq 1$. On the other hand, the ideal $p\mathcal{O}_K$ is the product of at most $n = p-1$ prime ideals by Theorem 10.1.8. Writing I as a product of prime ideals of $\mathcal{O}_K$ (Lemma 6.3.4), we deduce from (10.3.a) and Theorem 6.3.5 that $m = 1$ and $I = 1$. We conclude that $(1-\xi)\mathcal{O}_K$ is a prime ideal of $\mathcal{O}_K$, and obtain the stated decomposition of the ideal $p\mathcal{O}_K$. □

Remark 10.3.3. With the notation of §10.1 for $A = \mathbb{Z}, B = \mathcal{O}_K$, and the prime ideal $\mathfrak{p} = p\mathbb{Z}$ of $\mathbb{Z}$, Proposition 10.3.2 asserts that $r = 1$ and $\mathfrak{q}_1 = (1-\xi)\mathcal{O}_K$, as well as $f = 1$ and $e = n = p-1$.

4. Quadratic fields

Let $K = \mathbb{Q}$ and L be a quadratic field. We consider a prime number $p \in \mathbb{N}$, and let $\mathfrak{p} = p\mathbb{Z}$ be the corresponding ideal of $\mathbb{Z}$. Then, in the notation of §10.1

$$\sum_{i=1}^{r} e_i f_i = n = 2,$$

and we are thus in one of the following situations,

(a) $p\mathcal{O}_L = \mathfrak{q}_1\mathfrak{q}_2$ with $\mathfrak{q}_1, \mathfrak{q}_2$ distinct primes of $\mathcal{O}_L$ ($r = 2, e_1 = e_2 = f_1 = f_2 = 1$),
(b) $p\mathcal{O}_L$ is a prime ideal of $\mathcal{O}_L$ ($r = 1, e_1 = 1, f_1 = 2$),
(c) $p\mathcal{O}_L = \mathfrak{q}^2$ for a prime ideal $\mathfrak{q}$ of $\mathcal{O}_L$ ($r = 1, e_1 = 2, f_1 = 1$).

Definition 10.4.1. According to the three cases distinguished above, we say that the prime number p

(a) *decomposes in $\mathcal{O}_L$*,
(b) *remains prime in $\mathcal{O}_L$*,
(c) *ramifies in $\mathcal{O}_L$*,

We will use the following explicit description of the ring $\mathcal{O}_L$:

Lemma 10.4.2. *Let $L = \mathbb{Q}(\sqrt{d})$ be a quadratic field, with $d \in \mathbb{Z}$ square-free. Consider the polynomial in $\mathbb{Z}[X]$*

$$Q = \begin{cases} X^2 - d & \text{if } d = 2, 3 \mod 4 \\ X^2 - X - \frac{d-1}{4} & \text{if } d = 1 \mod 4. \end{cases}$$

Then we have a ring isomorphism

$$\varphi\colon \mathbb{Z}[X]/Q \xrightarrow{\sim} \mathcal{O}_K, \quad X \mapsto \begin{cases} \sqrt{d} & \text{if } d = 2, 3 \mod 4 \\ \dfrac{1+\sqrt{d}}{2} & \text{if } d = 1 \mod 4. \end{cases}$$

Proof. Consider the element $\alpha \in \mathcal{O}_K$ defined by

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

Then a straightforward computation shows that $Q(\alpha) = 0$, so that the morphism φ is well-defined. Since $\mathcal{O}_K = \mathbb{Z}[\alpha]$ by Theorem 2.2.3, the morphism φ is surjective. Let $x \in \mathbb{Z}[X]/Q$ be the class of X. We claim that the $\mathbb{Z}$-module $\mathbb{Z}[X]/Q$ is generated by $1, x$. Indeed since the polynomial Q is monic of degree two, the element x^2 is a $\mathbb{Z}$-linear combination of $1, x$. By induction we deduce that, for $k \in \mathbb{N}$, the element x^k is a $\mathbb{Z}$-linear combination of $1, x$, which implies the claim (because $\mathbb{Z}[X]/Q$ is generated by the powers of x). Now for $a, b \in \mathbb{Z}$, the element $\varphi(a + bx) = a + b\alpha$ vanishes only when $a = b = 0$, because the family $(1, \alpha)$ is $\mathbb{Z}$-linearly independent by Theorem 2.2.3. It follows that φ is injective, hence bijective. □

Proposition 10.4.3. *Let $L = \mathbb{Q}(\sqrt{d})$ be a quadratic field, with $d \in \mathbb{Z}$ square-free. Let $p \in \mathbb{N}$ be an odd prime number. Then:*

(i) p decomposes in $\mathcal{O}_L$ if p does not divide d, and d is a square modulo p,
(ii) p remains prime in $\mathcal{O}_L$ if d is not a square modulo p,
(iii) p ramifies in $\mathcal{O}_L$ if p divides d.

Proof. We claim that

$$\mathcal{O}_L/p\mathcal{O}_L \simeq \mathbb{F}_p[X]/(X^2 - d). \tag{10.4.a}$$

This is clear from Lemma 10.4.2 when $d = 2, 3 \mod 4$. If $d = 1 \mod 4$, the ring morphism

$$\rho\colon \mathbb{F}_p[X] \to \mathbb{F}_p[X], \quad X \mapsto 2X - 1$$

is an isomorphism (its inverse is given by $X \mapsto \frac{1-p}{2}(X + 1)$). Then

$$\rho(X^2 - d) = (2X - 1)^2 - d = 4\Big(X^2 - X - \frac{d-1}{4}\Big)$$

hence by Lemma 10.4.2 (as 4 is invertible in $\mathbb{F}_p$)

$$\mathcal{O}_L/p\mathcal{O}_L \simeq \mathbb{F}_p[X]/\Big(X^2 - X - \frac{d-1}{4}\Big) \simeq \mathbb{F}_p[X]/(\rho(X^2 - d)) \simeq \mathbb{F}_p[X]/(X^2 - d),$$

proving (10.4.a) in this case also.

In any case, the polynomial $X^2 - d \in \mathbb{F}_p[X]$ is the product of two distinct monic irreducible factors when $d \in \mathbb{F}_p$ is a nonzero square, irreducible when $d \in \mathbb{F}_p$ is not a square, and the square of an irreducible polynomial when $d \in \mathbb{F}_p$ is zero. In view of (10.4.a), this means that the ideal $p\mathcal{O}_L$ in $\mathcal{O}_L$ is a product of two distinct prime ideals

when $d \in \mathbb{F}_p$ is a nonzero square, a prime ideal when $d \in \mathbb{F}_p$ is not a square, and the square of a prime ideal when $d \in \mathbb{F}_p$ is zero. □

Proposition 10.4.4. *Let $L = \mathbb{Q}(\sqrt{d})$ be a quadratic field, with $d \in \mathbb{Z}$ square-free. Then:*

(i) 2 *decomposes in* $\mathcal{O}_L$ *if* d *is congruent to* 1 *modulo* 8,
(ii) 2 *remains prime in* $\mathcal{O}_L$ *if* d *is congruent to* 5 *modulo* 8,
(iii) 2 *ramifies in* $\mathcal{O}_L$ *if* d *is congruent to* 2 *or* 3 *modulo* 4.

Proof. If $d = 2, 3 \mod 4$, then by Lemma 10.4.2 we have a ring isomorphism

$$\mathcal{O}_L/2\mathcal{O}_L \simeq \mathbb{F}_2[X]/(X^2 - d).$$

The image of d in $\mathbb{F}_2$ is 0 or 1, and in particular is always a square. It follows $2\mathcal{O}_L$ is the square of a prime ideal in $\mathcal{O}_L$, hence 2 ramifies in $\mathcal{O}_L$ in this case.

Assume that $d = 1 \mod 4$. We have by Lemma 10.4.2

$$\mathcal{O}_L/2\mathcal{O}_L \simeq \mathbb{F}_2[X]/(X^2 - X - \delta),$$

where $\delta \in \mathbb{F}_2$ is the class of $(d-1)/4$, that is,

$$\delta = \begin{cases} 0 \in \mathbb{F}_2 & \text{if } d = 1 \mod 8, \\ 1 \in \mathbb{F}_2 & \text{if } d = 5 \mod 8. \end{cases}$$

If $d = 1 \mod 8$, then the polynomial $X^2 - X - \delta = X^2 - X - 1$ has no root in $\mathbb{F}_2$ (it takes the constant value 1 on $\mathbb{F}_2$), and this implies that the ring $\mathcal{O}/2\mathcal{O}_L$ is field, which means that 2 remains prime in $\mathcal{O}_L$. If $d = 5 \mod 8$, then $X^2 - X - \delta = X^2 - X = X(X-1) \in \mathbb{F}_2[X]$ is a product of two distinct monic irreducible polynomials, which implies that 2 decomposes in $\mathcal{O}_L$. □

CHAPTER 11

Galois extensions of number fields

1. Galois theory

When A is a k-algebra, we denote by $\mathrm{Aut}_{k-\mathrm{alg}}(A)$ the group of isomorphisms of k-algebras $A \to A$. When X is a set with an action of a group G, we denote by X^G the set of elements of X fixed by every element of G.

PROPOSITION 11.1.1. *Let L/k be a field extension of finite degree. Let G be a subgroup of $\mathrm{Aut}_{k-\mathrm{alg}}(L)$ such that $L^G = k$. Then $G = \mathrm{Aut}_{k-\mathrm{alg}}(L)$ and $\mathrm{card}(G) = [L : k]$.*

PROOF. We have $[L : k] \geq \mathrm{card}(\mathrm{Aut}_{k-\mathrm{alg}}(L))$ by Dedekind's Lemma 4.2.1. In particular the group $\mathrm{Aut}_{k-\mathrm{alg}}(L)$ (hence also its subgroup G) is finite, and it will suffice to prove that $\mathrm{card}(G) \geq [L : k]$. Let M be the set of maps $G \to L$, viewed as an L-algebra via pointwise operations. Consider the morphism of k-algebras

$$L \to M, \quad x \mapsto (g \mapsto g(x)).$$

By the universal property of the tensor product (see §4.3), this extends uniquely to a morphism of L-algebras

$$\varphi \colon L \otimes_k L \to M,$$

which maps $x \otimes y$ to the map $g \mapsto g(x)y$; here and below we view $L \otimes_k L$ as an L-vector space via the second factor.

We are going to show that φ is injective. Assume that the kernel of φ contains a nonzero element

$$v = x_1 \otimes y_1 + \cdots + x_r \otimes y_r, \text{ where } x_1, \ldots, x_r, y_1, \ldots, y_r \in L.$$

Choose r minimal with this property. Observe that then y_1 is nonzero. Replacing v with $(1 \otimes y_1^{-1})v$ (which still belongs to the L-subspace $\ker \varphi$), we may assume that $y_1 = 1$. In particular $y_1 \in k \subset L$.

We claim that the elements $x_1, \ldots, x_r \in L$ are k-linearly independent: indeed assume that

$$\lambda_1 x_1 + \cdots + \lambda_r x_r = 0, \quad \text{with } \lambda_1, \ldots, \lambda_r \in k,$$

and that $s \in \{1, \ldots, r\}$ is such that $\lambda_s \neq 0$. For ease of notation, after renaming the x_i's, we may assume that $s = r$. Then $x_r = -\lambda_r^{-1}(\lambda_1 x_1 + \cdots + \lambda_{r-1} x_{r-1})$, and so

$$v = \sum_{i=1}^{r-1} x_i \otimes y_i + \sum_{i=1}^{r-1} (-\lambda_r^{-1}\lambda_i x_i) \otimes y_r = \sum_{i=1}^{r-1} x_i \otimes (y_i - \lambda_i \lambda_r^{-1} y_r),$$

which contradicts the minimality of r. The claim is proved.

As $v \in \ker \varphi$, we have

$$0 = \varphi(v)(\mathrm{id}_L) = x_1 y_1 + \cdots + x_r y_r.$$

Since the elements $x_1, \dots, x_r$ are k-linearly independent, it follows that there exists $j \in \{2, \dots, r\}$ such that $y_j \in L$ does not lie in k (recall that $y_1 \in k$). As $k = L^G$, we may thus find $\gamma \in G$ such that $\gamma(y_j) \neq y_j$. Consider the element

$$w = x_1 \otimes \gamma(y_1) + \cdots + x_r \otimes \gamma(x_r) \in L \otimes_k L.$$

Then for any $g \in G$, we have

$$\begin{aligned}\varphi(w)(g) &= g(x_1)\gamma(y_1) + \cdots + g(x_r)\gamma(y_r) \\ &= \gamma\big(\gamma^{-1} \circ g(x_1)y_1 + \cdots + \gamma^{-1} \circ g(x_r)y_r\big) \\ &= \gamma\big(\varphi(v)(\gamma^{-1}g)\big) \\ &= 0,\end{aligned}$$

where the last equality follows from the fact that $\varphi(v) = 0$. This proves that $w \in \ker \varphi$, hence $v - w \in \ker \varphi$. Since $y_1 \in k$ we have $\gamma(y_1) = y_1$, and thus

$$v - w = \sum_{i=1}^{r} x_i \otimes y_i - \sum_{i=1}^{r} x_i \otimes \gamma(y_i) = \sum_{i=2}^{r} x_i \otimes (y_i - \gamma(y_i)) \in L \otimes_k L. \tag{11.1.a}$$

Since the elements $x_1, \dots, x_r \in L$ are k-linearly independent, it follows that the elements $x_1 \otimes 1, \dots, x_r \otimes 1 \in L \otimes_k L$ are L-linearly independent (exercise). Therefore the quantity appearing in (11.1.a) is nonzero (recall that $\gamma(y_j) - y_j \neq 0$) and belongs to $\ker \varphi$, a contradiction with the minimality of r. This proves that the L-linear map φ is injective, so that

$$[L : k] = \dim_L(L \otimes_k L) \leq \dim_L M = \operatorname{card}(G),$$

as required. □

Remark 11.1.2. In the conditions of Proposition 11.1.1 we have $L \otimes_k L \simeq L^n$ as L-algebras, where $n = [L : k]$. Indeed the morphism φ appearing in the proof of Proposition 11.1.1 must be surjective by dimensional reasons, and $M \simeq L^n$ as L-algebras.

Proposition 11.1.3. *Let L/k be a field extension of finite degree. The following are equivalent:*

(i) The minimal polynomial over k of every element of L splits into a product of linear factors in $L[X]$.
(ii) The k-algebra L is generated by elements whose minimal polynomials over k split into a product of linear factors in $L[X]$.
(iii) Let F/k a field extension. Then all morphisms of k-algebras $L \to F$ have the same image.

Proof. (i) ⇒ (ii): Clear.

(ii) ⇒ (iii): Consider a set of generators $\mathcal{G} \subset L$ of the k-algebra L, such that the minimal polynomial over k every element of $\mathcal{G}$ splits into a product of linear factors in $L[X]$. Let $\mathcal{P} \subset k[X]$ be the set of minimal polynomials over k of the elements of $\mathcal{G}$, and $\mathcal{R} \subset F$ the set of roots of the elements of $\mathcal{P}$. Let $E \subset F$ be the k-subalgebra generated by $\mathcal{R}$. We prove that E is the common image. Let $\sigma\colon L \to F$ be a morphism of k-algebras. If $x \in \mathcal{G}$, then $\sigma(x) \in F$ is a root of the minimal polynomial of x over k, hence $\sigma(x) \in \mathcal{R} \subset E$. Since $\mathcal{G}$ generates the k-algebra L, it follows that $\sigma(L) \subset E$. Conversely,

let $y \in \mathcal{R}$, and pick $P \in \mathcal{P}$ such that $P(y) = 0$. By the definition of $\mathcal{P}$, we may find elements $x_1, \dots, x_n \in L$ such that $P = (X - x_1) \cdots (X - x_n)$ in $L[X]$, hence

$$0 = \sigma(P(y)) = (\sigma(P))(y) = (y - \sigma(x_1)) \cdots (y - \sigma(x_n)) \in F,$$

so that $y = \sigma(x_i)$ for some $i \in \{1, \dots, n\}$. Therefore $\mathcal{R} \subset \sigma(L)$, and thus $E \subset \sigma(L)$.

(iii) $\Rightarrow$ (i): Consider an element $x \in L$ and its minimal polynomial $P \in k[X]$ over k. Let E/k be a field extension such that P splits into a product of linear factors in $E[X]$ (such exists by Proposition 4.1.8), so that

$$P = \prod_{i=1}^{n} (X - \alpha_i) \in E[X], \quad \text{with } \alpha_1, \dots, \alpha_n \in E.$$

Note that $n \geq 1$. Recall that the k-algebra $K = k[x] \subset L$ is isomorphic to $k[X]/P$, and is a field. For each $i \in \{1, \dots, n\}$, we may thus define a morphism of k-algebras $\sigma_i \colon K \to E$ by $x \mapsto \alpha_i$. By Proposition 4.1.9, we find for each $i \in \{1, \dots, n\}$ a finite field extension F_i/E and a morphism of k-algebras $L \to F_i$ extending σ_i. By Corollary 4.1.10, we may find a finite field extension F/E containing each F_i/E as subextension, for $i \in \{1, \dots, n\}$. Let $i \in \{1, \dots, n\}$. Denoting by $\tau_i \colon L \xrightarrow{\sigma_i} F_i \subset F$ the composite, we have $\tau_i(x) = \sigma_i(x) = \alpha_i$ in F. Since $\tau_1(L) = \tau_i(L) \subset F$ by (iii), we may find $x_i \in L$ such that $\alpha_i = \tau_1(x_i)$. Consider now the polynomial

$$Q = \prod_{i=1}^{n} (X - x_i) \in L[X].$$

Then $\tau_1(Q) = P = \tau_1(P)$ in $F[X]$. Since τ_1 is injective, it follows that $P = Q \in L[X]$, and thus P splits into a product of linear factors in $L[X]$. □

Definition 11.1.4. A field extension L/k of finite degree is called *normal* if it satisfies the conditions of Proposition 11.1.3.

Proposition 11.1.5. *Let F/k be a field extension of finite degree. The following are equivalent:*

(i) The extension F/k is separable and normal,
(ii) $F^{\mathrm{Aut}_{k-\mathrm{alg}}(F)} = k$.

Proof. (i) $\Rightarrow$ (ii) : Let $x \in F \smallsetminus k$, and $P \in k[X]$ the minimal polynomial of x over k. The polynomial P splits into a product of linear factors over F (as F/k is normal), and has no multiple root (as F/k separable). Since P has degree at least two (as $x \notin k$), we find $y \in F$ such that $y \neq x$ and $P(y) = 0$. Let K be the subfield of F generated by x over k. The morphism of k-algebras $k[X]/P \to K$ given by $X \mapsto x$ is an isomorphism, hence we can define a morphism of k-algebras $K \to F$ by $x \mapsto y$. That morphism extends to a morphism of k-algebras $\sigma' \colon F \to F'$, where F'/F is a field extension by Proposition 4.1.9. By Proposition 11.1.3, the image of σ' coincides with the image of the inclusion $F \subset F'$, so that $\sigma'(F) = F \subset F'$. The morphism σ' therefore induces a surjective morphism of k-algebras $\sigma \colon F \to F$. As σ is injective (since F is a field) we have found $\sigma \in \mathrm{Aut}_{k-\mathrm{alg}}(F)$ such that $\sigma(x) = y \neq x$, proving (ii).

(ii) $\Rightarrow$ (i) : Let $x \in F$. Let $S \subset F$ be the set of those elements $\sigma(x) \in F$, where σ runs over $\mathrm{Aut}_{k-\mathrm{alg}}(F)$. The elements of S are among the roots of the minimal polynomial

of x over k, and in particular the set S is finite (alternatively, we know that the group $\mathrm{Aut}_{k-\mathrm{alg}}(F)$ is finite by Proposition 11.1.1). Consider the polynomial

$$P = \prod_{s \in S} (X - s) \in F[X]. \tag{11.1.b}$$

Every automorphism $\sigma \in \mathrm{Aut}_{k-\mathrm{alg}}(F)$ permutes the elements of S, so that

$$\sigma(P) = \prod_{s \in S} (X - \sigma(s)) = \prod_{s \in S} (X - s) = P.$$

Thus $P = (F[X])^{\mathrm{Aut}_{k-\mathrm{alg}}(F)} = (F^{\mathrm{Aut}_{k-\mathrm{alg}}(F)})[X] = k[X]$. Since $P(x) = 0$, the minimal polynomial of x over k divides P, hence splits into a product of pairwise distinct monic linear factors in $F[X]$, because P does so by (11.1.b). □

Definition 11.1.6. A finite field extension F/k is called *Galois* if it satisfies the conditions of Proposition 11.1.5. Its *Galois group* $\mathrm{Gal}(F/k)$ is defined as the group $\mathrm{Aut}_{k-\mathrm{alg}}(F)$.

Lemma 11.1.7. *Let F/k be a Galois extension. Then* $\mathrm{card}(\mathrm{Gal}(F/k)) = [F : k]$.

Proof. This follows from Proposition 11.1.1. □

Lemma 11.1.8. *If F/k is a Galois extension and E/k a subextension of F/k, then the extension F/E is Galois.*

Proof. Let $x \in F$, and $P \in k[X]$, resp. $Q \in E[X]$, be the minimal polynomial of x over k, resp. E. As $P \in E[X]$ is such that $P(x) = 0$, it follows that Q divides P in $F[X]$, hence Q splits into a product of pairwise distinct monic linear factors in $F[X]$, because P does so. □

Theorem 11.1.9. *Let F/k be a Galois field extension of finite degree.*

(i) The associations

$$E/k \mapsto \mathrm{Gal}(F/E) \quad ; \quad H \mapsto F^H$$

yield inclusion-reversing, mutually inverse bijections between subextensions E/k of F/k and subgroups H of $\mathrm{Gal}(F/k)$.

(ii) A subextension E/k of F/k is Galois if and only if the subgroup $\mathrm{Gal}(F/E)$ *is normal in* $\mathrm{Gal}(F/k)$. *In this case, restricting automorphisms induces a group isomorphism*

$$\mathrm{Gal}(F/k)/\mathrm{Gal}(F/E) \simeq \mathrm{Gal}(E/k).$$

Proof. (i): Let E/k be a subextension of F/k. Then the field extension F/E is Galois (Lemma 11.1.8), so that $F^{\mathrm{Gal}(F/E)} = E$. Conversely let $H \subset \mathrm{Gal}(F/k)$ be a subgroup. Certainly we have $H \subset \mathrm{Gal}(F/F^H)$. Then it follows from Proposition 11.1.1 applied to the extension F/F^H and the subgroup $H \subset \mathrm{Gal}(F/F^H)$ that $H = \mathrm{Gal}(F/F^H)$.

(ii): First, let H be a normal subgroup of $\mathrm{Gal}(F/k)$, and $E = F^H$. Let $x \in E$. Then for any $\sigma \in \mathrm{Gal}(F/k)$ and $h \in H$, the automorphism $\sigma^{-1} \circ h \circ \sigma \in \mathrm{Gal}(F/k)$ belongs to H, hence fixes x. Therefore

$$h \circ \sigma(x) = \sigma \circ \sigma^{-1} \circ h \circ \sigma(x) = \sigma(x),$$

proving that $\sigma(x) \in F^H = E$. Thus the subfield $E \subset F$ is stable under the action of $\mathrm{Gal}(F/k)$, so that $E^{\mathrm{Aut}_{k-\mathrm{alg}}(E)} \subset F^{\mathrm{Gal}(F/k)} = k$. It follows that the extension E/k is Galois (Proposition 11.1.5).

Let now E/k be a subextension of F/k, and assume that E/k is Galois. Then E/k is normal by Proposition 11.1.5, hence every element of $\mathrm{Gal}(F/k)$ maps the subfield $E \subset F$ onto itself by Proposition 11.1.3. This permits to define a group morphism

$$\alpha\colon \mathrm{Gal}(F/k) \to \mathrm{Aut}_{k-\mathrm{alg}}(E), \quad \sigma \mapsto \sigma|_E.$$

Since $\mathrm{Gal}(F/E) = \ker \alpha$, the subgroup $\mathrm{Gal}(F/E)$ is normal in $\mathrm{Gal}(F/k)$. In addition, the morphism α induces an injective morphism

$$\mathrm{Gal}(F/k)/\mathrm{Gal}(F/E) \to \mathrm{Gal}(E/k),$$

which must also be surjective, because, by Lemma 11.1.7

$$\mathrm{card}(\mathrm{Gal}(F/k)/\mathrm{Gal}(F/E)) = [F:k]/[F:E] = [E:k] = \mathrm{card}(\mathrm{Gal}(E/k)). \qquad \square$$

Example 11.1.10 (Finite fields). Let k be a finite field, and set $q = \mathrm{card}(k) \in \mathbb{N}$. Let L/k be an extension of degree n. Then $\mathrm{card}(L) = q^n$. The Frobenius map

$$\phi\colon L \to L, \quad x \mapsto x^q \tag{11.1.c}$$

is a ring morphism (see (4.1.b)). It is injective (as L is a domain), hence surjective by a cardinality argument. Since $k^\times$ is a group of order $q-1$, we have $\phi(x) = x$ for all $x \in k^\times$. This also holds when $x = 0$. Therefore every element of k is a root of the polynomial $X^q - X \in L[X]$, and by degree reasons there are no other roots. We have proved that

$$k = \{x \in L | \phi(x) = x\}. \tag{11.1.d}$$

In particular $\phi \in \mathrm{Aut}_{k-\mathrm{alg}}(L)$. Let G be the subgroup of $\mathrm{Aut}_{k-\mathrm{alg}}(L)$ generated by ϕ. Now it follows from (11.1.d) that $L^G = k$, so that $G = \mathrm{Aut}_k(L)$ and $\mathrm{card}(G) = n$ by Proposition 11.1.1.

In conclusion, the extension L/k is Galois, and its Galois group $\mathrm{Gal}(L/k)$ is cyclic of order $n = [L:k]$, generated by the Frobenius automorphism ϕ of (11.1.c).

2. Decomposition and inertia groups

In this section A is a Dedekind domain with fraction field K, and L/K is a finite Galois extension. We let $n = [L:K]$ and $G = \mathrm{Gal}(L/K)$. We denote by B the integral closure of A in L.

Lemma 11.2.1. *Every $\sigma \in G$ restricts to a ring isomorphism $\sigma_B\colon B \xrightarrow{\sim} B$.*

Proof. It follows from Lemma 2.1.17 that $\sigma(B) \subset B$. Therefore $\sigma\colon L \to L$ induces a ring morphism $\sigma_B\colon B \to B$. For the same reason $\sigma^{-1}\colon L \to L$ induces a ring morphism $\sigma_B^{-1}\colon B \to B$. Since $\sigma_B \circ \sigma_B^{-1} = \mathrm{id}_B = \sigma_B^{-1} \circ \sigma_B$, the lemma follows. $\square$

It follows from Lemma 11.2.1 that the group G acts on the set of prime ideals of B.

Proposition 11.2.2. *Let $\mathfrak{p}$ be a nonzero prime ideal of A. The group G acts transitively on the set of prime ideals of B lying over $\mathfrak{p}$.*

Proof. Let $\sigma \in G$. Let $\mathfrak{q}$ be a prime ideal of B lying over A. Then $\sigma(\mathfrak{q})$ is a prime ideal of B (because σ induces a ring isomorphism $B/\mathfrak{q} \simeq B/\sigma(\mathfrak{q})$), and

$$\sigma(\mathfrak{q}) \cap A = \sigma(\mathfrak{q}) \cap \sigma(A) = \sigma(\mathfrak{q} \cap A) = \sigma(\mathfrak{p}) = \mathfrak{p}.$$

Let now $\mathfrak{q}, \mathfrak{q}'$ be prime ideals of B lying over $\mathfrak{p}$. We assume that $\sigma(\mathfrak{q}) \neq \mathfrak{q}'$ for all $\sigma \in G$, and come to a contradiction. As the prime ideal $\mathfrak{q}'$ is nonzero (Lemma 2.1.19) in the

Dedekind domain B, it is a maximal ideal. Therefore $\mathfrak{q}' \not\subset \sigma(\mathfrak{q})$ for all $\sigma \in G$. By prime avoidance (Lemma 1.1.4), we find an element $x \in \mathfrak{q}'$ such that $x \notin \sigma(\mathfrak{q})$ for all $\sigma \in G$ (recall that G is finite). Consider the element (Proposition 4.3.3)

$$\mathrm{N}_{L/K}(x) = \prod_{\sigma \in G} \sigma(x) \in K.$$

As observed above, we have $\sigma(x) \in B$ for all $\sigma \in G$. It follows that $\mathrm{N}_{L/K}(x) \in xB \subset \mathfrak{q}'$. As $\mathrm{N}_{L/K}(x) \in A$ by Corollary 5.1.2, we have $\mathrm{N}_{L/K}(x) \in \mathfrak{q}' \cap A = \mathfrak{p}$. In particular

$$\prod_{\sigma \in G} \sigma(x) = \mathrm{N}_{L/K}(x) \in \mathfrak{q},$$

and as the ideal $\mathfrak{q}$ is prime in B, there exists an element $\sigma \in G$ such that $\sigma(x) \in \mathfrak{q}$. Then $x \in \sigma^{-1}(\mathfrak{q})$, a contradiction with the choice of the element x. □

Corollary 11.2.3. *Let $\mathfrak{p}$ be a nonzero prime ideal of A. Let $\mathfrak{q}_1, \dots, \mathfrak{q}_g$ be the prime ideals of B lying over $\mathfrak{p}$. Then*

$$B\mathfrak{p} = \Big(\prod_{i=1}^{g} \mathfrak{q}_i\Big)^e \quad \textit{and} \quad n = efg,$$

where

$$f = [(B/\mathfrak{q}_1) : (A/\mathfrak{p})] = \cdots = [(B/\mathfrak{q}_g) : (A/\mathfrak{p})].$$

Proof. Recall from (10.1.a) (setting $r = g$) that we may write

$$B\mathfrak{p} = \prod_{i=1}^{g} \mathfrak{q}_i^{e_i}.$$

Let $j, k \in \{1, \dots, g\}$. By Proposition 11.2.2 there exists $\sigma \in G$ such that $\mathfrak{q}_j = \sigma(\mathfrak{q}_k)$. We have $\sigma(B\mathfrak{p}) = B\mathfrak{p}$, and thus

$$B\mathfrak{p} = \prod_{i=1}^{g} \sigma(\mathfrak{q}_i)^{e_i}.$$

Observe that $\sigma(\mathfrak{q}_1), \dots, \sigma(\mathfrak{q}_g)$ are pairwise distinct nonzero prime ideals of B, hence the unicity in the decomposition of Theorem 6.3.5, together with the fact that $\sigma(\mathfrak{q}_k) = \mathfrak{q}_j$, implies that $e_k = e_j$. We may thus set $e = e_1 = \cdots = e_g$ to obtain the stated decomposition of the ideal $B\mathfrak{p}$ in B.

In addition, the induced isomorphism of A-modules $\sigma_B \colon B \xrightarrow{\sim} B$ descends to an isomorphism of $(A/\mathfrak{p})$-vector spaces $B/\mathfrak{q}_k \xrightarrow{\sim} B/\mathfrak{q}_j$ (its inverse is induced by $(\sigma^{-1})_B$). This proves that $[(B/\mathfrak{q}_k) : (A/\mathfrak{p})] = [(B/\mathfrak{q}_j) : (A/\mathfrak{p})]$, hence

$$[(B/\mathfrak{q}_1) : (A/\mathfrak{p})] = \cdots = [(B/\mathfrak{q}_g) : (A/\mathfrak{p})],$$

and the formula $n = efg$ follows from Theorem 10.1.8. □

Definition 11.2.4. For a nonzero prime ideal $\mathfrak{q}$ of B, the subgroup of $\mathrm{Gal}(L/K)$ consisting of those σ such that $\sigma(\mathfrak{q}) = \mathfrak{q}$ is called the *decomposition group of* $\mathfrak{q}$, and is denoted by $D_{\mathfrak{q}}$.

Remark 11.2.5. Let $\mathfrak{q}$ of B be a nonzero prime ideal $\mathfrak{q}$ of B. Then an element $\sigma \in \mathrm{Gal}(L/K)$ belongs to $D_{\mathfrak{q}}$ as soon as $\sigma(\mathfrak{q}) \subset \mathfrak{q}$. Indeed $\sigma(\mathfrak{q})$ is a nonzero prime ideal of $\mathcal{O}_K$ by Lemma 11.2.1, hence a maximal ideal because B is a Dedekind domain. Thus $\sigma(\mathfrak{q}) = \mathfrak{q}$ as soon as $\sigma(\mathfrak{q}) \subset \mathfrak{q}$.

For the rest of this section, we fix a nonzero prime ideal $\mathfrak{q}$ of B, and set $\mathfrak{p} = \mathfrak{q} \cap A$. Then $\mathfrak{q}$ lies over $\mathfrak{p}$.

Lemma 11.2.6. *In the notation of Corollary 11.2.3, we have*

$$\mathrm{card}(D_{\mathfrak{q}}) = ef.$$

Proof. The group G acts transitively on the set $\{\mathfrak{q}_1, \dots, \mathfrak{q}_g\}$ of cardinality g, and $D_{\mathfrak{q}}$ is the stabilisator of some element in this set. This implies that

$$\mathrm{card}(D_{\mathfrak{q}}) \cdot g = \mathrm{card}(G).$$

But $\mathrm{card}(G) = n$ (see Lemma 11.1.7), and $n = efg$ by Corollary 11.2.3. The lemma follows. □

Every element $\sigma \in D_{\mathfrak{q}}$ induces an automorphism $\overline{\sigma}$ of the $(A/\mathfrak{p})$-algebra $B/\mathfrak{q}$, which allows us to define a group morphism

$$D_{\mathfrak{q}} \to \mathrm{Aut}_{(A/\mathfrak{p})-\mathrm{alg}}(B/\mathfrak{q}), \quad \sigma \mapsto \overline{\sigma}. \tag{11.2.a}$$

Definition 11.2.7. The kernel of the morphism (11.2.a) is called the *inertia group of* $\mathfrak{q}$, and is denoted by $I_{\mathfrak{q}} \subset D_{\mathfrak{q}}$.

Let us set $k = A/\mathfrak{p}$ and $\ell = B/\mathfrak{q}$.

Proposition 11.2.8. *The following hold:*

(i) The field extension ℓ/k is normal.

(ii) Assume that the field extension ℓ/k is separable. Then (11.2.a) *induces a surjective group morphism*

$$D_{\mathfrak{q}} \to \mathrm{Gal}(\ell/k),$$

whose kernel is $I_{\mathfrak{q}}$.

Proof. Let us set $K' = L^{D_{\mathfrak{q}}} \subset L$. Then L/K' is a Galois extension such that $\mathrm{Gal}(L/K') = D_{\mathfrak{q}}$ (see Theorem 11.1.9). The integral closure A' of A in K' satisfies $A' = B \cap K'$. Let $\mathfrak{p}' = \mathfrak{q} \cap A'$ and $k' = A'/\mathfrak{p}'$. The Galois group $D_{\mathfrak{q}}$ acts transitively on the set of prime ideals of B lying over $\mathfrak{p}'$ (Proposition 11.2.2). Since $\mathfrak{q}$ is among those prime ideals, it follows from the definition of $D_{\mathfrak{q}}$ that $\mathfrak{q}$ is the only such prime ideal of B. We thus have $\mathfrak{p}'B = \mathfrak{q}^{e'}$ for some integer $e' \in \mathbb{N}$. Let us set

$$f' = [B/\mathfrak{q} : A'/\mathfrak{p}'] = [\ell : k'].$$

We then have, using successively Corollary 11.2.3, Lemma 11.1.7 and Lemma 11.2.6

$$e'f' = [L : K'] = \mathrm{card}\, D_{\mathfrak{q}} = ef.$$

Now $k \subset k' \subset \ell$, and thus

$$f' = [\ell : k'] \leq [\ell : k] = f.$$

On the other hand

$$\mathfrak{p}B \subset \mathfrak{p}'B = \mathfrak{q}^{e'},$$

and so $e' \leq v_{\mathfrak{q}}(\mathfrak{p}B) = e$. We conclude that we must have $e = e', f = f'$, and so $k = k'$.

Let $\overline{y} \in \ell$, and pick a preimage $y \in B$ of $\overline{y}$. The characteristic polynomial of y over K' verifies, by Proposition 4.3.3 and Proposition 5.1.1

$$\chi_{L/K'}(y) = \prod_{\sigma \in D_{\mathfrak{q}}} (X - \sigma(y)) \in A'[X]$$

Its image in $k'[X] = k[X]$ is a polynomial $Q \in k[X]$ such that $Q(\overline{y}) = 0$, which splits into a product of linear factors

$$Q = \prod_{\sigma \in D_{\mathfrak{q}}} (X - \overline{\sigma}(\overline{y})) \in \ell[X]. \tag{11.2.b}$$

It follows that the minimal polynomial of $\overline{y} \in \ell$ over k splits into a product of linear factors (being a divisor of Q). This proves that the field extension ℓ/k is normal.

Now assume that the field extension ℓ/k is separable. We specialise to the case when $\overline{y}$ is a generator of the k-algebra ℓ; such an elements exists by the primitive element Theorem (Corollary 4.1.19). If $\tau \in \mathrm{Gal}(\ell/k)$, we thus have $Q(\tau(\overline{y})) = \tau(Q(\overline{y})) = 0$, which implies that $\tau(\overline{y})$ is among the elements $\overline{\sigma}(\overline{y})$ for $\sigma \in D_{\mathfrak{q}}$ (those are the roots of Q in ℓ by (11.2.b)). Since the element $\overline{y}$ generates the k-algebra ℓ, it follows that $\tau = \overline{\sigma}$, which proves the stated surjectivity. The fact the $I_{\mathfrak{q}}$ is the kernel of the given morphism follows from the Definition 11.2.7. □

Corollary 11.2.9. *Assume that the field extension ℓ/k is separable. Then, in the notation of Corollary 11.2.3, we have* $\mathrm{card}(I_{\mathfrak{q}}) = e$.

Proof. From Proposition 11.2.8 we obtain a group isomorphism

$$D_{\mathfrak{q}}/I_{\mathfrak{q}} \simeq \mathrm{Gal}(\ell/k),$$

hence, in view of Lemma 11.1.7 and Lemma 11.2.6,

$$f \cdot \mathrm{card}(I_{\mathfrak{q}}) = \mathrm{card}(\mathrm{Gal}(\ell/k)) \cdot \mathrm{card}(I_{\mathfrak{q}}) = \mathrm{card}(D_{\mathfrak{q}}) = ef,$$

and so $\mathrm{card}(I_{\mathfrak{q}}) = e$. □

Corollary 11.2.10. *Let $\mathfrak{q}$ be a prime ideal of B lying over $\mathfrak{p}$. Then the prime ideal $\mathfrak{p}$ does not ramify in B if and only $I_{\mathfrak{q}} = \{\mathrm{id}_L\}$.*

3. The Frobenius automorphism of a number field

In this section $K/\mathbb{Q}$ is a finite Galois extension.

Lemma 11.3.1. *Let p be a prime number which does not ramify in K, and let $\mathfrak{p}$ be a prime ideal of $\mathcal{O}_K$ lying over $p\mathbb{Z}$. Then there exists a unique element $\sigma_{\mathfrak{p}} \in \mathrm{Gal}(K/\mathbb{Q})$ such that*

$$\sigma_{\mathfrak{p}}(x) - x^p \in \mathfrak{p} \quad \textit{for all } x \in \mathcal{O}_K.$$

The element $\sigma_{\mathfrak{p}}$ belongs to the decomposition subgroup $D_{\mathfrak{p}} \subset \mathrm{Gal}(K/\mathbb{Q})$, and the order of $\sigma_{\mathfrak{p}}$ in the group $\mathrm{Gal}(K/\mathbb{Q})$ is $f = [(\mathcal{O}_K/\mathfrak{p}) : \mathbb{F}_p]$.

Proof. By Proposition 11.2.8 and Corollary 11.2.10, we have a group isomorphism

$$D_{\mathfrak{p}} \xrightarrow{\sim} \mathrm{Gal}((\mathcal{O}_K/\mathfrak{p})/\mathbb{F}_p), \tag{11.3.a}$$

sending $\sigma \in D_{\mathfrak{p}}$ to the automorphism in $\mathrm{Gal}((\mathcal{O}_K/\mathfrak{p})/\mathbb{F}_p)$ given by

$$(x \mod \mathfrak{p}) \mapsto (\sigma(x) \mod \mathfrak{p}) \quad \text{for } x \in \mathcal{O}_K.$$

Considering the Frobenius automorphism $\phi\colon y \mapsto y^p$ in $\mathrm{Gal}((\mathcal{O}_K/\mathfrak{p})/\mathbb{F}_p)$ (see Example 11.1.10), it follows that there exists a unique element $\sigma_{\mathfrak{p}} \in D_{\mathfrak{p}}$ such that $\sigma_{\mathfrak{p}}(x) = x^p \mod \mathfrak{p}$ for all $x \in \mathcal{O}_K$. Conversely, if $\sigma \in \mathrm{Gal}(K/\mathbb{Q})$ is such that $\sigma(x) = x^p \mod \mathfrak{p}$ for all $x \in \mathcal{O}_K$ then $\sigma(\mathfrak{p}) \subset \mathfrak{p}$, which implies that $\sigma \in D_{\mathfrak{p}}$ by Remark 11.2.5. This proves the first statement.

In view of the isomorphism (11.3.a), the order of $\sigma_{\mathfrak{p}}$ coincides with the order of the Frobenius automorphism $\phi \in \mathrm{Gal}((\mathcal{O}_K/\mathfrak{p})/\mathbb{F}_p)$, which equals f by Example 11.1.10. □

Definition 11.3.2. The element given by Lemma 11.3.1 is called the *Frobenius automorphism* and is denoted by $\sigma_{\mathfrak{p}}$.

Lemma 11.3.3. *Let p be a prime number which does not ramify in K, and let $\mathfrak{p}, \mathfrak{p}'$ be prime ideals of $\mathcal{O}_K$ lying over $p\mathbb{Z}$. Then there exists $\tau \in \mathrm{Gal}(K/\mathbb{Q})$ such that*

$$\sigma_{\mathfrak{p}'} = \tau \sigma_{\mathfrak{p}} \tau^{-1} \in \mathrm{Gal}(K/\mathbb{Q}).$$

Proof. By Proposition 11.2.2 there exists $\tau \in \mathrm{Gal}(K/\mathbb{Q})$ such that $\mathfrak{p}' = \tau(\mathfrak{p})$. Let $x \in \mathcal{O}_K$ and set $y = \tau^{-1}(x) \in \mathcal{O}_K$. Then by definition of $\sigma_{\mathfrak{p}}$, we have

$$\sigma_{\mathfrak{p}}(y) - y^p \in \mathfrak{p}.$$

Therefore the element

$$\tau \circ \sigma_{\mathfrak{p}} \circ \tau^{-1}(x) - x^p = \tau\big(\sigma_{\mathfrak{p}} \circ \tau^{-1}(x) - \tau^{-1}(x^p)\big) = \tau\big(\sigma_{\mathfrak{p}}(y) - y^p\big)$$

belongs to $\tau(\mathfrak{p}) = \mathfrak{p}'$, which implies that $\tau \circ \sigma_{\mathfrak{p}} \circ \tau^{-1} = \sigma_{\mathfrak{p}'}$. □

Definition 11.3.4. Assume that group $\mathrm{Gal}(K/\mathbb{Q})$ is abelian, and that p does not ramify in K. Then by Lemma 11.3.3 the Frobenius automorphism $\sigma_{\mathfrak{p}} \in \mathrm{Gal}(K/\mathbb{Q})$ is independent of the choice of the prime ideal $\mathfrak{p}$ of $\mathcal{O}_K$ lying over $p\mathbb{Z}$ (recall that such does exist by Remark 10.1.9). In this case, we will write

$$\left(\frac{K/\mathbb{Q}}{p}\right) = \sigma_{\mathfrak{p}} \in \mathrm{Gal}(K/\mathbb{Q}).$$

Lemma 11.3.5. *Let $K/\mathbb{Q}$ be a finite Galois extension, and $F/\mathbb{Q}$ a Galois subextension of $K/\mathbb{Q}$. Let p be a prime number which does not ramify in K, and $\mathfrak{p}$ a prime ideal of $\mathcal{O}_K$ lying over $p\mathbb{Z}$. Then the Frobenius automorphism $\sigma_{\mathfrak{p}} \in \mathrm{Gal}(K/\mathbb{Q})$ restricts to the Frobenius automorphism $\sigma_{\mathfrak{p}\cap\mathcal{O}_F} \in \mathrm{Gal}(F/\mathbb{Q})$.*

Proof. Let $\mathfrak{p}' = \mathfrak{p} \cap \mathcal{O}_F$. Note that $\mathcal{O}_F = L \cap \mathcal{O}_K$, hence $\mathfrak{p}' = \mathfrak{p} \cap F$. Write $\sigma = \sigma_{\mathfrak{p}}$. As $\sigma(\mathfrak{p}) = \mathfrak{p}$ (recall that $\sigma \in D_{\mathfrak{p}}$ by Lemma 11.3.1) and $\sigma(F) = F$ (as $F/\mathbb{Q}$ is normal), we have

$$\sigma(\mathfrak{p}') = \sigma(\mathfrak{p} \cap F) = \mathfrak{p} \cap F = \mathfrak{p}',$$

hence the restriction of σ to $\mathrm{Gal}(F/\mathbb{Q})$ belongs to the decomposition group $D_{\mathfrak{p}'}$. For any $x \in \mathcal{O}_F$, we have $\sigma(x) - x^p \in \mathfrak{p} \cap F = \mathfrak{p}'$. The lemma follows. □

4. Cyclotomic fields

Lemma 11.4.1. *Let L/k be a field extension and $\xi \in L^\times$ be an element of order $m \in \mathbb{N} \smallsetminus \{0\}$. Assume that $L = k(\xi)$. Then the field extension L/k is Galois, and there exists an injective group morphism*

$$j\colon \mathrm{Gal}(L/k) \to (\mathbb{Z}/m\mathbb{Z})^\times$$

such that $\sigma(\xi) = \xi^{j(\sigma)}$ for any $\sigma \in \mathrm{Gal}(L/k)$.

Proof. The powers of ξ are all roots of $X^m - 1$, and there are m of those. Thus

$$X^m - 1 = \prod_{i=0}^{m-1} (X - \xi^i) \in L[X].$$

The minimal polynomial P of ξ over k is a divisor of $X^m - 1$, hence also splits into a product of pairwise distinct monic linear factors in $L[X]$. It follows that the field extension L/k is normal, and that the polynomial $P \in k[X]$ is separable (see Remark 4.1.12). Thus by Proposition 4.2.6 and Corollary 4.4.7 the extension L/k is separable. We have proved that the extension L/k is Galois.

Since the k-algebra L is generated by ξ, every element $g \in \mathrm{Gal}(L/k)$ is determined by the element $g(\xi) \in L$. Since $g(\xi)$ is a root of the polynomial $X^m - 1$, there exists a unique element $j(g) \in \mathbb{Z}/m\mathbb{Z}$ such that $g(\xi) = \xi^{j(g)}$. In addition the element $g(\xi) \in L^\times$ has order m, hence $j(g) \in (\mathbb{Z}/m\mathbb{Z})^\times$. For any $g, h \in \mathrm{Gal}(L/k)$, it is easy to verify that $j(gh) = j(g)j(h)$, and $j(1) = 1$. Therefore j defines an injective ring morphism

$$j\colon \mathrm{Gal}(L/k) \to (\mathbb{Z}/m\mathbb{Z})^\times. \qquad \square$$

Bibliography

[Sam70] Pierre Samuel. *Algebraic theory of numbers*. Houghton Mifflin Co., Boston, Mass., 1970. Translated from the French by Allan J. Silberger.