Reading Notes on Théorie algébrique des nombres

Pierre Samuel

Contents

Notations, definitions, and prerequisites

We employ the usual notations from set theory: $\in, \subset, \cup, \cap$. The complement of a subset B of a set A is denoted $A \setminus B$. The cardinality (or power, or number of elements) of a set A is written $\mathrm{card}(A)$; if A is a group, we speak of the order of A.

We assume that the reader is acquainted with the notions of group, ring, field and vector space, as well as with the elementary theory of vector spaces (also called "linear algebra"). In this book, with the exception of 5.7, "ring" (respectively, "field") means *commutative* ring (respectively, field) *with unit element*.

Given a finite group G and a subgroup H of G, we recall that $\mathrm{card}(H)$ divides $\mathrm{card}(G)$. The quotient $\mathrm{card}(G)/\mathrm{card}(H)$ is called the *index* of H in G and is denoted $(G : H)$. Given two subsets A and B of an additive group G, we write $A + B$ for the for the set of sums $a + b$, $a \in A$, $b \in B$.

Given a ring A, we write $A[X]$ or $A[Y]$ (capital letter) for the ring of polynomials in one variable over A; we write $A[X_1, \ldots, X_n]$ for the polynomials in n variables and $A[[X]]$ for the ring of formal power series.

By convention, a subring A of a ring B contains the unit element of B. Given a ring B, a subring A of B, and an element $x \in B$, we write $A[x]$ for the subring of B generated by A and x, i.e. for the intersection of all subrings of B which contain A and x; it is the set of all sums of the form $a_0 + a_1 x + \cdots + a_n x^n$ ($a_i \in A$); we write $A[x_1, \ldots, x_n]$ for the subring of B generated by A and a finite set $(x_1, \ldots, x_n)$ of elements of B.

A ring A is called an *integral domain* if A contains more than one element and if the product of any two non-zero elements of A is not zero.
An ideal $\mathfrak{b}$ of a ring A is a subgroup of the additive group of A such that $x \in b$ and $a \in A$ implies $ax \in \mathfrak{b}$. The whole ring and the set consisting of the element 0 alone (and denoted (0)) are ideals, sometimes called "trivial" ideals. A field has no non-trivial ideals and this fact distinguishes fields from other rings. Given a set of elements (b_i from a ring A, the intersection of all ideals of A containing the b_i's is an ideal of A, called the ideal *generated by* the b_i's; it is the set of all elements of the form $\sum_i a_i b_i$, with $a_i \in A$. An ideal generated by a single element b is said to be *principal*; notation: Ab or (b).

Let A be a ring and $\mathfrak{b}$ an ideal of A. The equivalence classes $a + \mathfrak{b} (a \in A)$ form a ring, called the *quotient ring* [1] of A by $\mathfrak{b}$ and denoted $A/\mathfrak{b}$. The ideals of $A/\mathfrak{b}$ are of the form $\mathfrak{b}'/\mathfrak{b}$ where $\mathfrak{b}'$ runs through the set of ideals of A which contain $\mathfrak{b}$. In order that $A/\mathfrak{b}$ be a field it is necessary and sufficient that $\mathfrak{b}$ be maximal among the ideals of A distinct from A. We say then that $\mathfrak{b}$ is a *maximal* ideal. An ideal $\mathfrak{p}$ is said to *prime* if $A/\mathfrak{p}$ is an integral domain.

Let A and A' be rings with unit elements e and e'. A *homomorphism* $f\colon A \to A'$ is a mapping f of A to A' such that:

$$f(a+b) = f(a) + f(b), \quad f(ab) = f(a)f(b), \quad \text{and} \quad f(e) = e'.$$

Let A be a ring. An *A-algebra* is a pair consisting of a ring B and a homomorphism $\varphi\colon A \to B$. If A is a field, φ is injective, and we often identify A with its image $\varphi(A)$ (which is a subring of B).

Given a field L and a subfield K of L, we often say L is an *extension* of K.

Usually the unit element of a ring A will be denoted by 1.

The notion of *module* over a ring A (or A-module) is the direct generalisation of the notion of vector space over a field. An A-module M is an abelian group (the operation is addition) provided with a mapping $A \times M \to M$ (written as multiplication) such that $a(x+y) = ax + ay$, $(a+b)x = ax + bx$, $a(bx) = (ab)x$, $1x = x$, $(a, b \in A, x, y \in M)$. There are notions of submodule and of quotient module. Given two A-modules, M and M', a homomorphism (or A-linear mapping) of M to M' is a mapping $f\colon M \to M'$ such that

$$f(x+y) = f(x) + f(y) \quad \text{and} \quad f(ax) = af(x) \quad (a \in A, x, y \in M).$$

Given a homomorphism $f\colon X \to X'$ (of groups, rings, or modules), we call the *kernel* of f and write $\ker(f)$ for the inverse image under f of the neutral element of X'. It is a normal subgroup (or an ideal, or a submodule) of X. In order that f be injective it is necessary and sufficient that $\ker(f)$ consist of only the neutral element of X. We call the *image* of f the subset $f(X)$ of X'; it is a subgroup (or subring, or submodule) of X'.

Let X and X' be sets. A mapping f of X to X' is often denoted $f\colon X \to X'$. When a mapping $f\colon X \to X'$ is described by the value it takes at an arbitrary element $x \in X$, we use the notation $x \mapsto f(x)$. Thus the sine function, $\sin\colon \mathbb{R} \to \mathbb{R}$, can be defined by

$$x \mapsto \sum_{n=0}^{\infty} (-1)^n \frac{x^{2n+1}}{(2n+1)!}.$$

We shall employ the usual notations for the following mathematical objects:

$\mathbb{N}$: set of natural numbers $(0, 1, 2, \ldots, n, \ldots)$ (N for "numbers").

$\mathbb{Z}$: ring of rational integers (natural numbers and their negatives) (Z for "Zahlen").

$\mathbb{Q}$: field of rational numbers (quotients of elements of $\mathbb{Z}$) (Q for "quotients").

[1] The transcriber believes *residue class ring* is a better terminology.

$\mathbb{R}$**:** field of real numbers (R for "reals").

$\mathbb{C}$**:** field of complex numbers (C for "complexes").

$\mathbb{F}_q$**:** finite field with q elements (F for "finite" or "field")

Chapter 1

Principal ideal domains

Remark 1.0.1 (by the transcriber). The content of this chapter is, with a possible exception of Theorem 1.7.6, covered nowadays in most textbooks on modern algebra. But at the publishing of the original text, the situation was quite different, which explains the reason why the original authour often cites Bourbaki "Eléments de Mathématique" as reference. For the record the transcriber left out most citation on Bourbaki.

1.1 Divisibility in principal ideal domains

Let A be an integral domain, K its field of fractions, x and y elements of K. We say that x *divides* y if there exists $a \in A$ such that $y = ax$. Equivalently, we say x is a divisor of y, y is a multiple of x; notation $x \mid y$. This relation between the elements of K depends essentially on the ring A; if there is any confusion possible, we speak of divisibility in K *with respect to* A.

Given $x \in K$ we write Ax for the set of multiples of x. Thus we may write $y \in Ax$, or $Ay \subset Ax$ in place of $x \mid y$. The set Ax is called a *principal fractional ideal* of K with respect to A; if $x \in A$, Ax is the (ordinary) principal ideal of A generated by x. As the relation of divisibility, $x \mid y$, is equivalent to the *order* relation $Ay \subset Ax$, divisibility possesses the following two properties associated with order relations.

$$x \mid x; \quad \text{if } x \mid y \text{ and } y \mid z, \text{ then } x \mid z. \tag{1.1.1}$$

On the other hand, if $x \mid y$ and $y \mid x$, one cannot in general conclude that $x = y$, one has only that $Ax = Ay$, which (if $y \neq 0$) means that the quotient xy^{-1} is an invertible element of A; in this case x and y are called *associates*; they are indistinguishable from the viewpoint of divisibility.

Example 1.1.2. The elements of K which are associates of 1 are the elements invertible in A; they are often called the *units* in A; they form a group under multiplication, and we shall denote this group $A^\times$. The determination of the

units in a ring A is an interesting problem which we shall treat in the case where A is the ring of integers in a number field (see Chapter 4). Here are some simple examples:

(a) If A is a field, $A^\times = A \setminus (0)$.

(b) If $A = \mathbb{Z}$, $A^\times = \{+1, -1\}$.

(c) The units in the ring of polynomials $B = A[X_1, \ldots, X_n]$, A an integral domain, are the invertible constants; in other words $B^\times = A^\times$.

(d) The units in the ring of formal power series $A[X_1, \ldots, X_n]$ are the formal power series whose constant term is invertible.

Definition 1.1.3. A ring A is called a *principal ideal domain* (*PID* for short) if it is an integral domain and if every ideal of A is principal.

We know that the ring $\mathbb{Z}$ of rational integers is a PID. (Recall that any ideal $\mathfrak{a} \neq (0)$ of $\mathbb{Z}$ contains a least integer $b > 0$. Dividing $x \in \mathfrak{a}$ by b and using the fact that $\mathbb{Z}$ is Euclidean, one sees that x is a multiple of b.) If K is a field we know that the ring $K[X]$ of polynomials in one variable over K is a PID (same method of proof: take a non-zero polynomial $b(X)$ of lowest degree in the given ideal $\mathfrak{a} \neq (0)$ and make use of the fact that $K[X]$ is a Euclidean ring, i.e. the remainder under division of an arbitrary element of $\mathfrak{a}$ by $b(X)$ must be of lower degree than $b(X)$ or zero, which implies zero). This general method shows that any "Euclidean ring" is a PID. If K is a field, it is easy to see that any non-zero ideal in the ring of formal power series $A = K[[X]]$ is of the form AX^n with $n \geq 0$, so that $A = K[[X]]$ is a PID too.

Divisibility in the field of fractions K of a PID A is particularly simple. We shall review it briefly.

I. Two arbitrary elementsu, v of K have a *greatest common divisor* (gcd), i.e., an element d for which the relations

$$\text{“}x \mid u \text{ and } x \mid v\text{”} \quad \text{and} \quad \text{“}x \mid d\text{”}$$

are equivalent. This means the same thing as the assertion that Au and Av have a *least upper bound* in the partially ordered set of fractional ideals. This least upper bound is $Au + Av$, which is itself a principal fractional ideal, since the ring A is a PID (all this is clear for $u, v \in A$; one may reduce to this case by multiplying u and v by a common denominator). We obtain more than the existence of a gcd ("the identity of Bezout") there exist elements $a, b \in A$ such that the gcd of u and v may be written in the form

$$d = au + bv \tag{1.1.4}$$

The greatest common divisor of u and v is obviously unique up to multiplication by units in A.

II. Two arbitrary elements $u, v \in K$ have a *least common multiple* (lcm), i.e. there is an element $m \in K$ for which the relations

$$\text{“}u \mid x \text{ and } v \mid x\text{”} \quad \text{and} \quad \text{“}m \mid x\text{”}$$

are equivalent. This one can see from the fact that sending $t \mapsto t^{-1}$ in K reverses divisibility. So the proof of the existence of least common multiples reduces to the proof of the existence of greatest common divisors. From the relation

$$\operatorname{lcm}(u, v) = \gcd(u^{-1}, v^{-1})^{-1} \quad (u, v \neq 0)$$

we easily obtain the following well-known formula

$$\gcd(u, v) \cdot \operatorname{lcm}(u, v) = uv.$$

We may also proceed as in (I) to remark that the existence of $\operatorname{lcm}(u, v)$ is equivalent to the existence of a greatest lower bound for Au and Av in the partially ordered set of principal fractional ideals. The greatest lower bound for $Au$and Av is $Au \cap Av$.

III. Two elements a, b of A are said to be *relatively prime* if $\gcd(a, b) = 1$. Let us recall the important

Lemma 1.1.5 (Euclid)**.** *Let a, b, c be elements in a PID A. If a divides bc and is relatively prime to b, then a divides c.*

Here is a quick proof:

Proof. By Bezout (1.1.4) there exist $a', b' \in A$ such that $1 = a'a + b'b$; whence $c = a'ac + b'bc$. Since a divides both terms on the right-hand, side, a divides c as well. □

IV. Finally there is unique factorisation into products of primes.

Theorem 1.1.6. *Let A be a PID and let K be its field of fractions. There exists a subset $P \subset A$ such that any $x \in K$ may be uniquely expressed in the form*

$$x = u \prod_{p \in P} p^{v_p(x)},$$

where u is a unit in A and where the exponents $v_p(x)$ are elements of $\mathbb{Z}$, all zero except for a finite subset among them.

1.2 An example: the diophantine equations $X^2 + Y^2 = Z^2$ and $X^4 + Y^4 = Z^4$.

One of the most attractive parts of number theory is the study of *diophantine equations*. One considers polynomial equations $P(X_1, \ldots, X_n) = 0$ with coefficients in $\mathbb{Z}$ (respectively, in $\mathbb{Q}$) and one seeks solutions (x) in $\mathbb{Z}$ (respectively, in

$\mathbb{Q}$). One can replace $\mathbb{Z}$ (respectively, $\mathbb{Q}$) by more general rings A (respectively, fields K). We will give an example later (1.6).

We are going to study here two special cases of Fermat's famous equation:

$$X^n + Y^n = Z^n. \tag{1.2.1}$$

Fermat claimed to have shown that, for $n \geq 3$, this equation has no non-trivial integer solution (x, y, z). His proof has never been found. Numerous mathematicians have since Fermat's time worked intensively on this problem, and Andrew Wiles gave a proof for Fermat's claim in 1995.

(As Wiles made in his proof an extensive use of results in algebraic geometry and number theory that were not available to Fermat, present-day opinion holds that, in his "proof", Fermat made a mistake. However, in a retrospect, that mistake is worthy of a first-class mathematician. For example he might have conceived the idea (ingenious for his time) of working in the ring of integers of a field containing nth roots of unity; he may have believed that such a ring is always a PID. In fact, we know how to prove Fermat's claim for any exponent n for which the ring of nth roots of unity is a PID. However, this is not the case for all n. For n prime, this ring is a PID for finitely many values of n.)

For $n = 2$, equation (1.2.1) has integer solutions, e.g. $(3, 4, 5)$. One can give a complete description of all the integer solutions of (1.2.1).

Theorem 1.2.2. *If x, y, z are positive integers such that $x^2 + y^2 = z^2$, then there exists an integer d and two relatively prime integers u and v such that (except, possibly, for a permutation of x and y):*

$$x = d(u^2 - v^2), \quad y = 2duv, \quad \textit{and} \quad z = d(u^2 + v^2). \tag{1.2.3}$$

Proof. An easy calculation shows that formula (1.2.3) gives solutions for $X^2 + Y^2 = Z^2$. Conversely, let x, y, and z be positive integers such that $x^2 + y^2 = z^2$. After dividing x, y, z by their greatest common divisor, we may assume that the three numbers are relatively prime. It follows that they are pairwise relatively prime as well; for example, if x and z have a common prime factor p,, then p divides $y^2 = z^2 - x^2$ and, therefore, also y. In particular, two of the numbers x, y, z are odd; the third is necessarily even. The numbers x and y cannot both be odd, for, if they were, we would have $x^2 \equiv 1 \bmod 4, y^2 \equiv 1 \bmod 4$, and $z^2 \equiv 2 \bmod 4$, which contradicts the fact that z^2 is a square. We have, then, after possibly switching x and y:

$$x \text{ odd}, \quad y \text{ even}, \quad \text{and } z \text{ odd}. \tag{1.2.4}$$

Note that

$$y^2 = z^2 - x^2 = (z - x)(z + x).$$

Since the greatest common divisor of $2x$ and $2z$ is 2, and since $2x = (z + x) - (z - x), 2z = (z + x) + (z - x)$, the greatest common divisor of $z - x$ and $z + x$ can only be 2. Put $y = 2y', z + x = 2x', z - x = 2z'$, where y', x' , and z' are integers (since $y, z + x$, and $z - x$ are even by (1.2.4)). We have $y'^2 = x'z'$.

Since x' and z' are relatively prime, we see that x' and z' are squares u^2 and v^2; in fact any prime factor of y'^2 appears, with an even exponent, either in the prime factorisation of x' or in that of z', but not in both. We thus have $z+x = 2u^2, z-x = 2v^2$, and $y^2 = 2u^2 \cdot 2v^2$; whence, $x = u^2 - v^2, y = 2uv$, and $z = u^2+v^2$. Here u and v are relatively prime, since otherwise x, y, z would have a common prime factor. Multiplying through by the greatest common divisor of x, y, z, call it d, we obtain (1.2.3). □

Theorem 1.2.5. *The equation $X^4 + Y^4 = Z^2$ has no solution in positive integers x, y, z.*

Proof. If there is a solution (x, y, z), where x, y, and z are positive integers, then there is such a solution in which z is minimal. In this case, x, y, and z are pairwise relatively prime; if for example x and y have a common prime factor p, then p^4 divides z^2, so p^2 divides z and $(x/p, y/p, z/p^2)$ would be a solution, contradicting the minimality of z. The two other cases are analogous and even easier. As our equation may be written as $(X^2)^2 + (Y^2)^2 = Z^2$, we may apply Theorem 1.2.2 to it. After possibly permuting x and y we see that there are positive relatively prime integers u and v such that

$$x^2 = u^2 - v^2, \quad y^2 = 2uv, \quad \text{and} \quad z = u^2 + v^2. \tag{1.2.6}$$

Since $4 \mid y^2$, the relation $y^2 = 2uv$ implies that one of the two numbers u and v is even; the other is necessarily odd. Thus, u even and v odd entails $u^2 \equiv 0 \bmod 4$ and $v^2 \equiv 1 \bmod 4$, whence $x^2 = u^2 - v^2 \equiv -1 \bmod 4$, an impossibility. So u is odd and $v = 2v'$. The relation $y^2 = 4uv'$ and the fact that u and v' are relatively prime implies that u and v^2 are squares a^2 and b^2. We apply Theorem 1.2.2 once more, this time to the equation $x^2 + v^2 = u^2$ (cf (1.2.6)). Since x and u are odd, v even, and x, v, and u pairwise prime, we obtain two relatively prime positive integers c and d such that

$$x = c^2 - d^2, \quad v = 2cd, \quad \text{and} \quad u = c^2 + d^2. \tag{1.2.7}$$

Now, from$v = 2v' = 2b^2$, it follows that $cd = b^2$, so that c and d are again squares x'^2 and y'^2 (they are relatively prime). Since $u = a^2$, (1.2.7) may be rewritten as

$$a^2 = x'^4 + y'^4,$$

which is of the same form as the original equation. On the other hand, by (1.2.6), $z = u^2 + v^2 = a^4 + 4b^4 > a^4$, whence $z > a$, which contradicts the minimality of z, proving Theorem 1.2.5. □

1.3 Some lemmas concerning ideals; Euler's φ-function

Let $n \geq 1$ be a natural number. We write $\varphi(n)$ for the number of integers $q, 0 \leq q \leq n$, such that q and n are relatively prime (since 0 and n are divisible

by n, it is equivalent to take $1 \leq q \leq n-1$ for any $n > 1$; set $\varphi(1) = 1$). The function φ so defined is called *Euler's φ-function* (or *Euler's totient function*). If p is a prime number, then clearly:

$$\varphi(p) = p - 1.$$

For $n = p^s$, a power of a prime, the integers relatively prime to n are those integers which are not multiples of p. There are p^{s-1} multiples of p between 1 and p^s. Therefore,

$$\varphi(p^s) = p^s - p^{s-1} = p^{s-1}(p-1). \tag{1.3.1}$$

Now we intend to calculate $\varphi(n)$ by making use of the fact that n may be expressed as a product of powers of primes. For this purpose we need some properties of $\varphi(n)$ and we need some lemmas concerning ideals. These lemmas will be useful later.

Proposition 1.3.2. *Let $n \geq 1$ be a natural number. The value $\varphi(n)$ of Euler's φ-function equals the number of elements of $\mathbb{Z}/n\mathbb{Z}$ which generate this group. It also equals the number of units in the ring $\mathbb{Z}/n\mathbb{Z}$.*

Proof. Let us recall that each congruence class mod $n\mathbb{Z}$ contains a unique integer q such that $0 \leq q \leq n-1$. For such an integer q we write $\overline{q}$ for its residue class mod $n\mathbb{Z}$. It suffices to prove the following implications: q relatively prime to $n \Rightarrow \overline{q}$ a unit in the ring $\mathbb{Z}/n\mathbb{Z} \Rightarrow \overline{q}$ generates the additive group $\mathbb{Z}/n\mathbb{Z} \Rightarrow q$ relatively prime to n. If q is relatively prime to n, Bezout's identity (1.1.4) implies that there are integers x and y such that $qx + ny = 1$; whence $\overline{qx} = \overline{1}$, so $\overline{q}$ is a unit in $\mathbb{Z}/n\mathbb{Z}$. Writing x for an integer such that $\overline{q} \cdot \overline{x} = 1$, we see that $\overline{a} = \overline{a} \cdot \overline{x} \cdot \overline{q}$ (in the ring $\mathbb{Z}/n\mathbb{Z}$), where $\overline{a}$ is an arbitrary element of $\mathbb{Z}/n\mathbb{Z} (0 \leq a < n)$. It follows that $\overline{a} = (ax) \cdot \overline{q}$ (in the additive group $\mathbb{Z}/n\mathbb{Z}$), so $\overline{q}$ generates the group $\mathbb{Z}/n\mathbb{Z}$. Finally, if $\overline{q}$ generates $\mathbb{Z}/n\mathbb{Z}$, there is an x such that $x\overline{q} = \overline{1}$, thus such that $xy \equiv 1 \bmod n$; thus there exists an integer y for which $xq - 1 = yn$, so $1 = xq - yn$. This is an instance of Bezout's identity, which shows that q is relatively prime to n. □

Lemma 1.3.3. *Let A be a ring, $\mathfrak{a}$ and $\mathfrak{b}$ ideals of A such that $\mathfrak{a} + \mathfrak{b} = A$. Then $\mathfrak{a} \cap \mathfrak{b} = \mathfrak{ab}$ and the canonical homomorphism $\varphi\colon A \to A/\mathfrak{a} \times A/\mathfrak{b}$ induces an isomorphism $[\theta\colon A/\mathfrak{ab} \to A/\mathfrak{a} \times A/\mathfrak{b}$.]*

Recall that the homomorphism φ sends any $x \in A$ into the pair consisting of the class of x mod $\mathfrak{a}$ and the class of x mod $\mathfrak{b}$.

Proof. We know that, in general, $\mathfrak{ab} \subset \mathfrak{a}$ and $\mathfrak{ab} \subset \mathfrak{b}$, so $\mathfrak{ab} \subset \mathfrak{a} \cap \mathfrak{b}$. Let $x \in \mathfrak{a} \cap \mathfrak{b}$. Since $\mathfrak{a} + \mathfrak{b} = A$, there are elements $a \in \mathfrak{a}$ and $b \in \mathfrak{b}$ such that $a + b = 1$. Thus $x = ax + xb$ is a sum of two elements of $\mathfrak{ab}$, whence $a \in \mathfrak{ab}$ and $\mathfrak{a} \cap \mathfrak{b} \subset \mathfrak{ab}$. Therefore $\mathfrak{ab} = \mathfrak{a} \cap \mathfrak{b}$.

Clearly $\mathfrak{a} \cap \mathfrak{b}$ is the kernel of φ. Since $\mathfrak{a} \cap \mathfrak{b} = \mathfrak{ab}$, φ is constant on each residue class mod $\mathfrak{ab}$. Thus, we obtain a mapping $\theta\colon A/\mathfrak{ab} \to A/\mathfrak{a} \times A/\mathfrak{b}$, which

is obviously a homomorphism. Since $\varphi^{-1}(0) = \mathfrak{a}\mathfrak{b}, \theta^{-1}(0) = (0)$, so θ is injective. It remains to show that θ is surjective.

We have "passed to the residue class ring" in the course of the above argument. Henceforth, we shall be much more brief in explaining analogous arguments.

In order to show that θ (or, equivalently, φ) is surjective, we have to find, for any pair $y \in A$ and $z \in A$, an element $a \in A$ such that $x + \mathfrak{a} = y + \mathfrak{a}$ and $x + \mathfrak{b} = z + \mathfrak{b}$. Take $a \in \mathfrak{a}$ and $b \in \mathfrak{b}$ such that $a + b = 1$. Set $x = az + by$. Modulo $\mathfrak{a}, x \equiv by \equiv (1-a)y \equiv y - ay \equiv y$; similarly, $x \equiv z \bmod \mathfrak{b}$. □

Lemma 1.3.4 (Chinese remainder theorem)**.** *Let A be a ring and $(\mathfrak{a}_i)_{1 \leq i \leq r}$, a finite set of ideals of A such that $\mathfrak{a}_i + \mathfrak{a}_j = A$ for $i \neq j$ (such ideals are said to be* coprime*). Then there is a canonical isomorphism of $A/\mathfrak{a}_1 \cdots \mathfrak{a}_r$ onto $\prod_{i=1}^{r} A/\mathfrak{a}_i$.*

Proof. Lemma 1.3.3 is the case $r = 2$ of Lemma 1.3.4. We proceed by induction on r. Put $\mathfrak{b} = \mathfrak{a}_2 \cdots \mathfrak{a}_r$. Let us show that $\mathfrak{a}_1 + \mathfrak{b} = A$. For $i \geq 2$ we have $\mathfrak{a}_1 + \mathfrak{a}_i = A$, so there are elements $c_i \in \mathfrak{a}_1$ and $a_i \in \mathfrak{a}_i$, such that

$$c_i + a_i = 1, \quad 1 = \prod_{i=1}^{r} (c_i + a_i) = c + a_2 \cdots a_r,$$

where c is a sum of terms each of which contains at least one c_i, as a factor. Therefore, $c \in a_1$. As $a_2 \cdots a_r \in \mathfrak{a}$, it follows that $\mathfrak{a}_1 + \mathfrak{b} = A$.

By Lemma 1.3.3, $A/\mathfrak{a}_1\mathfrak{b}$ is isomorphic to $A/\mathfrak{a}_1 \times A/\mathfrak{b}$. According to the induction hypothesis $A/\mathfrak{b} = A/\mathfrak{a}_2 \cdots \mathfrak{a}_r$, which is isomorphic to $A/\mathfrak{a}_2 \times \cdots \times A/\mathfrak{a}_r$. The lemma follows by composing these isomorphisms. □

Let us apply these lemmas to $\mathbb{Z}$.

Proposition 1.3.5. *Let n and m be relatively prime integers. Then the ring $\mathbb{Z}/nm\mathbb{Z}$ is isomorphic to the product ring $\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$.*

Proof. This is a special case of Lemma 1.3.3, the hypothesis $n\mathbb{Z} + m\mathbb{Z} = \mathbb{Z}$ being Bezout's identity. □

Corollary 1.3.6. *If n and m are relatively prime positive integers, then $\varphi(nm) = \varphi(n)\varphi(m)$.*

Proof. $\varphi(nm)$ is the number of units in $\mathbb{Z}/nm\mathbb{Z}$ (Proposition 1.3.2) which is isomorphic to $\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$. Now an element (α, β) of a ring product is invertible if and only if each of its components α, β is invertible. Thus our assertion follows from Proposition 1.3.2. □

Corollary 1.3.7. *Let n be a positive integer and let $n = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$ be its prime factorisation. Then $\varphi(n) = n(1 - 1/p_1) \cdots (1 - 1/p_r)$.*

Proof. By Corollary 1.3.6 $\varphi(n) = \varphi(p_1^{\alpha_1}) \cdots \varphi(p_r^{\alpha_r})$. By (1.3.1) $\varphi(p_i^{\alpha_i}) = p_i^{\alpha_i - 1}(p_i - 1) = p_i^{\alpha_i}(1 - 1/p_i)$. Multiplication gives our formula. □

1.4 Some preliminaries concerning modules

Before studying modules over a PID, we make some remarks concerning modules over arbitrary commutative rings.

Let A be a commutative ring and let I be a set. Let $A^{(I)}$ denote the set of sequences $(a_i)_{i\in I}$ indexed by I, of elements of A such that $a_i = 0$ except for a finite number of indices $i \in I$. Thus $A^{(I)}$ is a subset of the cartesian product set A^i, and also a submodule of A^I — if one provides $A - I$ with the A-module structure defined by componentwise addition and scalar multiplication.

If I is finite, then $A^{(I)} = A^I$.

For $j \in I$, the sequence $(\delta_{ji})_{i\in I}$ such that $\delta_{jj} = 1$ and $\delta_{ji} = 0$ for $i \neq j$ is an element e_j of $A^{(I)}$. Every element $(a_j)_{j\in I}$ of $A^{(I)}$ has a unique expression as a (finite) linear combination of the e_j. More precisely,

$$(a_j)_{j\in I} = \sum_{j\in I} a_j e_j$$

(note that, in the summation on the right, all the terms are zero except for a finite number, so that the summation makes sense).

We call $(e_j)_{j\in I}$ the *canonical basis* for $A^{(I)}$.

Let A be a ring, M an A-module, and $(x_i)_{i\in I}$ a family of elements of M. To everv element $(a_i)_{i\in I}$ of $A^{(I)}$ let us associate the element $\sum_i a_i x_i$ of M (as before, the summation makes sense). Thus we obtain a mapping $\varphi\colon A^{(I)} \to M$, which is obviously linear. If $(e_i)_{i\in I}$ is the canonical basis for $A^{(I)}$, then $\varphi(e_i) = x_i$ for any $i \in I$. The equivalence of the following statements is immediate:

$$(x_i)_{i\in I} \text{ is a linearly independent set } \Leftrightarrow \varphi \text{ is injective.}$$
$$(x_i)_{i\in I} \text{ geneates } M \Leftrightarrow \varphi \text{ is surjective.}$$

If φ is bijective, $(x_i)_{i\in I}$ is called a *basis* for M. This means that every element of M has a unique expression as a linear combination of the elements $(x_i)_{i\in I}$. A module M which has a basis is called a *free module*.

Remark 1.4.1. In contrast to the case of vector spaces over a field, a module over a ring need not have a basis. For example, the $\mathbb{Z}$-module $\mathbb{Z}/n\mathbb{Z}$ does not have a basis for $n \neq 0$ or 1. In the ensuing discussion we shall show that certain modules are free. This type of result is *seldom* trivial.

A module is said to be of *finite type* if it contains a finite generating set. The following theorem is basic for the study of the properties of Noetherian rings and modules. We develop this topic further in Chapter 3.

Theorem 1.4.2. *Let A be a ring and M an A-module. The following conditions are equivalent.*

(a) Every non-empty family of submodules of M contains a maximal element (with respect to inclusion).

(b) Every ascending sequence $(M_n)_{n\geq 0}$ (again with respect to inclusion) of submodules of M is stationary (i.e. there exists n_0 such that $M_n = M_{n_0}$ for all $n \geq n_0$).

(c) Every submodule of M is of finite type.

Proof. (a) $\Rightarrow$ (c): Let E be a submodule of M and let Φ be the collection consisting of all submodules of finite type of E. Then Φ is not empty, since $(0) \in \Phi$. By (a) Φ contains a maximal element F. For $x \in E$, $F + Ax$ is a submodule of finite type of E (it is generated by the union of $\{x\}$ and any finite set of generators for F). Thus $F + Ax = F$, since $F + Ax \supset F$ and F is maximal. Therefore, $x \in F, E \subset F, E = F$, and E is of finite type.
(c) $\Rightarrow$ (b): Let $(M_n)_{n\geq 0}$ be an ascending chain of submodules of M. Then $E = \cup_{n\geq 0} M_n$. is a submodule of M. By (c) it contains a finite set of generators $(x_1, \ldots, x_q)$. For every i there is an index $n(i)$ such that $x_i \in M_{n(i)}$. Let n_0 be the largest of the $n(i)$'s. Then $x_i \in M_{n_0}$ for all i, so $E \subset M_{n_0}$ and $E = M_{n_0}$. For $n > n_0$ the inclusion relations $M_{n_0} \subset M_n \subset E$ and the equality $M_{n_0} = E$ imply that $M_{n_0} = M_n$. Thus the sequence (M_n) is stationary beyond n_0.
(b) $\Rightarrow$ (a): This is concluded as a special case of Lemma 1.4.3 concerning partially ordered sets that proves a stronger result (a) $\Leftrightarrow$ (b). $\square$

Lemma 1.4.3. *Let $(T, \succeq)$ be a partially ordered set. The following statements are equivalent:*

(i) Every non-empty subset of T contains a maximal element.

(ii) Every ascending chain $(t_n)_{n\geq 0}$ of elements of T is stationary.

Proof. (i) $\Rightarrow$ (ii): Let t_q be a maximal element of the ascending chain (t_n). Then, for $n \succeq q, t_n \succeq t_q$ (the chain ascends), so $t_n = t_q$ (maximality).
(ii) $\Rightarrow$ (i): We will show the contrapositive. Suppose (i) does not hold, thus there exists a subset S of T which does not contain a maximal element. Then, for any $x \in S$, the set of elements $\succ x$ of S is nonempty. By the axiom of choice there exists a mapping $f\colon S \to S$ such that $f(x) \succ x$ for all $x \in S$. Since S is not empty, one may choose $t_0 \in S$ and define by induction the chain $(t_n)_{n\geq 0}$ by setting $t_{n+1} = f(t_n)$. The chain is strictly ascending; it is therefore not stationary. Thus (ii) does not hold, so (ii) $\Rightarrow$ (i) is established. $\square$

Corollary 1.4.4 (to Theorem 1.4.2)**.** *In a PID A, every non-empty family of ideals contains a maximal element.*

Proof. If one considers A as a module over itself, its submodules are its ideals. As all ideals are principal, they are A-modules generated by a single element, thus of finite type. The corollary follows from the implication (c) $\Rightarrow$ (a) of Theorem 1.4.2. $\square$

1.5 Modules over PIDs

Let A be an integral domain and let K be its field of fractions. A free A-module (isomorphic to an $A^{(I)}$ for some I) may be injected into a vector space over K ($K^{(I)}$ in the case of $A^{(I)}$). It follows that the same thing is true for any submodule M of a free A-module. The dimension of the subspace generated by M is called the *rank* of M. If M is itself free and admits a basis having n elements, then the rank of M is n.

Theorem 1.5.1. *Let A be a PID, M a free A-module of rank n, and M' a submodule of M. Then:*

(a) M' is free of rank $q, 0 \leq q \leq n$.

(b) If $M' \neq (0)$, there exists a basis $(e_1, \ldots, e_n)$ of M and non-zero elements $a_1, \ldots, a_q \in A$ such that $(a_1 e_1, \ldots, a_q e_q)$ is a basis of M' and such that a_i divides $a_{i+1}, 1 \leq i \leq q-1$.

Proof. The theorem is trivial for $M' = (0)$, so we may assume $M' \neq (0)$. Let $L(M, A)$ be the set of linear forms on M. For $u \in L(M, A), u(M')$ is a submodule of A, an ideal of A. We may write $u(M') = Aa_u$ with $a_u \in A$, since the ideal is principal. Let $u \in L(M, A)$ be such that Aa_u is maximal among the $Aa_v (v \in L(M, A))$ (Corollary 1.4.4). Let us take a basis $(x_1, \ldots, x_n)$ of M, which identifies M with A^n. Let $\mathrm{Pr}_i\, M \to A$ be the projection on the i'th coordinate, i.e. $\mathrm{Pr}_i(x_j) = \delta_{ij}$. Since $M' \neq (0)$, for at least one $i, 1 \leq i \leq n, \mathrm{Pr}_i(M')$ is not (0). Thus $a_u \neq (0)$. By our construction there exists $e' \in M'$ such that $u(e') = a_u$. Let us show that for every $v \in L(M, A), a_u \mid v(e')$. Indeed, if $d = \gcd(a_u, v(e'))$, then $d = ba_u + cv(e')$ with $b, c \in A$, whence $d = (bu + cv)(e')$. Since $bu + cv$ is a linear form on $M, Aa_u \subset Ad \subset u(M')$. The maximality of Aa implies that $Ad = Aa_u$, so a_u must divide ve').

In particular, $a_u \mid \mathrm{Pr}_i(e')$, so let $\mathrm{Pr}_i(e') = a_u b_i$ with $b_i \in A$. Put $e = \sum_{i=1}^{n} b_i x_i$. Then $e' = a_u e$. Since $u(e') = a_u = a_u \cdot u(e)$, it follows that $u(e) = 1$ (note that $a_u \neq 0$). Let us show that

(1) $M = \ker(u) + Ae$

(2) $M' = (M' \cap \ker(u)) + Ae' \quad$ ((where $e' = a_u e$),

the sum being direct.
(1): For every $x \in M, x = u(x)e + (x - u(x)e)$. We see that $u(x - u(x)e) = u(x) - u(x)u(e) = 0$, since $u(e) = 1$, so $x - u(x)e \in \ker(u)$. This shows that $Ae + \ker(u) = M$; obviously $Ae \cap \ker(u) = (0)$.
(2): For $y \in M', u(y) = ba_u$ with $b \in A$, so $y = ba_u e + (y - u(y)e) = be' + (y - u(y)e)$. Again it is clear that $y - u(y)e \in \ker(u)$ and also that $y - u(y)e = y - be' \in M'$, i.e. $y - u(y)e \in M' \cap \ker(u)$ and $be' \in Ae' \subset Ae$. This entails (2).

Now we prove (a) by induction on the rank q of M'. If $q = 0, M' = (0)$ and there is nothing to prove. If $q > 0, M' \cap \ker(u)$ is of rank $q - 1$ according to (2), and is therefore free according to the induction hypothesis. As, in (2), the sum

is direct, we obtain a basis for M' by adding e' to a basis for $M' \cap \ker(u)$. Thus M' is free and (a) is true.

To prove (b) we argue by induction on the rank n of M. Again the case $n = 0$ is trivial. By (a), $\ker(u)$ is free and of rank $n-1$, since, in (b), the sum is direct. We apply the induction hypothesis to the free module $\ker(u)$ and to its submodule $M' \cap \ker(u)$: if $M' \cap \ker(u) \neq (0)$, there exists $q \leq n$, a basis $(e_2, \ldots, e_n)$ of $\ker(u)$, and there are non-zero elements $a_2, \ldots, a_q$, of A such that $(a_2e_2, \ldots, a_qe_q)$ is a basis for $M' \cap \ker(u)$ and such that a_i divides $a_{i+1}, 2 \leq i \leq q-1$. Keeping the same notations as above, we set $a_1 = a_u$ and $e_1 = e$. Then $(e_l, e_2, \ldots, e_n)$ is a basis for M (according to (1)), and $(a_1e_1, \ldots, a_qe_q)$ is a basis for M' (according to (1)) and the fact that $e' = a_1e_1$). It remains to prove that $a_1 \mid a_2$. Let v be the linear form on M defined by the relation $v(e_1) = v(e_2) = 1$ and $v(e_i) = 0$ for $i \geq 3$. Then $a_1 = a_u = v(a_ue_1) = v(e') \in v(M')$, so $Aa_u \subset v(M')$. By the maximality of Aa_u we may conclude that $v(M') = Aa_u = Aa_1$. Since $a_2 = v(a_2e_2) \in v(M')$, we see that $a_2 \in Aa_1$, i.e. $a_1 \mid a_2$. □

Remark 1.5.2. The ideals Aa_i of Theorem 1.5.1 are called the *invariant factors* of M' in M. One can show that they are uniquely determined by M and M'.

Corollary 1.5.3. *Let A be a PID. Let E be an A-module of finite type. Then E is isomorphic to a product $(A/\mathfrak{a}_1) \times (A/\mathfrak{a}_1) \times \cdots \times (A/\mathfrak{a}_n)$, where the $\mathfrak{a}$'s are ideals of A such that $\mathfrak{a}_1 \supset \mathfrak{a}_2 \supset \cdots \supset \mathfrak{a}_n$.*

Proof. Let $(x_1, \ldots, x_n)$ be a finite set of generators of E. According to the beginning of 1.4, there is a surjective homomorphism $\varphi\colon A^n \to E$, such that E is isomorphic to $A^n/\ker(\varphi)$. By Theorem 1.5.1, there is a basis $(e_1, \ldots, e_n)$ of A^n, an integer $q \leq n$, and nonzero elements $a_1, \ldots, a_q$ of A such that $(a_1e_1, \ldots, a_qe_q)$ is a basis of $\ker(\varphi)$ and such that a_i divides a_{i+1} for all $i, 1 \leq i \leq q-1$. Put $a_p = 0$ for $q+1 \leq p \leq n$. Then $A^n/\ker(\varphi)$ is isomorphic to the product of the $Ae_i/Aa_ie_i, (1 \leq i \leq n)$, and Ae_i/Aa_ie_i is isomorphic to A/Aa_i. Putting $\mathfrak{a} = Aa_i$, we obtain the corollary. □

We shall say that a module E over an integral domain A is *torsion free* if the relation $ax = 0, (a \in A, x \in E)$ implies $a = 0$ or $x = 0$.

Corollary 1.5.4. *Over a PID A, every module E of finite type which is torsion free is free.*

Proof. We make use of Corollary 1.5.3: $E \cong (A/\mathfrak{a}_1) \times \cdots \times (A/\mathfrak{a}_n)$. Suppressing the factors which are zero, we may suppose that $\mathfrak{a}_i \neq A$ for all i. If $\mathfrak{a}_1 \neq (0)$, if a is a non-zero element of $\mathfrak{a}_1$, if x_1 is a non-zero element of $A/\mathfrak{a}_1$ and if $x = (x_1, 0, \cdots, 0)$, then $ax = 0$ contradicting the fact that E is torsion free. Thus $\mathfrak{a}_1 = (0), \mathfrak{a}_i = (0)$ for all i (since $\mathfrak{a}_i \subset \mathfrak{a}_1$), and E is isomorphic to A^n. □

Remark 1.5.5. The hypothesis that E is of finite type is essential: for example $\mathbb{Q}$ is a torsion free $\mathbb{Z}$-module which is not free.

Corollary 1.5.6. *Over a PID A, every module E of finite type is isomorphic to a finite product of modules M_i, where each M_i is equal to A or to a quotient A/Ap^s with p prime.*

Proof. We make use of Corollary 1.5.3 and we decompose each factor $A/A\mathfrak{a}$ where $a \neq 0$, by means of Lemma 1.3.4: if $a = up_1^{s_1} \cdots p_r^{s_r}$ is the prime factorisation of a, A/Aa is isomorphic to the product of the $A/Ap_i^{s_i}$. □

Corollary 1.5.7. *Let G be a finite commutative group. There exists $x \in G$ whose order is the least common multiple of the orders of the elements of G.*

Proof. A commutative group is a $\mathbb{Z}$-module (the operation being addition). According to Corollary 1.5.3

$$G \cong \mathbb{Z}/a_1\mathbb{Z} \times \cdots \times \mathbb{Z}/a_n\mathbb{Z}$$

where $a_1 \mid a_2 \mid \cdots \mid a_n$. We have $a_i \neq 0$ for all i; otherwise G would be infinite. We write y for the residue class of 1 in $\mathbb{Z}/a_n\mathbb{Z}$ and we put $x = (0, \ldots, 0, y)$. The order of x is obviously a_n. For $z = (z_1, \ldots, z_n) \in G$, we have $a_n z = 0$, since a_i divides a_n for all i. Therefore a_n is a multiple of the order of z and x is the element sought. □

1.6 Roots of unity in a field

Theorem 1.6.1. *Let K be a field. Every finite subgroup G of the multiplicative group $K^\times$ consists of roots of unity and is cyclic.*

Proof. According to Corollary 1.5.7, there exists $z \in G$ whose order n is such that $y^n = 1$ for every $y \in G$. Since a polynomial of degree n over a field (for example $X^n - 1$) has at most n roots in the field, the number of elements of G is at most n. Now, inasmuch as z has order n, G contains the n elements $z, z^2, \ldots, z^n = 1$, which are all distinct. Thus G is comprised of these elements and is cyclic. □

If a field K contains n nth roots of unity, they form a cyclic group of order n (isomorphic to $\mathbb{Z}/n\mathbb{Z}$). A generator of this group is called a *primitive* nth root of unity, every nth root of unity is thus a power of such a primitive root. According to Proposition 1.3.2, the number of these primitive roots is $\varphi(n)$.

1.7 Finite fields

Let K be a field. There is a unique ring homomorphism $\varphi\colon \mathbb{Z} \to K$ (defined by $\varphi(n) = \overbrace{1 + 1 + \cdots + 1}^{n}$ for $n \geq 0$ and by $\varphi(-n) = -\varphi(n)$). If φ is injective, it identifies $\mathbb{Z}$ with a subring of K; then K also contains the field of fractions $\mathbb{Q}$, of $\mathbb{Z}$. In this case we say that K is *of characteristic* 0. If φ is not injective, its kernel is an ideal $p\mathbb{Z}$ where $p > 0$; then $\mathbb{Z}/p\mathbb{Z}$ is identified with a subring of K;

thus $\mathbb{Z}/p\mathbb{Z}$ is an integral domain (in fact, a field) from which it follows that p is a prime number. We say, in this case, that K is *of characteristic* p. From here on, we write $\mathbb{F}_p$ for $\mathbb{Z}/p\mathbb{Z}$.

Remark 1.7.1. The subfield, $\mathbb{Q}$, or $\mathbb{F}_p$, of K is the smallest subfield of K; it is called the *prime subfield* of K. For every prime number p there exist fields of characteristic p, e g. $\mathbb{F}_p$.

Proposition 1.7.2. *If K is a field of characteristic $p \neq 0$, then $px = 0$ for every $x \in K$ and $(x+y)^p = x^n + y^n$ for every $x, y \in K$.*

Proof. For $x \in K$, we have $p \cdot x = (p \cdot 1) \cdot x = 0 \cdot x = 0$. On the other hand, the binomial formula gives

$$(x+y)^p = x^p + y^p + \sum_{j=1}^{p-1} \binom{p}{j} x^j y^{p-j}.$$

The binomial coefficient $\binom{p}{j}$ is an integer; its value is $p!/[j!(p-j)!]$. Inasmuch as the prime p appears in the numerator but not in the denominator, $\binom{p}{j}$ is a multiple of p for $1 \leq j \leq p-1$. The intermediate terms in the expansion of $(x+y)^p$ thus vanish in a field of characteristic p. □

By induction one sees that $(x+y)^{p^n} = x^{p^n} + y^{p^n}$ for every $n \geq 0$.

Theorem 1.7.3. *Let K be a finite field. Set $q = \mathrm{card}(K)$. Then:*

(a) The characteristic of K is a prime p, K is a finite dimensional vector space of dimension s over $\mathbb{F}_p$, and $q = p^s$.

(b) The multiplicative group $K^\times$ is cyclic of order $q-1$.

(c) $x^{q-1} = 1$ for every $x \in K^\times$; $x^q = x$ for every $x \in K$.

Proof. (a): Since $\mathbb{Z}$ is infinite, K cannot be of characteristic 0. Thus K contains $\mathbb{F}_p$, p prime; in fact K is a vector space over $\mathbb{F}_p$, whose dimension s must be finite — otherwise K would be an infinite field. As a vector space, K is isomorphic to $(\mathbb{F}_p)^s$, so K contains p^s elements.
(b); Follows from Theorem 1.6.1.
(c): An immediate consequence of (b). □

Example 1.7.4. Let us interpret (b) for the case of $\mathbb{F}_p$, p prime. There exists an integer $x \in \mathbb{Z}$ such that $0 < x \leq p-1$ and such that every integer y which is not a multiple of p is congruent modulo p to a power of x. Such an x is called a *primitive root modulo* p. The problem of finding primitive roots modulo p is by no means trivial. For instance there are $\varphi(6) = 2$ roots primitive modulo 7; they are 3 and 5 (one sees that $1^2 \equiv 6^2 \equiv 1 \bmod 7$ and $2^3 \equiv 4^3 \equiv 1 \bmod 7$, 3 and 5 are the only other possibilities).

Remark 1.7.5. (a) and (c) imply that a finite field K with q elements is the set of roots of the polynomial $X^q - X$ (which has exactly q roots). One can show that two finite fields with q elements are isomorphic. We write $\mathbb{F}_q$, unambiguously for a field with q elements.

As an exercise we are going to digress in order to prove the following elegant theorem which concerns diophantine equations over a finite field.

Theorem 1.7.6 (Chevalley)**.** *Let K be a finite field and let $F(X_1, \ldots, X_n)$ be a homogeneous polynomial of degree d over K. Suppose $d < n$. Then there exists a point $(x_1, \ldots, x_n) \in K^n$ distinct from the origin $(0, \ldots, 0)$ such that $F(x_1, \ldots, x_n) = 0$.*

Proof. Let us write q for $\mathrm{card}(K)$ and p for the characteristic of K (so $q = p^s$). Let $V \subset K^n$ be the set of zeros of F, i.e. the points $(x_1, \ldots, x_n) \in K^n$ such that $F(x) = 0$ (we use, hereafter, the symbol x to stand for a point $(x_1, \ldots, x_n) \in K^n$). According to Theorem 1.7.3, (c), $F(x)^{q-1} = 0$ for $x \in V$ and $F(x)^{q-1} = 1$ for $x \in K^n \setminus V$. Thus the polynomial $G(x) = F(x)^{q-1}$ is the *characteristic function of* $K^n \setminus V$ with values in $\mathbb{F}_p$. The number modulo p of points of $K^n \setminus V$ will thus be given by the sum $\sum_{x \in K^n} G(x)$. We are going to calculate this sum and show that it is zero. It will follow that $\mathrm{card}(K^n \setminus V)$ is a multiple of p; inasmuch as $\mathrm{card}(K^n) = q^n = p^{ns}$ is also a multiple of p, $\mathrm{card}(V)$ will also have to be a multiple of p. Certainly V contains the origin, so if $p \mid \mathrm{card}(V)$, V necessarily contains other points, $p \geq 2$. Thus, to prove Theorem 1.7.6 it suffices to show that $\sum_{x \in K^n} G(x) = O \in \mathbb{F}_p$. Now, to calculate $\sum_{x \in K^n} G(x)$, wc observe that the polynomial G is a linear combination of monomials $M_\alpha(X) = X_1^{\alpha_1} \cdots X_n^{\alpha_n}$. To determine $\sum_{x \in K^n} G(x)$ it suffices to calculate

$$\sum_{x \in K^n} M_\alpha(x) = \sum_{x \in K^n} x_1^{\alpha_1} \cdots x_n^{\alpha_n} = (\sum_{x_1^K} x_1^{\alpha_1}) \cdots (\sum_{x_n^K} x_n^{\alpha_n}).$$

The problem reduces to that of calculating sums of the form $\sum_{z \in K} z^\beta, (\beta \in \mathbb{N})$.

(a) For $\beta = 0$, $z^\beta = 1$ for all $z \in K$. Consequently, $\sum_{x \in K} z^\beta = \sum_{x \in K} 1 = q = 0$.

(b) For $\beta > 0$, the term 0^β is 0, so the sum reduces to $\sum_{x \in K^\times} z^\beta$. $K^\times$ is a cyclic group of order $q - 1$ (Theorem 1.7.3 b). Let ω generate $K^\times$. Then $\sum_{x \in K^\times} z^\beta = \sum_{j=0}^{q-2} \omega^{\beta j}$ which is the sum of a geometric progression. Thus:

   (i) If $\omega^\beta \neq 1$, i.e. if β is not a multiple of $q - 1$, then

$$\sum_{j=0}^{q-2} \omega^{\beta j} = \frac{\omega^{\beta(q-1)} - 1}{\omega^\beta - 1} = 0,$$

since $\omega^{q-1} = 1$.

(ii) If $\omega^\beta = 1$, i.e. if β is a multiple of $q-1$, then

$$\sum_{j=0}^{q-2} \omega^{\beta j} = q - 1.$$

If follows from (a), (bi), and (bii) that $\sum_{x \in K^n} x_1^{\alpha_1} \cdots x_n^{\alpha_n}$ vanishes unless all the a_i's are non-zero and multiples of $(q-1)n$. However, since $G = F^{q1}$, G has degree $(q-1)d$ and $(q-1)d < (q-1)n$ by assumption. Thus $\sum_{x \in K^n} M_\alpha(x) = 0$ for every monomial $M_\alpha(X)$ which appears in G with a non-zero coefficient. Therefore, $\sum_{x \in K^n} G(x) = 0$. We have seen that this relation implies the theorem. □

Remark 1.7.7. Let us remark that it would have been sufficient, in place of the assumption that F was homogeneous, to have considered F with no constant term. Naturally, the strict inequality $d < n$ between the degree and the number of variables is essential. For example, the *norm* of $\mathbb{F}_{q^n}$ to $\mathbb{F}_q$, (cf. Section 2.6) is a homogeneous polynomial of degree n in n variables over $\mathbb{F}_p$, with no non-trivial zero.

Example 1.7.8. A quadratic form in three variables over a finite field "represents zero" (i. e. has a non-trivial zero). Passing from K^3 to the projective plane $P_2(K)$, this means that a *conic* over K contains a point rational over K (i.e. whose coordinates may be chosen in K). The example of the conic $X^2 + Y^2 + Z^2 = 0$ over $\mathbb{R}$ (respectively $X^2 + Y^2 - 3Z^2 = 0$ over $\mathbb{Q}$; in order to see that $X^2 + Y^2 - 3Z^2 = 0$ has no non-trivial solution in $\mathbb{Q}$, it suffices to consider the case where x, y, z are relatively prime integers and then to reduce mod 4) shows that we are not dealing with a property common to all fields.

Chapter 2

Integral elements over a ring; algebraic elements over a field

Among the complex numbers those which will concern us in this book are the so-called *algebraic numbers*, that is, those which satisfy an equation of the form

$$x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 = 0,$$

where the coefficients are rational numbers. When the coefficients are integers ($a_i \in \mathbb{Z}$) the algebraic number x is called an *algebraic integer*. Thus $\sqrt{2}$, $\sqrt{3}$, i, $e^{2i\pi/5}$ are algebraic integers. It is not a priori clear that sums or products of algebraic numbers (respectively algebraic integers) are again algebraic numbers (respectively algebraic integers). Consider, for example, $x = \sqrt{2}+\sqrt{3}$. Squaring, one obtains $x^2 = 2+3+2\sqrt{6}$ adding and shifting across the equal sign gives $x^2 - 5 = 2\sqrt{6}$: again a squaring operation yields $(x^2-5)^2 = 24$, which shows that x is an algebraic integer. The reader will have to exert himself to show that $\sqrt[3]{5}+\sqrt[3]{7}$ is an algebraic integer and will be convinced that the sequence of steps which leads to a proof that this number is algebraic may not be easily generalised. In order to overcome this difficulty the algebraists of the nineteenth century, Dedekind in particular, had the idea of "linearising" the problem, which means that they introduced the notion of module. We will begin with some results concerning modules. Considering modules over commutative rings (rather than over $\mathbb{Z}$ or $\mathbb{Q}$) will not require an extra effort and will be quite useful later. We will begin with the general case of integral elements over a ring and then specialise to algebraic elements over a field.

2.1 Integral elements over a ring

Theorem 2.1.1. *Let R be a ring, A a subring of R, and x an element of R. The following statement are equivalent:*

(a) There exist $a_0, \ldots, a_n \in A$ such that

$$x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 = 0 \tag{2.1.2}$$

(i.e. x is a root of a monic polynomial with coefficients in A).

(b) The ring $A[x]$ is an A-module of finite type.

(c) There exists a subring B of R which contains A and x and which is an A-module of finite type.

Proof. (a) $\Rightarrow$ (b): Call M the A-submodule of R generated by $1, x, \ldots, x^n - 1$. By (a) $x^n \in M$. Multiplying (2.1.2) by x^j, we obtain $x^{n+j} = -a_{n-1}x^{n+j-1} - \cdots - a_0 x^j$. In fact, induction on j implies that $x^{n+j} \in M$, for all $j \geq 0$. As $A[x]$ is the A-module generated by the $x^k (k \geq 0)$, we see that $A[x] = M$.
(b) $\Rightarrow$ (c): Thiis clear.
(c) $\Rightarrow$ (a): Let $(y_1, \ldots, y_n)$ be a finite set of generators for B as a module over A, i.e. $B = Ay_1 + \cdots + Ay_n$. Since $x \in B$ and since B is a subring of R, it follows that $xy_i \in B$ for all $i = 1, \ldots, n$. Therefore,

$$xy_i = \sum_{j=1}^{n} a_{ij} y_j = 0, \quad \text{for any} \quad i = 1, \ldots, n, \quad a_{ij} \in A, \quad 1 \leq i, j \leq n.$$

This means that

$$\sum_{j=1}^{n} (\delta_{ij} x - a_{ij}) y_j = 0, \quad i = 1, \ldots, n.$$

Consider this system of n homogeneous linear equations in $(y_1, \ldots, y_n)$. Write d for the determinant $\det(\delta_{ij} x - a_{ij})$. The calculation leading to Cramer's rule shows that $dy_i = 0$ for all i. This means that $db = 0$ for all $b \in B$; in particular, $d \cdot 1 = 0$, so $d = 0$. But d is clearly a monic polynomial in x, since the highest order term appears in the expansion of the product $\prod_{i=1}^{m}(x - a_{ii})$ of the entries on the principal diagonal. Thus (c) implies (a). □

Definition 2.1.3. Let R be a ring and let A be a subring of R. An element x of R is said to be *integral* over A if it satisfies the equivalent conditions (a), (b), and (c) of Theorem 2.1.1. Let $P \in A[X]$ be a monic polynomial such that $P(x) = 0$ ((a) implies that such a polynomial exists). The relation $P(x) = 0$ is called an *equation of integral dependence* of x over A.

Example 2.1.4. The element $x = \sqrt{2}$ of $\mathbb{R}$ is integral over $\mathbb{Z}$. The relation $x^2 - 2 = 0$ is an equation of integral dependence.

Proposition 2.1.5. *Let R be a ring, A a subring of R, and let $(x_i)_{1 \leq i \leq n}$ be a finite set of elements of R. If, for all i, x is integral over $A[x_1, \ldots, x_{n-1}]$ (in particular if all the x_i's are integral over A), then $A[x_1, \ldots, x_n]$ is an A-module of finite type.*

Proof. We argue by induction on n. For $n = 1$, we have a repeat of assertion (b) of Theorem 2.1.1. Assume that $B = A[x_1, \ldots, x_{n-1}]$ is an A-module of finite type. Then $B = \sum_{j=1}^{p} Ab_j$. The case $n = 1$ implies that $A[x_1, \ldots, x_n] = B[x_n]$ is a B-module of finite type. Write $B[x_n J = \sum_{k=1}^{q} Bc_k$. Then

$$A[x_1, \ldots, x_n] = \sum_{k=1}^{q} Bc_k = \sum_{k=1}^{q} (\sum_{j=1}^{p} Ab_j)c_k = \sum_{j,k} Ab_j c_k.$$

Thus $(b_j c_k)$ is a finite set of generators for $A[x_1, \ldots, x_n]$ as a module over A. □

Corollary 2.1.6. *Let R be a ring, A a subring of R, x and y elements of R which are integral over A. Then $x + y$, $x - y$, and xy are integral over A.*

Proof. Clearly $x + y$, $x - y$, and $xy \in A[x, y]$. According to Proposition 2.1.5 $A[x, y]$ is an A-module of finite type. According to part (c) of Theorem 2.1.1, $x + y$, $x - y$, and xy are integral over A. □

Corollary 2.1.7. *Let R be a ring and let A be a subring of R. The set A' of elements of R which are integral over A is a subring of R which contains A.*

Proof. Corollary 2.1.6 implies that A' is a subring of R. We have $A \subset A'$, since, if $a \in A$, a is a root of the monic polynomial $P(X) = X - a$, which has coefficients in A. □

Definition 2.1.8. Let R be a ring, A a subring of R. The ring A' of elements of R which are integral over A is called the *integral closure of A in R*. Let A be an integral domain and let K be its field of fractions. The integral closure of A in K is called the *integral closure* of A. Let B be a ring and A a subring of B. We say that B is *integral over A* if every element of B is integral over A (i.e. if the integral closure of A in B is B itself).

Proposition 2.1.9 (Transitivity)**.** *Let C be a ring, B a subring of C, and A a subring of B. If B is integral over A and if C is integral over B, then C is integral over A.*

Proof. Let $x \in C$. Then x is integral over B, so there is an equation of integral dependence $x_n + b_{n-1}x^{n-1} + \cdots + b_0 = 0$ with $b_i \in B, i = 0, \ldots, n-1$. Put $B' = A[b_0, \ldots, b_{n-1}]$. Then x is integral over B'. As B is integral over A, the b_i are integral over A. Therefore Proposition 2.1.5 implies that $B'[x] = A[b_0, \ldots, b_{n-1}, x]$ is an A-module of finite type. By part (c) of Theorem 2.1.1, x is integral over A. Thus C is integral over A. □

Proposition 2.1.10. *Let B be an integral domain and A a subring of B such that B is integral over A. In order that B be a field it is necessary and sufficient that A be a field.*

Proof. Suppose that A is a field and let $b \in B, b \neq 0$. Then $A[b]$ is a finite dimensional vector space over A (part (b) of Theorem 2.1.1). On the other hand $y \mapsto by$ is an A-linear transformation of $A[b]$. It is injective since $A[b]$ is

an integral domain and since $b \neq 0$. Therefore, it is surjective. There exists $b' \in A[b]$ such that $bb' = 1$. This means that, for any $b \in B \setminus (0)$, b is invertible in B, so B is a field [1].

Conversely, suppose that B is a field. Let $a \in A \setminus (0)$. Then a has an inverse $a^{-1} \in B$ which satisfies an equation of integral dependence

$$a^{-n} + a_{n-1}a^{-n+1} + \cdots + a_1 a^{-1} + a_0 = 0, \quad a_i \in A.$$

Multiplying by a^{n-1}, we obtain

$$a^{-1} = -(a_{n-1} + \cdots + a_1 a^{n-2} + a_0 a^{n-1}),$$

which shows that $a^{-1} \in A$. Thus A is a field. □

2.2 Integrally closed domains

Definition 2.2.1. A ring A is said to be *integrally closed* if it is an integral domain and if it is its own integral closure.

In other words, A is integrally closed if every element x of the field of fractions K of A which is integral over A belongs to A.

Example 2.2.2. Let A be an integral domain and let K be its field of fractions. Then the integral closure A' of A (i.e. the integral closure of A in K) is integrally closed. This follows from the fact that the integral closure of A' is integral over A', therefore over A (Proposition 2.1.9). It therefore equals A'.

Example 2.2.3. Every PID is integrally closed.

Proof. By definition a PID is an integral domain. Let x be an element of the field of fractions of A which is integral over A. Let

$$x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 = 0 \quad (a_I \in A) \tag{2.2.4}$$

be an integral dependence equation for x over A. Write $x = a/b$ with a and b relatively prime elements of A. Substitute in (2.2.4) and multiply through by b^n to obtain

$$a^n + b(a_{n-1}a^{n-1} + \cdots + a_1 a b^{n-2} + a_0 b^{n-1}) = 0.$$

Thus b divides a^n. As b is relatively prime to a, repeated application of Euclid's lemma shows that b divides a. Therefore, b is a unit in A. Thus, $x = a/b \in A$ and A is integrally closed. □

Remark 2.2.5. One may observe that only the multiplicative properties of PID have been used (relative primeness, Euclid's lemma). The same argument thus shows that every UFD is integrally closed.

[1] The same reasoning, involving the mapping $y \mapsto by$, allows one to conclude that any finite integral domain is a field.

2.3 Algebraic elements over a field. Algebraic extensions

Definition 2.3.1. Let R be a ring and K a subfield of R. An element $x \in R$ is said to be *algebraic* over K if there exist elements $a_0, \cdots, a_n \in K$, not all of which are zero, such that $a_n x^n + \cdots + a_1 x + a_0 = 0$.

Equivalently, the monomials $(x^j)_{j\in\mathbb{N}}$ are linearly dependent over K. An element of R which is not algebraic over K is called *transcendental* over K; i.e. x is transcendental over K if and only if the monomials $(x^j)_{j\in\mathbb{N}}$ are linearly independent over K.

In the relation of Definition 2.3.1, we may assume that $a_n \neq 0$. In this case $_n^{-1} \in K$; multiplying through by a_n^{-1} we obtain an equation of integral dependence. Therefore:

$$\textit{Over a field, algebraic } = \textit{ integral.} \tag{2.3.2}$$

We may thus apply the theory of integral elements. For example, for $K \subset R$ and $x \in R$, Theorem 2.1.1, (b) asserts:

$$x \textit{ algebraic over } K \Leftrightarrow [K[x] : K] \textit{ finite.} \tag{2.3.3}$$

We say that a ring R containing a field K is algebraic over K if every element of R is algebraic over K. If R is a field, then R is called an *algebraic extension* of K.

Given a field L and a subfield K of L, we call the dimension $[L : K]$ the *degree* of L over K. In this context Theorem 2.1.1, (c) has the following interpretation:

If the degree of L over K is finite, L is an algebraic extension of K. (2.3.4)

Any extension field of finite degree over $\mathbb{Q}$, is called an *algebraic number field* (or simply a *number field*).

Proposition 2.3.5. *Let K be a field, L an algebraic extension of K, and M an algebraic extension of L. Then M is an algebraic extension of K. Furthermore, $[M : K] = [M : L][L : K]$ ("multiplicativity of degrees").*

Proof. The first assertion is a special case of Proposition 2.1.9. Moreover, if $(x_i)_{i,\in I}$ is a basis of L over K and $(y_i)_{i\in J}$ is a basis for M over L, then $(x_i y_j)_{(i,j)\in I\times J}$ is a basis for M over K. As in Proposition 2.1.5 we see that $(x_i y_j)_{(i,j)\in I\times J}$ generates M over K. A relation $\sum a_{ij} x_i y_j = 0$ with $a_i \in K$ entails $\sum(\sum a_{ij} x_i) y_j = 0$, whence $\sum a_{ij} x_i = 0$ for all j (since $\sum a_{ij} x_i \in L$), and consequently $a_{ij} = 0$ for all $(i, j) \in I \times J$. This proves that $[M : K] = [M : L][L : K]$. □

Proposition 2.3.6. *Let R be a ring and K a subfield of R. Then:*

1. *The set K' of elements of R algebraic over K is a subring of R containing K.*

2. If R is an integral domain, K' is a subfield of R.

Proof. (1) is a special case of Corollary 2.1.7, and (2) follows from Proposition 2.1.10. □

Now we study the elements algebraic over a field in greater detail. Let R be a ring, K a subfield of R, and let x be an element of R. Write $K[X]$ for the ring of polynomials in one variable over K. There exists a unique homomorphism $\varphi\colon K[X] \to R$ such that $\varphi(X) = x$ and such that $\varphi(a) = a$ for all $a \in K$. The image of φ is $K[x]$. The definition of algebraic element may be reformulated as follows:

$$\textit{An element } x \textit{ is algebraic over } K \Leftrightarrow \ker(\varphi) \neq (0). \tag{2.3.7}$$

Proof. If x is transcendental over K, then obviously $\ker(\varphi) = (0)$. In any case the ideal $\ker(\varphi)$ is a principal ideal $(F(X))$ (since $K[X]$ is a PID). In the case that x is algebraic over K, it is generated by a non-zero polynomial $F(X)$. □

We may assume that $F(X)$ is monic, since K is a field. $F(X)$ is then uniquely determined by K and x; we call it the *minimal polynomial* of x over K. Its properties are as follows:

$$\begin{gathered}\textit{Let } F(X) \textit{ be the minimal polynomial of } x \textit{ over } K. \textit{ Let } G(X) \in K[X].\\ G(x) = 0 \textit{ if and only if } F(X) \textit{ divides } G(X) \textit{ in } K[X].\end{gathered} \tag{2.3.8}$$

Passing to the residue ring, we obtain a *canonical isomorphism*:

$$K[X]/F(x)K[X] \xrightarrow{\sim} K[x]. \tag{2.3.9}$$

With the same notations, suppose now that x is algebraic over K and let $F(X)$ be its minimal polynomial. Applying (2.3.8) and Proposition 2.1.10, we obtain the equivalence of the following statements:

$$K[X] \textit{ is a field } \Leftrightarrow K[x] \textit{ is an integral domain } \Leftrightarrow F(X) \textit{ is irreducible.} \tag{2.3.10}$$

On the other hand, if K is a field and $F(X) \in K[X]$ is irreducible, then $K[X]/F(X)K[X]$ is a field containing K and, writing x for the projection of $X \in K[X]$ into this field, we have $F(x) = 0$. Thus $X - x$ divides $F(X)$ in the field $K[x]$. More generally:

Proposition 2.3.11. *Let K be a field and let $P(X) \in K[X]$ be a nonconstant polynomial. There exists an algebraic extension of finite degree K' of K such that $P(X)$ factors in $K'[X]$ into a product of polynomials of degree one (linear polynomials).*

Proof. We argue by induction on the degree $\deg P$. There is nothing to prove in the case $\deg P = 1$. Let $F(X)$ be an irreducible factor of $P(X)$. We have just seen that there exists an extension K'' of finite degree over K (e.g. $K[X]/F(X)K[X]$) containing an element x such that $X - x$ divides $F(X)$ in

$K''[X]$. Thus $P(X) = (X - x)P_1(X)$ with $P_1(X) \in K''[X]$. According to the induction hypothesis $P_1(X)$ factors into a product of linear polynomials in an extension K' of finite degree over K''. By Proposition 2.3.5, K'' is of finite degree over K, and $P(X)$ is a product of linear polynomials in $K'[X]$. □

Remark 2.3.12 (*Algebraically closed fields*). A field K is said to be *algebraically closed* if every non-constant polynomial $P(X) \in K[X]$ may be expressed as a product of linear factors, all lying in $K[X]$. For this, as follows by induction on the degree of the polynomial, it suffices that even non-constant polynomial have a root in K. Extending Proposition 2.3.11 by means of Zorn's lemma, one may show that any field is imbeddable in an algebraically closed field (*Steiniz's theorem*).

One may prove, by means of the techniques of mathematical analysis and in many different ways, that the field $\mathbb{C}$ of complex numbers is algebraically closed (*Fundamental theorem of algebra*). We will give in Appendix A a more algebraic proof, which will involve no analysis beyond the most elementary properties of the real numbers. We shall not need more than this.

2.4 Conjugate elements, conjugate fields

Given two fields L and L' both containing a field K we call K-isomorphism of L on L' any isomorphism $\varphi\colon L \to L'$ such that $\varphi(a) = a$ for all $a \in K$. In this case we say that L and L' are *K-isomorphic*, or (if they are algebraic over K) we say that they are *conjugate* over K. Given two extensions L and L' of K, we say that two elements $x \in L$ and $x' \in L'$ are *conjugate* over K if there exists a K-isomorphism $\varphi\colon K(x) \to K(x')$ such that $\varphi(x) = x'$. Such a φ is, of course, unique. The existence of a φ means that either x and x' are both transcendental over K or both are algebraic over K with the same minimal polynomial (cf 2.3.8).

Example 2.4.1. Let $F(X)$ be an irreducible polynomial of degree n over K and let $x_1, \cdots, x_n$ be its roots in an extension K' of K (Proposition 2.3.11). Then the x_i's are pairwise conjugate over K (2.3.9), and the fields $K[x_i]$ are also pairwise conjugate.

Lemma 2.4.2. *Let K be a field of characteristic 0 or a finite field, let $F(X) \in K[X]$ be a monic irreducible polynomial, and let $F(X) = \prod_{i=1}^{n}(X - x_i)$ be its decomposition into a product of linear factors in an extension K' of K (Proposition 2.3.11). Then the n roots $x_1, \cdots, x_n$ of $F(X)$ are distinct.*

Proof. We resort to contradiction. Suppose $F(X)$ has a root in common with its derivative $F'(X)$, thus $F(X)$ divides $F'(X)$ (2.3.7). Since $\deg F' < \deg F$, this means that $F'(X)$ is the zero polynomial. However, $F(X) = X^n + a_{n-1}X^{-1} + \cdots a_0$, $(a_i \in K)$ and

$$F'(X) = nX^{m-1} + (n-1)a_{n-1}X^{n-2} \cdots + a_1.$$

Thus $n \cdot 1 = 0$, $j \cdots a$, $j = 1, \cdots, n-1$, which is impossible in characteristic 0. In characteristic $p \neq 0$, these relations imply that p divides n and that $a_j = 0$ for all j not divisible by p (recall that p is a prime number). Thus $F(X)$ is of the form

$$F(X) = X^{qp} + b_{q-1}X^{(q-1)p} + \cdots b_1 X^p + b_0 \quad (b_i \in K).$$

If each b_i is a pth power, i.e. $b_i = c_i^p$ with $c_i \in K$, then

$$F(X) = (X^q + b_{q-1}X^{q-1} + \cdots + c_0)^p \quad (1.7.2),$$

and $F(X)$ is not irreducible. But, if K is a finite field with its characteristic $p \neq 0$, the mapping $x \mapsto x^p$ of K into K is injective (since $x^p = y^p$ implies $x^p - y^p = 0$, so $(x-y)^p = 0$ which implies $x - y = 0$); it is thus surjective, since K is finite. Therefore, $F(X)$ is not irreducible and we have a contradiction. □

Remark 2.4.3. The fields K of characteristic $p \neq 0$ for which $x \mapsto x^p$ is surjective (i.e. for which every element of K is a pth power) are called perfect fields. We have just shown that finite fields are perfect. By convention, fields of characteristic 0 are also considered perfect. The preceding lemma is true for K any perfect field (and our proof works in this more general case). The field $\mathbb{F}_p(T)$ of rational functions in one variable over $\mathbb{F}_p$ is not perfect, inasmuch as the variable T is not a pth power in $\mathbb{F}_p(T)$.

Theorem 2.4.4. *Let K be afield of characteristic 0 or a finite field, let K' be a finite extension of K of degree n, and let C be an algebraically closed field containing K. Then there exist n distinct K-isomorphisms of K' into C.*

Proof. Our assertion is true for any extension field K' of K which is of the form $K[x]$ with $x \in K'$. In fact, the minimal polynomial $F(X)$ of x over K is then of degree n. It has n roots $x_1, \ldots, x_n$ in C, all of which are distinct according to Lemma 2.4.2. For any $i = 1, \ldots, n$ we have then a K-isomorphism $\sigma_i \colon K' \to C$ such that $\sigma_i(x) = x_i$.

We continue by induction on the degree n of K'. Let $x \in K'$ and consider the fields $K \subset K[x] \subset K'$ and put $q = [K[x] : K]$. We may assume $q > 1$. We have seen that there are q distinct K-isomorphisms $\sigma_1, \ldots, \sigma_q$ of $K[x]$ into C. As $K[\sigma_i(x)]$ and $K[x]$ are isomorphic, it is possible to construct an extension K_i' of $K[\sigma_i(x)]$ and an isomorphism $\tau_i \colon K' \to K_i'$ which extends σ_i. Clearly $K[\sigma_i(x)]$ is a field of characteristic 0 or a finite field. Since

$$[K_i' : K[\sigma_i(x)]] = [K' : K[x]] = \frac{n}{q} < n,$$

the induction hypothesis implies that there are $\frac{n}{q}$ distinct $K[\sigma_i(x)]$-isomorphisms θ_{ij} of K_i' into C. Therefore, the n composed mappings $\theta_{ij} \circ \tau$ provide $q \cdot \frac{n}{q} = n$ K-isomorphisms of K' into C. They are distinct since for $i \neq i'$ and $\theta_{ij} \circ \tau$ and $\theta_{i'j'} \circ \tau_i'$ differ on $K[x]$ if $i \neq i'$, and, if $i = i'$, θ_{ij} and $\theta_{ij'}$ differ on $K_{i'}$. □

Remark 2.4.5. Theorem 2.4.4 extends to the case of a perfect field K. One shows that any algebraic extension of a perfect field (in particular $K[\sigma_i(x)]$) is a perfect field. The rest of the proof remains unchanged.

Corollary 2.4.6 (*Primitive element theorem*)**.** *Let K be a finite field or a field of characteristic 0. Let K' be an extension of K of finite degree n. Then there exists an element x of K' (called a* primitive element*) such that $K' = K[x]$.*

Proof. If K is finite, K' is finite and its multiplicative group $K'^{\times}$ is comprised of the powers of a single element x (Theorem 1.7.3, (b)). Thus $K' = K[x]$.

Suppose that K is of characteristic 0 and thus an infinite field. According to Theorem 2.4.4 there are n K-isomorphisms σ_i, of K''' into an algebraically closed field C containing K. For $i \neq j$ the equation $\sigma_i(y) = \sigma_j(y)(y \in K')$ defines a subset V_{ij} of K', which is clearly a K-subspace of the vector space K' and which is distinct from K' since $\sigma_i \neq \sigma_j$. Since K is infinite, linear algebra shows that the union of the V_{ij} is strictly contained in K'. Take x outside this union: $x \in K' \setminus (\cup V_{ij})$. The $\sigma_i(x)$ are then pairwise distinct, so that the minimal polynomial $F(X)$ of x over K has at least n distinct roots (the $\sigma_i(x)$) in C. Therefore, $\deg F \geq n$, i.e. $[K[x] : K] \geq n$. Since $K[x] \subset K'$ and since $[K' : K] = n$, we conclude that $K' = K[x]$. □

2.5 Integers in quadratic fields

We pause a moment from the development of the general theory to give an example.

Definition 2.5.1. Any extension field of degree 2 over the field $\mathbb{Q}$ of rational numbers is called a *quadratic field.*

If K is a quadratic field, any element $x \in K \setminus \mathbb{Q}$, is of degree 2 over $\mathbb{Q}$, thus is a primitive element of K (i.e. $K = \mathbb{Q}[x]$ and (l, x) is a basis of K over $\mathbb{Q}$). Let $F(X) = X^2 + bX + c$ $(b, c \in \mathbb{Q})$ be the minimal polynomial of such an element $x \in K$. Solving the quadratic equation $x^2 + bx + c = 0$ gives $2x = -b \pm \sqrt{b^2 - 4c}$. Thus $K = \mathbb{Q}(\sqrt{b^2 - 4c})$ [2] Now $b^2 - 4c$ is a rational number $\frac{u}{v} = \frac{uv}{v^2}$ with $u, v \in \mathbb{Z}$. One sees that $K = \mathbb{Q}(\sqrt{uv})$ with $u, v \in \mathbb{Z}$. In fact, one sees that it is possible to write $K = \mathbb{Q}(\sqrt{d})$ where d is a square-free integer (d is plus or minus a product of distinct primes). Thus we have proved:

Proposition 2.5.2. *Every quadratic field is of the form $\mathbb{Q}(\sqrt{d})$, where d is a square-free integer.*

The element $\sqrt{d}$ is a root of the irreducible polynomial $X^2 - d$. This element $\sqrt{d}$ has a conjugate in K, namely $-\sqrt{d}$. There exists an automorphism σ of K which sends $\sqrt{d}$ to $-\sqrt{d}$ (2.4). Any element of K is of the form $a + b\sqrt{d}$ with $a, b \in \mathbb{Q}$. We have

$$\sigma(a + b\sqrt{d}) = a - b\sqrt{d}. \tag{2.5.3}$$

[2] By $\sqrt{b^2 - 4c}$ we mean one of the two elements of K whose square is $b^2 - 4c$.

Let us study the ring A of integers of K, i.e. the set of $x \in K$ which are integral over $\mathbb{Z}$ (Corollary 2.1.7). If $x \in A$, $\sigma(x)$ is a root of the same equation of integral dependence as x, so $\sigma(x) \in A$. We have then that $x+\sigma(x) \in A$ and $x \cdot \sigma(x) \in A$. But, if $x = a + b\sqrt{d}$ with $a, b \in \mathbb{Q}$, then, according to (2.5.3),

$$x + \sigma(x) = 2a \in \mathbb{Q} \quad \text{and} \quad x \cdot \sigma(x) = a^2 - db^2 \in \mathbb{Q}.$$

Since $\mathbb{Z}$ is a PID and hence integrally closed (Example 2.2.3), we see that

$$2a \in \mathbb{Z} \quad a^2 - db^2 \in \mathbb{Z}. \tag{2.5.4}$$

The conditions (2.5.4) are necessary in order that $x = a + b\sqrt{d}$ be integral over $\mathbb{Z}$; they are also sufficient since x is a root of

$$X^2 - 2aX + a^2 - db^2 = 0.$$

According to (2.5.4), $(2a)^2 - d(2b)^2 \in \mathbb{Z}$. Since $2a \in \mathbb{Z}$, we have $d(2b)^2 \in \mathbb{Z}$ too. On the other hand, d is square-free, so, if $2b$ were not an integer, its denominator would have to include a prime factor p. This prime factor would have to appear as p^2 in the denominator of $(2b)^2$, and the multiplication by d would fail to send it into $\mathbb{Z}$. We may conclude that $2b \in \mathbb{Z}$.

In brief, we may take $a = \frac{u}{2}, b = \frac{v}{2}$ with $u, v \in \mathbb{Z}$. Condition (2.5.4) becomes:

$$u^2 - dv^2 \in 4\mathbb{Z}. \tag{2.5.5}$$

If v is even, (2.5.5) shows that u is even too. In this case, $a, b \in \mathbb{Z}$. If v is odd, then $v^2 \equiv 1 \bmod 4$. The possibilities of $u^2 \bmod 4$ are 0 and 1 (write down the table of squares mod 4 to be sure); since d is square-free, it is not a multiple of 4. Necessarily $u^2 \equiv 1 \bmod 4$ and $d \equiv 1 \bmod 4$. We have proved the following:

Theorem 2.5.6. *Let $K = \mathbb{Q}(\sqrt{d}))$ be a quadratic field with $d \in \mathbb{Z}$ square-free (therefore $\neq 0 \bmod 4$).*

(a) If $d \equiv 2$ or $d \equiv 3 \bmod 4$, the ring A of integers of K consists of all elements of the form $a + b\sqrt{d}$ with $a, b \in \mathbb{Z}$.

(b) If $d \equiv 1 \bmod 4$, A consists of all elements of the form $\frac{1}{2}(u + v\sqrt{d})$ with u and $v \in \mathbb{Z}$ of the same parity.

In the case that $d \equiv 2$ or $3 \bmod 4$, $(1, \sqrt{d})$ is a basis for A as a $\mathbb{Z}$-module. If $d \equiv 1 \bmod 4$, $(1, \frac{1}{2}(1 + \sqrt{d})$ is a $\mathbb{Z}$-module basis for A. Indeed, by (b), 1 and $\frac{1}{2}(1 + \sqrt{d})$ belong to A. Conversely, to show that $\frac{1}{2}(u + v\sqrt{d})$ (with $u, v \in \mathbb{Z}$ of the same parity) is a $\mathbb{Z}$-linear combination of 1 and $\frac{1}{2}(1 + \sqrt{d})$, one may reduce the problem to the case where u and v are even by subtracting $\frac{1}{2}(1 + \sqrt{d})$. In this case

$$\frac{1}{2}(u + vv\sqrt{d}) = (\frac{u}{2} - \frac{v}{2}) \cdot 1 + v \cdot \frac{1}{2}(1 + \sqrt{d}).$$

Wc conclude with some terminology. If $d > 0$, we say $\mathbb{Q}(\sqrt{d})$ is a *real quadratic field* (for there exists a subfield of R conjugate to $\mathbb{Q}(\sqrt{d})$ over $\mathbb{Q}$). If $d < 0$, then we say $\mathbb{Q}(\sqrt{d})$ is an *imaginary quadratic field.*

2.6 Norms and traces

(a) Review of linear algebra

Let A be a ring, E a *free* A-module of finite rank and let u be an endomorphism of E. In linear algebra one defines the *trace*, the *determinant*, and the *characteristic polynomial* of u. If a basis (e_i) of E has been chosen and if (a_{ij}) is the matrix for u with respect to this basis, then the trace, determinant, and characteristic polynomial of a are, respectively,

$$\mathrm{Tr}(u) = \sum_{i=1}^{n} a_{ii}, \quad \det(u) = \det(a_{ii}), \qquad \text{and } \det(X \cdot I_E - u) = \det(X\delta_{ij} - a_{ij}). \tag{2.6.1}$$

Remark 2.6.2. NB. These quantities are independent of the choice of basis.

The formulas (2.6.1) imply:

$$\begin{aligned} \mathrm{Tr}(u+u') &= \mathrm{Tr}(u) + \mathrm{Tr}(u'), \\ \det(uu') &= \det(u)\det(u'), \\ \text{and } \det(XI_E - u) &= X^n - (\mathrm{Tr}(u))X^{n-1} + \cdots + (-1)^n \det(u). \end{aligned} \tag{2.6.3}$$

(b) Norms and traces in an extension

Let B be a ring and let A be a subring of B such that B is a free A-module of finite rank n (for example, A can be a field and B a finite extension of degree n of A). For $x \in B$, multiplication m_x by x (i.e. $y \mapsto xy$) is an endomorphism of the A-module B.

Definition 2.6.4. We call *trace* (respectively, *norm*, *characteristic polynomial*) of $x \in B$, relative to B and A, the trace (respectively, determinant, characteristic polynomial) of the endomorphism m_x of multiplication by x.

The trace (respectively, norm) of x is denoted $\mathrm{Tr}_{B/A}(x)$ (respectively, $\mathrm{Nm}_{B/A}(x)$), or $\mathrm{Tr}(x)$ (respectively, $\mathrm{Nm}(x)$) when there is no fear of confusion. They are elements of A. The characteristic polynomial is a monic polynomial with coefficients in A.

For $x, x' \in B$ and $a \in A$ we have $m_x + m_{x'} = m_{x+x'}$, $m_x \circ m_{x'} = m_{xx'}$ and $m_{ax} = am_x$. Furthermore, the matrix of m_a, with respect to any basis for B over A, is the diagonal matrix in which all the diagonal entries are a. From formulas (2.6.1) and (2.6.3) we obtain:

$$\begin{gathered} \mathrm{Tr}(x+x') = \mathrm{Tr}(x) + \mathrm{Tr}(x'), \quad \mathrm{Tr}(ax) = a\,\mathrm{Tr}(x), \quad \mathrm{Tr}(a) = n \cdot a \\ \mathrm{Nm}(xx') = \mathrm{Nm}(x)\,\mathrm{Nm}(x'), \quad \mathrm{Nm}(a) = a^n, \quad \text{and} \quad \mathrm{Nm}(ax) = a^n\,\mathrm{Nm}(x). \end{gathered} \tag{2.6.5}$$

Proposition 2.6.6. *Let K be a field of characteristic 0 or a finite field, let L be an algebraic extension of degree n of K, let x be an element of L, and let*

$x_1, \ldots, x_n$ be the roots of the minimal polynomial of x over K (in a suitable extension of K; cf. Proposition 2.3.11), each one repeated $[L : K[x]]$ times. Then $\mathrm{Tr}_{L/K}(x) = x_1 + \cdots + x_n$, $\mathrm{Nm}_{K/K}(x) = x_1 \cdots x_n$. The characteristic polynomial of x, relative to L and K is $(X - x_1) \cdots (X - x_n)$.

Thus the characteristic polynomial is the $[L : K[x]]$th power of the minimal polynomial of x over K.

Proof. Let us first treat the case where x is a primitive element of L over K (cf. Corollary 2.4.6). Let $F(X)$ be the minimal polynomial of x over K. Then L is K-isomorphic to $K[X]/F(X)K[X]$ (formula 2.3.9), and $(1, x, \ldots, x^{n-1})$ is a basis for L over K. Let us put $F(X) = X^n + a_{n-1}X^{n-1} + \cdots + a_1 X + a_0$. The matrix of the endomorphism m_x with respect to this basis is

$$\begin{bmatrix} 0 & 0 & \ldots & 0 & -a_0 \\ 1 & 0 & \ldots & 0 & -a_1 \\ 0 & 1 & \ldots & 0 & \vdots \\ \vdots & 0 & \ddots & \vdots & \vdots \\ \vdots & \vdots & \ldots & 0 & -a_{n-2} \\ 0 & 0 & \ldots & 1 & -a_{n-1} \end{bmatrix}$$

The determinant of $X \cdot I_L - m_x$ is therefore

$$\det \begin{bmatrix} X & 0 & \ldots & 0 & a_0 \\ -1 & X & \ldots & 0 & a_1 \\ 0 & -1 & \ldots & 0 & \vdots \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ \vdots & \vdots & \ldots & X & a_{n-2} \\ 0 & 0 & \ldots & -1 & X + a_{n-1} \end{bmatrix}$$

Expanding this determinant as a polynomial in X, we obtain the characteristic polynomial of x, which is equal to the minimal polynomial $F(X)$ of x. By (2.6.3) $\mathrm{Tr}(x) = -a_{n-1}$ and $\mathrm{Nm}(x) = (-1)^n a_0$. Since x is primitive, $F(X) = (X - x_1) \cdots (X - x_n)$, equating coefficients we see that

$$\mathrm{Tr}(x) = x_1 + \cdots + x_n \quad \text{and} \quad \mathrm{Nm}(x) = x_1 \cdots x_n.$$

Consider now the general case, and put $r = [L : K[x]]$. It suffices to show that the characteristic polynomial $P(X)$ of x with respect to L and K is equal to the rth power of the minimal polynomial of x over K. Let $(y_i)_{i=1,\ldots,q}$ be a basis for $K[x]$ over K, and let $(z_j)_{j=1,\ldots,r}$ be a basis for L over $K[x]$; then $(y_i z_j)$ is a basis for L over K and $n = qr$ (Proposition 2.3.5). Let $M = (a_{ih})$ be the matrix for multiplication by x in $K[x]$ with respect to the basis (y_i): thus $xy_i = \sum_h a_{ih} y_h$. We have then

$$x(y_i z_j) = (\sum_h a_{ih} y_h) z_j = \sum_h a_{ih} (y_h z_j).$$

Ordering lexicographically the basis $(y_i z_j)$ of L over K, we see that the matrix M_1 for multiplication by x in L with respect to this basis takes the form of diagonal "tableau" of matrices

$$M_1 = \begin{bmatrix} M & 0 & \dots & 0 \\ 0 & M & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & M \end{bmatrix}$$

The matrix $X \cdot I - M_1$ thus consists of r diagonal blocks, each of the form $X \cdot I_q - M$. Consequently, $\det(X \cdot I_n - M_1) = (\det(X \cdot I_q - M))^r$. The left-hand side of the preceding equation is $P(X)$, and $\det(X \cdot I_q - M)$ is the minimal polynomial of x over K, according to the first part of the proof. □

In conclusion we present a result regarding traces and norms of integral elements.

Proposition 2.6.7. *Let A be an integral domain, K its field of fractions, L an extension of finite degree of K, and x an element of L integral over A. Assume K has characteristic 0. Then the coefficients of the characteristic polynomial $P(X)$ of x relative to L and K, in particular $\mathrm{Tr}_{L/K}(x)$ and $\mathrm{Nm}_{L/K}(x)$ are integral over A.*

Proof. We make use of Proposition 2.6.6. We have $P(X) = (X - x_1) \cdots (X - x_n)$; the coefficients of $P(X)$ are thus, up to a sign, sums of products of the x_i's. It suffices to show that the x_i's are integral over A (Corollary 2.1.6). But each x_i is a conjugate of x over K (Section 2.4), and there is a K-isomorphism $\sigma_i \colon K[x] \to K[x_i]$ such that $\sigma_i(x) = x_i$. Applying σ_i to an equation of integral dependence of x over A, we obtain an equation of integral dependence for x_i over A. □

Corollary 2.6.8. *Suppose, further, that A is integrally closed. Then the coefficients of the characteristic polynomial of x, in particular $\mathrm{Tr}_{L/K}(x)$ and $\mathrm{Nm}_{L/K}(x)$, are elements of A.*

Proof. By definition these coefficients are elements of K. By Proposition 2.6.7 they are integral over A. □

Remark 2.6.9. We remark that the quantities $x + \sigma(x)$ and $x \cdot \sigma(x)$ used in the discussion of quadratic fields (2.5) are the trace and the norm of x. We proved there (2.5.4) a special case of the above corollary.

2.7 Discriminant

Definition 2.7.1. Let B be a ring and let A be a subring of B such that B is a free A-module of finite rank n. For $(x_1, \dots, x_n) \in B^n$ we call the *discriminant* of the set $(x_1, \dots, x_n)$ the element of A defined by the relation

$$\mathrm{disc}(x_1, \dots, x_n) = \det(\mathrm{Tr}_{B/A}(x_i x_j)). \tag{2.7.2}$$

Proposition 2.7.3. *If $(y_1, \ldots, y_n) \in B^n$ is another set of elements of B such that $y_i = \sum_{j=1}^n a_{ij} x_j$ with $a_{ij} \in A$, then*

$$\operatorname{disc}(y_1, \ldots, y_n) = (\det(a_{ij}))^2 \operatorname{disc}(x_1, \ldots, x_n).$$

Proof.

$$\operatorname{Tr}(y_p y_q) = \operatorname{Tr}(\sum_{i,j} a_{pi} a_{qj} x_i x_j) = \sum_{i,j} a_{pi} a_{qj} \operatorname{Tr}(x_i x_j).$$

This gives the matrix equation: $(\operatorname{Tr}(y_p y_q)) = (a_{pi})(\operatorname{Tr}(x_i x_j)) \cdot {}^t(a_{qj})$ (where ${}^t M$ denotes the transpose of the matrix M). To complete the proof it suffices to take determinants. □

Proposition 2.7.3 implies that the discriminants of bases for B over A are *associates* in A; i.e. the matrix (a_{ij}) which expresses one basis in terms of another has an inverse with entries in A. Therefore both $\det(a_{ij})$ and $\det(a_{ij})^{-1}$ are units in A. We may thus formulate the following definition :

Definition 2.7.4. Under the hypotheses of Definition 2.7.1 we call the principal ideal of A generated by the discriminant of any basis of B over A the *discriminant of B over A*. We denote it $\mathfrak{D}_{B/A}$.

Proposition 2.7.5. *Suppose that $\mathfrak{D}_{B/A}$ contains an element which is not a zero-divisor. Then, in order that a set $(x_1, \ldots, x_n) \in B^n$ be a basis for B over A, it is necessary and sufficient that* $\operatorname{disc}(x_1, \ldots, x_n)$ *generate $\mathfrak{D}_{B/A}$.*

Proof. Necessity has already been proved. Suppose that $d = \operatorname{disc}(x_1, \ldots, x_n)$ generates $\mathfrak{D}_{B/A}$. Let $(e_1, \ldots, e_n)$ be a basis of B over A. Put $d'' = \operatorname{disc}(e_1, \ldots, e_n)$ and $x_i = \sum_{j=1}^n a_{ij} e_j$ with $a_{ij} \in A$. Then $d = \det(a_{ij})^2 d'$. By hypothesis $Ad = \mathfrak{D}_{B/A} = Ad'$. Thus there exists $b \in A$ such that $d' = bd$. It follows that $d(1 - b\det(a_{ij})^2) = 0$. We know that d is not a divisor of zero, since otherwise every element of $Ad = \mathfrak{D}_{B/A}$ would be a divisor of zero. Therefore $1 - b\det(a_{ij})^2 = 0$. This shows that $\det(a_{ij})$ is invertible, so the matrix (a_{ij}) must be invertible, too. Consequently, $(x_1, \ldots, x_n)$ is a basis of B over A. □

Proposition 2.7.6. *Let K be a field which is finite or of characteristic 0, let L be an extension of finite degree n of K, and let $\sigma_1, \ldots, \sigma_n$ be the n distinct K-isomorphisms of L into an algebraically closed field C containing K (Theorem 2.4.4). Then, if $(x_1, \ldots, x_n)$ is a basis for L over K, we have*

$$\operatorname{disc}(x_1, \ldots, x_n) = \det(\sigma_i(x_j))^2 \neq 0. \tag{2.7.7}$$

Proof. The first equality follows from a simple calculation

$$\begin{aligned}\operatorname{disc}(x_1,\dots,x_n) &= \det(\operatorname{Tr}(x_i x_j)\\ &= \det(\sum_k \sigma_k(x_i X_j))\\ &= \det(\sum_k \sigma_k(x_i)\sigma_k(x_j))\\ &= \det(\sigma_k(x_i))\cdot\det(\sigma_k(x_j))\\ &= \det(\sigma_i(x_i)^2.\end{aligned}$$

It remains to show that $\det(\sigma_i(x_j)) \neq 0$. We look for a contradiction. If $\det(\sigma_i(x_j)) = 0$, there exist $u_1,\dots,u_n \in C$, not all zero, such that $\sum_{i=1}^n u_i\sigma_i(x_j) = 0$ for all j. By linearity we conclude that $\sum_{i=1}^n u_i\sigma_i(x) = 0$ for all $x \in L$. This contradicts the following lemma. □

Lemma 2.7.8 (Dedekind)**.** *Let G be a group, C a field, and let $\sigma_1,\dots,\sigma_n$ be distinct homomorphisms of G into the multiplicative group $C^\times$. Then the σ_i's are linearly independent over C (i.e. $\sum u_i\sigma_i(g) = 0$ for all $g \in G$ implies that all the u_i's are zero).*

Proof. If the σ_i's are linearly dependent, consider a non-trivial relation $\sum_{i,j} u_i\sigma_i = 0$, $(u_i \in C)$ such that the number q of the u_i's which are non-zero is minimum. After renumbering, we may suppose that

$$u_1\sigma_1(g) + \cdots + u_q\sigma_q(g) = 0 \quad \text{for all} \quad g \in G. \tag{2.7.9}$$

We have $q \geq 2$ since the σ_i's are not zero. For g and h arbitrary in G, we see that

$$u_1\sigma_1(hg) + \cdots + u_q\sigma_q(hg) = u_1\sigma_1(h)\sigma_1(g) + \cdots + u_q\sigma_q(h)\sigma_q(g) = 0.$$

Multiply 2.7.9 by $\sigma_1(h)$ and subtract. It becomes

$$u_2(\sigma_1(h) - \sigma_2(h))\sigma_1(g) + \cdots + u_q(\sigma_1(h) - \sigma_q(h))\sigma_q(g) = 0.$$

As this holds for any $g \in G$ and as q has been chosen as small as possible, it follows that $u_2(\sigma_1(h) - \sigma_2(h)) = 0$. Thus $\sigma_1(h) = \sigma_2(h)$ for all $h \in G$, since $u_2 \neq 0$. But this contradicts the hypothesis that the σ_i's are distinct. □

Remark 2.7.10. Under the conditions of Proposition 2.7.6, the relation $\operatorname{disc}(x_1,\dots,x_n) \neq 0$ means that the bilinear form $(x,y) \mapsto \operatorname{Tr}_{L/K}(xy)$ is *non-degenerate*, i.e. $\operatorname{Tr}_{L/K}(xy) = 0$ for all $y \in L$ implies $x = 0$. Thus the K-linear mapping which attaches to each $x \in L$ the K-linear form $s_x\colon y \mapsto \operatorname{Tr}_{L/K}(xy)$ is an injection of L in its dual $\operatorname{Hom}_K(L,K)$ (for the structure of vector space over K). As L and $\operatorname{Hom}_K(L,K)$ are of the same finite dimension n over K, it follows that $x \mapsto s_x$ is a bijection. The existence of "dual bases" of a vector space and its

dual implies that, for any basis $(x_1, \ldots, x_n)$ of L over K, there exists a basis $(y_1, \ldots, y_n)$ such that

$$\mathrm{Tr}_{L/K}(x_i y_j) = \delta_{ij} \quad (1 \leq i, j \leq n). \tag{2.7.11}$$

This remark will prove useful.

Theorem 2.7.12. *Let A be an integrally closed domain, let K be its field of fractions, L an extension of finite degree n of K, and A' the integral closure of A in L. Suppose K is of characteristic 0. Then A' is an A-submodule of a free A-module of rank n.*

Proof. Let $(x_1, \ldots, x_n)$ be a basis of L over K. Each x_i is algebraic over K, so, we have $a_n x_i^n + a_{n-1} x_i^{n-1} + \cdots + a_0 = 0$ with $a_j \in A$ for $j = 0, \ldots, n$. We may assume $a_n \neq 0$ by multiplication by a power of s_i; by multiplication by a_n^{n-1}, we see that $a_n x$, is integral over A. Put $x_i' = a_n x_i$. Then $(x_1', \ldots, x_n')$ is a basis for L over K contained in A'.

According to the remark preceding this theorem, there is another basis $(y_1, \ldots, y_n)$ of L over K such that $\mathrm{Tr}(x_i' y_j) = \delta_{ij}$ (2.7.11). Let $z \in A'$. Since $(y_1, \ldots, y_n)$ is a basis for L over K, we may write $z = \sum_{j=1}^n b_i y_j$ with $b_j \in K$. For any i we have $x_i' z \in A'$ (since $x_i' \in A'$). Therefore, $\mathrm{Tr}(x_i' z) \in A$ (Corollary 2.6.8). Thus,

$$\begin{aligned} \mathrm{Tr}(x_i' z) &= \mathrm{Tr}(\sum_j b_j x_i' y_j) \\ &= \sum_j b_j \,\mathrm{Tr}(x_i') \\ &= \sum b_j \delta_{ij} \\ &= b_j. \end{aligned}$$

We may conclude that $b_i \in A$ for all i, which implies that A' is a submodule of the free A-module $\sum_{j=1}^n A y_j$. □

Corollary 2.7.13. *Add to the hypotheses of Theorem 2.7.12 the assumption that A is a PID. Then A' is a free A-module of rank n.*

Proof. A submodule of a free A-module is, under our additional assumption, free (Theorem 1.5.1, (b)) and of rank $\leq n$. On the other hand we have seen in the course of the proof of Theorem 2.7.12 that A' contains a basis of L over K. Therefore, it is of rank n. □

Remark 2.7.14. As an exercise, the reader who is not familiar with the content of Remark 2.7.10 may want to look for a more computational proof of this theorem: with the notations defined above, set $d = \mathrm{disc}(x_1', \ldots, x_n')$ and show that, if $z = \sum_i c_i x_i'$ ($c_i \in K$) is integral over A, then $dc_i \in A$ (calculate $\mathrm{Tr}(z x_j')$ and use Cramer's rule).

An example of the calculation of a discriminant

Let K be a field which is finite or of characteristic 0, let $L = K[x]$ be an extension of finite degree n of K, and let $F(X)$ be the minimal polynomial of x over K. Then

$$\mathrm{disc}(1, x, \ldots, x^{n-1}) = (-1)^{\frac{n(n-1)}{2}} N_{L/K}(F'(x)) \tag{2.7.15}$$

(where $F'(X)$ denotes the derivative of $F(X)$). Denote by $x_1, \ldots, x_n$ the roots of $F(X)$ in an extension of K; they are conjugates of x (Proposition 2.3.11, and Section 2.4). We see that

$$\begin{aligned}
\mathrm{disc}(a, x, \ldots, x^{n-1}) &= \det(\sigma_i(c')^2 \quad \text{(by Proposition 2.7.6)} \\
&= \det(x_i')^2 \\
(-1)^{n(n-1)/2} \det(x_i')^2 &= [\prod_{i<j}(x_i - x_j)]^2 \quad \text{(Vandermonde)} \\
&= \prod_{i<j}(\prod_{i\neq j}(x_i - x_j)) \\
&= F'(x_i) = \mathrm{Nm}_{L/K}(F'(x))
\end{aligned}$$

(for the $F'(x_i)$'s are the conjugates of $F'(x)$). In particular, applying (2.7.15) to the case where $F(X)$ is a trinomial $X^n + aX + b$ (a and $b \in K$). Putting $y = F'(x)$, we obtain

$$y = nx^{n-1} + a = -(n-1)a - nbx^{-1}$$

(since $x^n + ax + b = 0$, whence $nx^{n-1} = -na - nbx^{-1}$). We obtain from this $x = -nb(y+(n-1)a)^{-1}$. The minimal polynomial of y over K is the numerator of $F(-nb(Y + (n-1)a)^{-1})$; the result of the computation is

$$(Y + (n-1)a)^n - na(Y + (n-1)a)^{n-1} + (-1)^n b^{n-1}.$$

The norm of y is $(-1)^n$ times the constant term of this polynomial, i.e.

$$n^n b^{n-1} + (-1)^{n-1}(n-1)^{n-1} a^n.$$

Thus,

$$\mathrm{disc}(1, x, \ldots, x^{n-1}) = [n^n + (-1)^{n-1}(n-1)^{n-1}a^n](-1)^{n(n-1)/a}. \tag{2.7.16}$$

For $n = 2$ (respectively, 3) we rediscover the well-known expressions $4b - a^2$ (respectively, $-4a^3 - 27b^2$).

2.8 The terminology of number fields

We call any finite (and therefore algebraic) extension of $\mathbb{Q}$, an *algebraic number field* (or *number field*). For a number field K, the degree $[K : \mathbb{Q}]$ is called the

degree of K. A number field of degree 2 (respectively, 3) is called a *quadratic field* (cf Section 2.5) (respectively, *cubic field*). Note that a number field always has characteristic 0.

The elements of a number field K which are integral over $\mathbb{Z}$ are called the *integers of* K. They form a subring A of K (Corollary 2.1.7). This ring A is a *free* $\mathbb{Z}$-module of rank $[K:\mathbb{Q}]$ (Corollary 2.7.13). The discriminants of the bases of the $\mathbb{Z}$-module A differ by a unit in $\mathbb{Z}$ (Definition 2.7.4), a unit which is even a square in $\mathbb{Z}$ (Proposition 2.7.3). This can only be $+1$, i.e. the discriminant of the $\mathbb{Z}$-module A is a well-defined element of $\mathbb{Z}$. It is called the *absolute discriminant*, or the *discriminant* of K.

As the nunber field K determines the ring A of integers of K in a unique fashion, we often make the abuse of language to attribute to K notions which are defined relative to A. Thus when we speak of ideals (or units) of K, we mean ideals (or units) of A.

2.9 Cyclotomic fields

We call any number field generated over $\mathbb{Q}$, by roots of unity a *cyclotomic field*. Given a prime number p, we write ζ for a primitive pth root of unity (in $\mathbb{C}$ for example). We are going to study the cyclotomic field $\mathbb{Q}[\zeta]$. The number ζ is a root of the polynomial X^p-1. Since $\zeta \neq 1$, it is also a root of the polynomial $\frac{X^p-1}{X-1} = X^{p-1}+X^{p-2}+\cdots+X+1$, which is called a *cyclotomic polynomial*. It is not obvious that this polynomial is irreducible over $\mathbb{Q}$, (i.e. that the field $Q[\zeta]$ is of degree $p-1$). In order to prove that this is indeed the case we need the following

Proposition 2.9.1 (Eisenstein's irreducibility criterion)**.** *Let A be a PID, p a prime element of A, and*

$$F(X) = X^n + a_{n-1}X^{n-1} + \ldots + a_1X + a_0 \in A[X]$$

such that p divides a_i $(0 \leq i \leq n-1)$ and p^2 does not divide a_0. Then $F(X)$ is irreducible over the field of fractions of A.

Proof. Suppose that $F = G \cdot H$ with G and $H \in K[X]$, both G and H monic polynomials. The roots of F are integral over A. Any root of G (resp. H) is a root of F, therefore also integral over A. The coefficients of G (resp. H) are sums of products of roots of G (resp. H); they are therefore also integral over A (Proposition 2.1.5). Since A is a PID, it is integrally closed (Example 2.2.3). Therefore $G \in A[X]$ and $H \in A[X]$.

Now let $\overline{F}, \overline{G}$, and $\overline{H}$ be the images of F, G, and H in $(A/Ap)[X]$, so $\overline{F} = \overline{G}\overline{H}$. According to the hypothesis on the a_i's we have $\overline{F} = X^n$. Since A/Ap is an integral domain, the factorization $X^n = \overline{G} \cdot \overline{H}$ is necessarily of the form $X^n = X^q \cdot X^{n-q}$ (since $\overline{G}$ and $\overline{H}$ are monic), thus $\overline{G} = X^q$ and $\overline{H} = X^{n-q}$. If G and H are both non-constant, then p divides the constant terms of both G and H. Therefore p^2 divides the constant term a_0 of F, and this contradicts the hypothesis. Thus, either G or H is constant, and F is irreducible. □

Example 2.9.2. The polynomial $X^3 - 2X + 6$ is irreducible over $\mathbb{Q}$ (take $p = 2, A = \mathbb{Z}$).

Theorem 2.9.3. *For any prime number p the cyclotomic polynomial $X^{p-1} + X^{p-2} + \cdots + X + 1$ is irreducible in $\mathbb{Q}[X]$.*

Proof. Put $X = Y + l$. Then

$$\begin{aligned} X^{p-1} + X^{p-2} + \cdots + X + 1 &= \frac{X^P - 1}{X - 1} \\ &= \frac{(Y+1)^p - 1}{Y} \\ &= Y^{p-1} + \sum_{j=p-1}^{1} \binom{p}{j} Y^{j-1} \\ &= F_1(Y). \end{aligned}$$

Then p divides each of the binomial coefficients $\binom{p}{j}$, but p^2 does not divide the constant term $\binom{p}{1} = p$. Thus $F_1(Y)$ is irreducible by Eisenstcin's criterion, so is the cyclotomic plynomial $X^{p-1} + X^{p-2} + \cdots + X + 1$. □

Let ζ be a primitive $p$the root of unity. By Theorem 2.9.3, the field $\mathbb{Q}[\zeta]$ is of degree $p - 1$; so $(1, \zeta, \ldots, \zeta^{p-2})$ is a basis of $\mathbb{Q}[\zeta]$ over $\mathbb{Q}$. We are going to study the ring of integers of $\mathbb{Q}[\zeta]$ and show that it is $\mathbb{Z}[\zeta]$.

For this purpose we need to calculate some *traces and norms* (we write $\mathrm{Tr}(x)$ and $\mathrm{Nm}(x)$ in place of $\mathrm{Tr}_{\mathbb{Q}(\zeta)/\mathbb{Q}}(x)$ and $\mathrm{Nm}_{\mathbb{Q}(\zeta)/\mathbb{Q}}(x)$). Let us note that the conjugates of *zeta* over $\mathbb{Q}$ are the ζ^j's $(j = 1, \ldots, p-1)$ (Theorem 2.9.3). The irreducibility of the cyclotomic polynomial implies immediately

$$\mathrm{Tr}(\zeta) = -1 \quad \text{and} \quad \mathrm{Tr}(1) = p - 1. \tag{2.9.4}$$

Therefore, $\mathrm{Tr}(\zeta^j) = -1$ for $j = 1, \ldots, p-1$, and thus

$$\mathrm{Tr}(1 - \zeta) = \mathrm{Tr}(1 - \zeta^2) = \cdots = \mathrm{Tr}(1 - \zeta^{p-1}) = p. \tag{2.9.5}$$

On the other hand,the calculation done in Theorem 2.9.3 shows that $\mathrm{Nm}(\zeta - 1) = (-1)^{p-1}p$, from which it follows that $\mathrm{Nm}(1-\zeta) = p$. As the norm of $(1-\zeta)$ is the product of the conjugates of $1 - \zeta$, we have

$$p = (1 - \zeta)(1 - \zeta^2) \cdots (1 - \zeta^{p-1}). \tag{2.9.6}$$

Let us write A for the ring of integers in $\mathbb{Q}[\zeta]$. Evidently a contains ζ and its power. We are going to show that

$$A(1 - \zeta) \cap \mathbb{Z} = p\mathbb{Z} \tag{2.9.7}$$

We know that $p \in A(l - \zeta)$ by (2.9.6). Thus, $A(1 - \zeta) \cap \mathbb{Z} \supset p\mathbb{Z}$. Since $p\mathbb{Z}$ is a maximal ideal of $\mathbb{Z}$, the relation $A(1 - \zeta) \cap \mathbb{Z} \neq p\mathbb{Z}$ implies $A(1 - \zeta) \cap \mathbb{Z}_{=}\mathbb{Z}$, i.e.

that $1-\zeta$ is a unit in A. But in this case the conjugates $1-\zeta^j$ of $1-\zeta$ must also be units; p must be a unit in $A \cap \mathbb{Z}$ by (2.9.7); and thus p^{-1} must belong to $\mathbb{Z}$, which is absurd (Â§ 2, Example 2.2.3). Let us show that, for any $y \in A$,

$$\mathrm{Tr}(y(1-\zeta)) \in A(1-\zeta); \tag{2.9.8}$$

Each conjugate $y_j(1-\zeta^j)$ of $y(1-\zeta)$ is a multiple (in A) of $1-\zeta^j$, which is itself a multiple of $1-\zeta$, since

$$1-\zeta^j = (1-\zeta)(1+\zeta+\cdots+\zeta^{j-1}).$$

Since the trace is the sum of the conjugates, we have

$$\mathrm{Tr}(y(1-\zeta)) \in A(1-\zeta).$$

Now (2.9.8) follows immediately from (2.9.7), for the trace of an integer belongs to $\mathbb{Z}$ (Corollary 2.6.8).

Now we are ready to determine the ring of integers of $\mathbb{Q}[\zeta]$.

Theorem 2.9.9. *Let p be a prime number and ζ a primitive pth root of unity in $\mathbb{C}$. Then the ring A of integers of the cyclotomic field $\mathbb{Q}[\zeta]$ is $\mathbb{Z}[\zeta]$, and $(1, \zeta, \ldots, \zeta^{p-2})$ is a basis of the $\mathbb{Z}$-module A.*

Proof. Let $x = a_0 + a_1\zeta + \cdots + a_{p-2}\zeta^{p-2}$ $(a_i \in \mathbb{Q})$ be an element of A. Then

$$x(1-\zeta) = a_0(1-\zeta) + a_1(\zeta-\zeta^2) + \cdots + a_{p-2}(\zeta^{p-2}-\zeta^{p-1}).$$

Taking traces and making use of (2.9.4) and (2.9.5), we obtain

$$\mathrm{Tr}(x(1-\zeta)) = a_0 \,\mathrm{Tr}(1-\zeta) = a_0 p.$$

By (2.9.8) $pa_0 \in p\mathbb{Z}$, so $a_0 \in \mathbb{Z}$. Since $\zeta^1 = \zeta^{p-1}$, $\zeta^{-1} \in A$, thus

$$(x-a_0)\zeta^{-1} = a_1 + a_2\zeta + \cdots + a_{p-2}\zeta^{p-3} \in A.$$

By the same argument as before, $a_1 \in \mathbb{Z}$. Applying the same argument successively, we conclude that each $a_i \in \mathbb{Z}$ □

Remark 2.9.10. The results of this section easily extend to the case of cyclotomic fields $\mathbb{Q}[t]$ where $t$is a primitive pth root of unity (p prime). Such a field is of degree $p^{r-1}(p-1)$, and its ring of integers is $\mathbb{Z}[t]$. The minimal polynomial of t over $\mathbb{Q}$ is

$$X^{p^{r-1}(p-1)} + Xp^{r-1}(p-2) + \cdots + X^{p^{r-1}} + 1 = \frac{X^{p^r}-1}{X^{p^{r-1}}-1}.$$

Chapter 3

Noetherian rings and Dedekind rings

The reader who wonders why we discuss Dedekind rings can refer to Section 3.4, and read the example and the discussion following Theorem 3.4.2. Noetherian rings, which we first study a minimum properties, are more general than Dedekind rings. We define Noetherian rings in order to place these properties in their natural context, as well as because Noetherian rings are of fundamental importance in other areas of algebra and in algebraic geometry. Finally, the generalisation of certain results regarding Noetherian rings to the case of Noetherian modules is another example of "linearisation", a technique whose power the reader has already observed.

3.1 Noetherian modules and rings

In Section 1.4, we proved the following:

Theorem 3.1.1. *[= Theorem 1.4.2] Let A be a ring and M an A-module. The following conditions are equivalent.*

(a) Every non-empty family of submodules of M contains a maximal element.

(b) Every ascending sequence of submodules of M is stationary.

(c) Every submodule of M is of finite type.

Definition 3.1.2. An A-module M is said to be *Noetherian* if it satisfies the equivalent conditions of Theorem 3.1.1. A ring A is said to be *Noetherian* if, considered as an A-module, it is a Noetherian module.

We have seen (Corollary 1.4.4) that a PID is Noetherian.

Proposition 3.1.3. *Let A be a ring, E an A-module, and E' a submodule of E. In order that E be Noetherian it is necessary and sufficient that E' and E/E' be Noetherian.*

Proof. First, we prove necessity. Suppose E is Noetherian. The lattice of submodules of E' (respectively, E/E') is isomorphic to the lattice of submodules of E contained in E' (respectively, containing E'). Thus E' and E/E' are Noetherian by Theorem 3.1.1 (a) or (b).

Conversely, suppose E' and E/E' are Noetherian. Let $(F_n)_{n\geq 0}$ be an increasing sequence of submodules of E. As E' is Noetherian, there is an integer n_0 such that $F_n \cap E' = F_{n+1} \cap E'$ for all $n > n_0$. As E/E' is Noetherian, there is an integer n_1 such that

$$(F_n + E')/E' = (F_{n+1} + E')/E' \text{ for all } n \geq n_1.$$

Therefore, $(F_n + E') = (F_{n+1} + E')$ for $n \geq n_1$. Take $n \geq \sup(n_0, n_1)$. We shall show that $F_n = F_{n+1}$. It suffices to show that $F_{n+1} \subset F_n$. To see this take $x \in F_{n+1}$. Since $F_n + E' = F_{n+1} + E'$, there exists $y \in F_n$ and $z', z'' \in E'$ such that $x + z' = y + z''$. Thus, $x - y = z' - z' \in F_{n+1} \cap E'$. Note that $F_n \cap E' = F_{n+1} \cap E'$. Thus, since $x - y$ and $y \in F_n$, $x \in F_n$ too. We conclude that $F_{n+1} = F_n$ for all $n \geq \sup(n_0, n_1)$, thus E is Noetherian by Theorem 3.1.1 (b). □

Corollary 3.1.4. *Let A be a ring and let $E_1, \ldots, E_n$ be Noetherian A-modules. Then the A-module product $\prod_{i=1}^{n} E_i$, is Noetherian.*

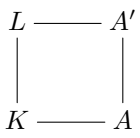
Proof. For $n = 2$, E_1 may be identified with the submodule $E \times (0)$ of $E_1 \times E_2$ and the corresponding residue module is isomorphic to E_2. Our assertion follows from Proposition 3.1.3. The general case is proved by induction on n. □

Corollary 3.1.5. *Let A be a Noetherian ring and let E be an A-module of finite type. Then E is a Noetherian module (and, therefore, all its submodules are of finite type).*

Proof. By Section 1.4, E is isomorphic to a residue module A^n/R (n being the cardinality of a finite set of generators of E). Corollary 3.1.4 implies that A^n is Noetherian and this fact, combined with Proposition 3.1.3, implies that A^n/R is Noetherian too. □

3.2 An application concerning integral elements

Proposition 3.2.1. *Let A be a Noetherian integrally closed ring (hence a domain). Let K be its field of fractions, L a finite extension of K, and A' the integral closure of A in L. Suppose that K is of characteristic 0. Then A' is an A-module of finite type and a Noetherian ring.*



Proof. We know that A' is a submodule of a free A-module of rank n (Theorem 2.7.12). Thus A' is an A-module of finite type (Corollary 3.1.5), and therefore a Noetherian module (ibid.). On the other hand, the ideals of A' are special cases of A-submodules of A'. They satisfy the maximal condition (Theorem 3.1.1 (a)), so A' is a Noetherian ring. □

Example 3.2.2. The ring of integers of a number field is Noetherian (take $A = \mathbb{Z}, K = \mathbb{Q}$).

3.3 Some preliminaries concerning ideals

An ideal $\mathfrak{p}$ of a ring A is said to be *prime* if the residue class ring $A/\mathfrak{p}$ is an integral domain. Equivalently, the relations $x \in A \setminus \mathfrak{p}, y \in A \setminus \mathfrak{p}$ imply $xy \in A \setminus \mathfrak{p}$, i.e. $A \setminus \mathfrak{p}$ is stable under multiplication.

In order that an ideal $\mathfrak{m}$ of A be *maximal* (i.e. maximal among the ideals of A distinct from A), it is necessary and sufficient that $A/\mathfrak{m}$ contain no ideals besides itself and (0), i.e. that $A/\mathfrak{m}$ be a *field*. Thus, every maximal ideal is prime. The converse is false, as the ideal (0) of $\mathbb{Z}$ is prime but not maximal.

Lemma 3.3.1. *Let A be a ring, $\mathfrak{p}$ a prime ideal of A, and let A' be a subring of A. Then $\mathfrak{p} \cap A'$ is a prime ideal of A'.*

Proof. $\mathfrak{p} \cap A'$ is the kernel of the composition of the homomorphisms $A' \to A \to A/\mathfrak{p}$, so there is an injective homomorphism $A'/(\mathfrak{p} \cap A') \to A/\mathfrak{p}$. Clearly, a subring of an integral domain is an integral domain. □

Given two ideals $\mathfrak{a}$ and $\mathfrak{b}$ of a ring A, we define the product of $\mathfrak{a}$ and $\mathfrak{b}$ not as the set of products ab where $a \in \mathfrak{a}$ and $b \in \mathfrak{b}$ (note this set is not an ideal in general), but as the set of *finite sums* $\sum a_i b_i$ of such products. One sees immediately that $\mathfrak{ab}$ is an ideal of A. We have:

$$\mathfrak{ab} \subset \mathfrak{a} \cap \mathfrak{b}$$

Remark 3.3.2. The two expressions are not always equal. In a PID the left-hand side corresponds to the product of ideal generators and the right-hand side to the least common multiple of generators.

Ideal multiplication is associative and commutative, and A acts as an identity element in the monoid.

Remark 3.3.3. Given an A-module E, a submodule F, and an ideal $\mathfrak{a}$ of A, we define in the same way the product $\mathfrak{a}F$. It is a submodule of E.

Lemma 3.3.4. *If a prime ideal $\mathfrak{p}$ of a ring A contains a product $\mathfrak{a}_1, \mathfrak{a}_2, \ldots, \mathfrak{a}_n$ of ideals, then $\mathfrak{p}$ contains at least one of the ideals $\mathfrak{a}_i$.*

Proof. If $\mathfrak{a}_i \not\subset \mathfrak{p}$ for any i, then there exists $a_i \in \mathfrak{a}_i$ such that $a_i \notin \mathfrak{p}$ for all i. Therefore, $a_1 \cdots a_n \notin \mathfrak{p}$, since $\mathfrak{p}$ is prime. But $a_1 \cdots a_n \in \mathfrak{a}_l \cdots \mathfrak{a}_n$, which contradicts the hypothesis of the lemma. □

Lemma 3.3.5. *In a Noetherian ring every ideal contains a product of prime ideals. In a Noetherian integral domain A, every non-zero ideal contains a product of non-zero prime ideals.*

Proof. We are going to make use of a reasoning typical in the theory of Noetherian rings. Let us prove the second assertion (the proof of the first is analogous; it suffices to delete the word "non-zero" three times). We look for a contradiction. Assume that the collection Φ of non-zero ideals of A which contain no product of non-zero prime ideals is *not empty*. Since A is Noetherian, Φ contains a maximal element $\mathfrak{b}$ (Theorem 3.1.1, (a)). The ideal $\mathfrak{b}$ cannot be prime; otherwise $\mathfrak{b}$ would contain the product of the family reducing to $\mathfrak{b}$, thus would not belong to Φ. Thus, there exist $x, y \in A \setminus \mathfrak{b}$ such that $xy \in \mathfrak{b}$. Then the ideals $\mathfrak{b} + Ax$ and $\mathfrak{b} + Ay$ contain $\mathfrak{b}$ as a proper subset. Therefore, since $\mathfrak{b}$ is maximal, they do not belong to Φ. It follows that they both contain products of non-zero prime ideals:

$$\mathfrak{b} + Ax \supset \mathfrak{p}_1 \cdots \mathfrak{p}_n \quad \text{and} \quad \mathfrak{b} + Ay \supset \mathfrak{q}_1 \cdots \mathfrak{q}_r.$$

Since $xy \in \mathfrak{b}$, we have

$$(\mathfrak{b} + Ax)(\mathfrak{b} + Ay) \subset \mathfrak{b}, \quad \text{whence} \quad \mathfrak{p}_1 \cdots \mathfrak{p}_n \mathfrak{q}_1 \cdots \mathfrak{q}_r \subset \mathfrak{b},$$

a contradiction. □

Now let A be an *integral domain* and let K be its field of fractions. We call any A-submodule I of K for which there exists $d \in A, d \neq 0$ such that $I \subset A$ a *fractional ideal* of A (or of K with respect to A). This means that the elements of I have a "common denominator" $d \in A$. The ordinary ideals of A are fractional ideals (with $d = 1$). We sometimes call them *integral ideals* to distinguish them from fractional ideals. Any A-submodule I of *finite type* contained in K is a fractional ideal. This follows from the fact that, if $(x_1, \ldots, x_n)$ is a finite set of generators for I, the x_i's have a common denominator d (e.g. the product of the denominators d_i where $x_i = a_i d_i^{-1}$. with $a_i, d_i \in A$), and d is a common denominator for I. Conversely, if A is *Noetherian*, any fractional ideal I is an A-module of *finite type*, i.e $I \subset d^{-1}A$ and $d^{-1}A$ being an A-module isomorphic to A, is a Noetherian module.

We define the *product* II' of two fractional ideals I and I' as the set of finite sums $\sum x_i y_i$ where $x_i \in I$ and $y_i \in I'$. If I and I' are fractional ideals, with common denominators d and d' then the sets

$$I \cap I', \quad I + I', \quad II'$$

are all *fractional ideals*. They are clearly A-submodules of K and they have as common denominators d (or d'), dd' and dd', respectively. The non-zero fractional ideals of A constitute a commutative *monoid* under multiplication.

3.4 Dedekind rings

Definition 3.4.1. A ring A is called a *Dedekind ring* if it is Noethenan and integrally closed (hence is an integral domain), and if every non-zero prime ideal of A is maximal.

The ring $\mathbb{Z}$, and more generally any PID, is a Dedekind ring. The following theorem implies that the ring of integers in a number field is a Dedekind ring:

Theorem 3.4.2. *Let A be a Dedekind ring, K its field of fractions, L an extension of finite degree of K, and A' the integral closure of A in L. Assume K is of characteristic 0. Then A' is a Dedekind ring and an A-module of finite type.*

$$\begin{array}{ccc} L & \text{———} & A' \\ | & & | \\ K & \text{———} & A \end{array}$$

Proof. The ring A' is integrally closed by construction. It is Noetherian and an A-module of finite type by Proposition 3.2.1. It remains to show that every prime ideal $\mathfrak{p} \neq (0)$ of A' is maximal. For this purpose choose an element $x \in \mathfrak{p}' \setminus (0)$ and consider an equation of integral dependence of x over A, the degree of which is a minimum.

$$x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 = 0 \quad (a_i \in A). \tag{3.4.3}$$

Then $a_0 \neq 0$, since otherwise one could factor out an x and obtain an equation of lower degree. By (3.4.3), we have $a_0 \in A'x \cap A \subset \mathfrak{p}' \cap A$. Therefore, $\mathfrak{p}' \cap A \neq (0)$. Since $\mathfrak{p}' \cap A$ is a prime ideal of A (Lemma 3.3.1), we see that $\mathfrak{p} \cap A$ is a maximal ideal of A and $A/(\mathfrak{p}' \cap A)$ is a field. But $A/(\mathfrak{p}' \cap A)$ may be identified with a subring of $A'/\mathfrak{p}'$, and $A'/\mathfrak{p}'$ is integral over $A/(\mathfrak{p}' \cap A)$ (since A' is integral over A). Thus $A'/\mathfrak{p}'$ is a field (Proposition 2.1.10), so $\mathfrak{p}'$ is maximal. □

Remark 3.4.4. Interest in Dedekind rings arises from the fact that the ring of integers in a number field is a Dedekind ring, but not always a PID.

Example 3.4.5. Consider the ring of integers $A = \mathbb{Z}[\sqrt{-5}]$ in $\mathbb{Q}[\sqrt{-5}]$ (Theorem 2.5.6). Observe that

$$(1 + \sqrt{5})(1 - \sqrt{5}) = 2 \cdot -3. \tag{3.4.6}$$

The norms of the four factors are, respectively, $6, 6, 4$, and 9. Note that $1 + \sqrt{5}$ can have no non-trivial divisor in A, since the norm of such a divisor would have to be a non-trivial divisor of 6. This is impossible, because the equations

$$a^2 + 5b^2 = 2 \quad \text{and} \quad a^2 + 5b^2 = 3$$

have no solutions in $\mathbb{Z}$. If A were a PID, the element $1 + \sqrt{5}$, which divides the product $2 \cdot 3$ by (3.4.6), would have to divide either 2 or 3. But then, taking norms, we see that 6 would divide 4 or 9, which is not the case.

Remark 3.4.7. Historically, the arithmetician Kummer (1810-1893) observed that the rings of integers in certain number fields were not PIDs (in fact, certain cyclotomic fields; Kummer observed this in connection with his work on Fermat's equation, cf. Section 1.2). In order, at least in part, to get around this inconvenience, he and Dedekind (1831-1916) introduced the notion of *ideal*. Dedekind then studied the rings which now carry his name. The most important property of PIDs is unique factorization into products of primes. There is an elegant generalisation of this property to the case of Dedekind rings. In a Dedekind ring ideals factor uniquely into products of *prime ideals*. There are many interesting consequences of this unique factorisation, which we intend now to describe precisely and prove.

Theorem 3.4.8. *Let A be a Dedekind ring which is not a field. Every maximal ideal of A is invertible in the monoid of fractional ideals of A.*

Proof. Let $\mathfrak{m}$ be a maximal ideal of A. Then $\mathfrak{m} \neq (0)$, since A is not a field. Put

$$\mathfrak{m}' = \{x \in K \mid x\mathfrak{m} \subset A\}. \tag{3.4.9}$$

Clearly, $\mathfrak{m}'$ is an A-submodule of K; any nonzero element of $\mathfrak{m}$ serves as a common denominator for the elements of $\mathfrak{m}'$. Thus $\mathfrak{m}'$ is a fractional ideal of A. It suffices to show that $\mathfrak{m}\mathfrak{m}' = A$. We see that (3.4.9) implies that $\mathfrak{m}\mathfrak{m}' \subset A$; on the other hand, $A \subset \mathfrak{m}'$ (since $\mathfrak{m}$ is an ideal), so $\mathfrak{m} = A\mathfrak{m} \subset \mathfrak{m}'\mathfrak{m}$. As $\mathfrak{m}$ is maximal and $\mathfrak{m} \subset \mathfrak{m}'\mathfrak{m} \subset A$, either $\mathfrak{m}'\mathfrak{m} = A$ or $\mathfrak{m}'\mathfrak{m} = \mathfrak{m}$. It remains to show that $\mathfrak{m}'\mathfrak{m} = \mathfrak{m}$ is impossible.

For this purpose take a non-zero element $a \in \mathfrak{m}$. The ideal Aa contains a product $\mathfrak{p}_1\mathfrak{p}_2 \cdots \mathfrak{p}_n$ of non-zero prime ideals (Lemma 3.3.5). We may take n as small as possible. We have $\mathfrak{m} \supset Aa \supset \mathfrak{p}_1\mathfrak{p}_2 \cdots \mathfrak{p}_n$, which means that $\mathfrak{m} \supset \mathfrak{p}_i$, for some i (Lemma 3.3.4), say $i = 1$. As $\mathfrak{p}_1$ is maximal by hypothesis, $\mathfrak{m} = \mathfrak{p}_1$. Put $\mathfrak{b} = \mathfrak{p}_2 \cdots \mathfrak{p}_n$. Then $Aa \supset \mathfrak{m}\mathfrak{b}$ and $Aa \not\supset \mathfrak{b}$, since n was chosen as small as possible. There thus exists $b \in \mathfrak{b}$ such that $b \notin Aa$. Since $\mathfrak{m}\mathfrak{b} \subset Aa$, $\mathfrak{m}b \subset Aa$, whence $\mathfrak{m}ba^{-1} \subset A$. According to the definition (3.4.9) of $\mathfrak{m}'$, this means that $ba^{-1} \in \mathfrak{m}'$. But, since $b \notin Aa$, $ba^{-1} \notin A$. Thus $\mathfrak{m}' \neq A$. □

Theorem 3.4.10. *Let A be a Dedekind ring and let P be the set of non-zero prime ideals of A. Then*

(a) Every non-zero fractional ideal $\mathfrak{b}$ of A may be uniquely expressed in the form

$$\mathfrak{b} = \prod_{\mathfrak{p} \in P} \mathfrak{p}^{n_{\mathfrak{p}}(\mathfrak{b})} \tag{3.4.11}$$

where $n_{\mathfrak{p}}(\mathfrak{b}) \in \mathbb{Z}$ and, for almost all $\mathfrak{p} \in P$, $n_{\mathfrak{p}}(\mathfrak{b}) = 0$.

(b) The monoid of non-zero fractional ideals of A is a group.

Proof. First we prove the existence of (a), i.e. that any fractional ideal $\mathfrak{b}$ is a product of powers (≥ 0 or ≤ 0) of prime ideals. There exists $d \in A \setminus (0)$ such that $d\mathfrak{b} \subset A$, i.e. such that $d\mathfrak{b}$ is an integral ideal of A, $\mathfrak{b} = (d\mathfrak{b}) \cdot (Ad)^{-1}$. We

may, without loss of generality, prove (a) for integral ideals. Proceeding as in Lemma 3.3.5, we consider the collection Φ of non-zero ideals in A which are not products of prime ideals. Suppose that Φ is not empty. Let $\mathfrak{a}$ be a maximal element of Φ (A is Noetherian). Then $\mathfrak{a} \neq A$, since A is the product of the empty collection of prime ideals. So $\mathfrak{a}$ is contained in a maximal ideal $\mathfrak{p}$, which is thus a maximal element in the collection of non-trivial ideals of A which contain $\mathfrak{a}$. Let $\mathfrak{p}'$ be the inverse fractional ideal of $\mathfrak{p}$. Since $\mathfrak{a} \subset \mathfrak{p}$, $\mathfrak{a}\mathfrak{p}' \subset \mathfrak{p}\mathfrak{p}' = A$. As $\mathfrak{p}' \supset A$, $\mathfrak{a}\mathfrak{p}' \supset \mathfrak{a}$ and indeed $\mathfrak{a}\mathfrak{p}' \neq \mathfrak{a}$; in fact if $\mathfrak{a}\mathfrak{p}' = \mathfrak{a}$ and if $x \in \mathfrak{p}'$, then $x\mathfrak{a} \subset \mathfrak{a}$, $x^n\mathfrak{a} \subset \mathfrak{a}$ for all n, x integral over A, and $x \in A$ (as in Theorem 3.4.8). But this is impossible, since $\mathfrak{p}' \neq A$ (otherwise $\mathfrak{p}' = A$ and $\mathfrak{p}\mathfrak{p}' = \mathfrak{p}$). According to the maximality of $\mathfrak{a}$ in Φ, we have $\mathfrak{a}\mathfrak{p}' \notin \Phi$, so $\mathfrak{a}\mathfrak{p}' = \mathfrak{p}_1 \cdots \mathfrak{p}_n$, a product of prime ideals. Multiplying by $\mathfrak{p}$, we see that $\mathfrak{a} = \mathfrak{p}\mathfrak{p}_1 \cdots \mathfrak{p}_n$. Thus every integral ideal of A is a product of prime ideals.

Let us consider next the uniqueness of (a). Suppose that

$$\prod_{\mathfrak{p} \in P} \mathfrak{p}^{n(\mathfrak{p})} = \prod_{\mathfrak{p} \in P} \mathfrak{p}^{m(\mathfrak{p})} \quad \text{i.e.} \quad \prod_{\mathfrak{p} \in P} \mathfrak{p}^{(n(\mathfrak{p}) - m(\mathfrak{p}))} = A.$$

If $n(\mathfrak{p}) - m(\mathfrak{p}) \neq 0$ for some prime ideals $\mathfrak{p} \in P$, we may separate the positive and negative exponents and write:

$$\mathfrak{p}_1^{\alpha_1} \cdots \mathfrak{p}_r^{\alpha_r} = \mathfrak{q}_1^{\beta_1} \cdots \mathfrak{q}_s^{\beta_s} \tag{3.4.12}$$

where $\mathfrak{p}_i, \mathfrak{q}_j \in P, \alpha_i, \beta_j > 0, \mathfrak{p}_i \neq \mathfrak{q}_j$ for all i and j. Thus $\mathfrak{p}_1$ contains $\mathfrak{q}_1^{\beta_1} \cdots \mathfrak{q}_s^{\beta_s}$; $\mathfrak{p}_1 \supset \mathfrak{q}_j$ for some j (Lemma 3.3.4), say $\mathfrak{p}_1 \supset \mathfrak{q}_1$. But $\mathfrak{p}_1$ and $\mathfrak{q}_1$ arc both maximal, which implies $\mathfrak{p}_1 = \mathfrak{q}_1$, a contradiction. Finally (3.4.12) implies that $\prod_{\mathfrak{p} \in P} \mathfrak{p}^{-n_\mathfrak{p}(\mathfrak{b})}$ is the inverse of $\mathfrak{b}$ and this proves (b). □

Remark 3.4.13. We have just seen that the monoid $I(A)$ of non-zero fractional ideals of a Dedekind ring is a group. The principal fractional ideals (i.e. those of the form $Ax, x \in K^\times$) form a subgroup $F(A)$ of $I(A)$ (since $(Ax) \cdot (Ay)^{-1} = Axy^{-1}$). The residue class group $C(A) = I(A)/F(A)$ is called the *ideal class group of* A. In order that A be a PID, it is necessary and sufficient that $C(A)$ consist of a single element.

Let us complete this section with some formulas, in which $n_\mathfrak{p}(b)$ denotes the exponent of $\mathfrak{p}$ in the factorisation of $\mathfrak{b}$ into a product of prime ideals (cf. (3.4.11)).

$$n_\mathfrak{p}(\mathfrak{a}\mathfrak{b}) = n_\mathfrak{p}(\mathfrak{a}) + n_\mathfrak{p}(\mathfrak{b}) \quad \text{(proof obvious)} \tag{3.4.14}$$

$$\mathfrak{b} \subset A \Leftrightarrow n_\mathfrak{p}(\mathfrak{b}) \geq 0 \quad \text{for all} \quad \mathfrak{p} \in P \tag{3.4.15}$$

($\Rightarrow$ seen in the course of the proof of Theorem 3.4.10; $\Leftarrow$ obvious)

$$\mathfrak{a} \subset \mathfrak{b} \Leftrightarrow n_\mathfrak{p}(\mathfrak{a}) \geq n_\mathfrak{p}(\mathfrak{b}) \quad \text{for all} \quad \mathfrak{p} \in P. \tag{3.4.16}$$

($\mathfrak{a} \subset \mathfrak{b}$ means the same as $\mathfrak{a}\mathfrak{b}^{-1} \subset A$. Now apply (3.4.14) and (3.4.15)).

$$n_\mathfrak{p}(\mathfrak{a} + \mathfrak{b}) = \inf(n_\mathfrak{p}(\mathfrak{a}), n_\mathfrak{p}(\mathfrak{b})) \tag{3.4.17}$$

($\mathfrak{a}+\mathfrak{b}$ is the least upper bound of a and b for ideal inclusion; to complete the proof use (3.4.16)).

$$n_{\mathfrak{p}}(\mathfrak{a}\cap\mathfrak{b}) = \sup(n_{\mathfrak{p}}(\mathfrak{a}), n_{\mathfrak{p}}(\mathfrak{b})) \tag{3.4.18}$$

(analogous argument involving greatest lower bounds; again use (3.4.16)).

3.5 The norm of an ideal

In this section, K denotes a number field, n its degree, and A the ring of integers of K. We write $\mathrm{Nm}(x)$ in place $\mathrm{Nm}_{K/\mathbb{Q}}(x)$.

Proposition 3.5.1. *If x is a non-zero element of A, then $|\mathrm{Nm}(x)| = \mathrm{card}(A/Ax)$.*

Note that, since $x \in A$, we have $\mathrm{Nm}(x) \in \mathbb{Z}$ (Corollary 2.6.8), so the preceding formula makes sense.

Proof. Wc know that A is a free $\mathbb{Z}$-module of rank n (Section 2.8), and Ax is a $\mathbb{Z}$-submodule of A. It is also of rank n, since multiplication by x maps A to Ax is a bijection. According to Theorem 1.5.1, there exists a basis $(e_1,\dots,e_n)$ of the $\mathbb{Z}$-module A together with elements c_i of $\mathbb{N}$ such that $(c_ie_1,\dots,c_ne_n)$ is a basis of Ax.

Furthermore, the abelian group A/Ax is isomorphic to the finite abelian group $\prod_{i=1}^{n}(\mathbb{Z}/c_i\mathbb{Z})$ whose order is $c_1c_2\cdots c_n$. Write u for the $\mathbb{Z}$-linear mapping of A on Ax defined by $u(e_i) = c_ie_i$ for $i = 1,\dots,n$. We have $\det(u) = c_1c_2\cdots c_n$. On the other hand $(xe_1,\cdots,xe_n)$ is also a basis for Ax. There is thus an automorphism v of the $\mathbb{Z}$-module Ax such that $v(c_ie_i) = xe_i$. Then $\det(v)$ is invertible in $\mathbb{Z}$, so $\det(v) = \pm 1$. But $v\cdot u$ is multiplication by x, and its determinant is, by definition, $\mathrm{Nm}(x)$ (Definition 2.6.4). Since $\det(v\cdot u) = \det(v)\cdot\det(u)$, we may conclude that $\mathrm{Nm}(x) = \pm c_1c_2\cdots c_n = \pm\,\mathrm{card}(A/Ax)$. □

Definition 3.5.2. Given a non-zero integral ideal $\mathfrak{a}$ de A, we call the number $\mathrm{card}(A/\mathfrak{a})$ the *norm* of $\mathfrak{a}$ and denote it by $\mathrm{Nm}(\mathfrak{a})$.

Let us observe that $\mathrm{Nm}(\mathfrak{a})$ is finite. In fact, if a is a non-zero element of $\mathfrak{a}$, then $Aa \subset \mathfrak{a}$, and $A/\mathfrak{a}$ may be identified with a quotient of A/Aa (by the first isomorphism theorem). Thus $\mathrm{card}(A/\mathfrak{a}) \le \mathrm{card}(A/Aa)$, which is finite by Proposition 3.5.1. On the other hand we saw that, for a principal ideal Ab, $\mathrm{Nm}(Ab) = |\mathrm{Nm}(b)|$.

Proposition 3.5.3. *If $\mathfrak{a}$ and $\mathfrak{b}$ are both non-zero integral ideals of A, then* $\mathrm{Nm}(\mathfrak{ab}) = \mathrm{Nm}(\mathfrak{a})\,\mathrm{Nm}(\mathfrak{b})$.

Proof. The ideal $\mathfrak{b}$ factors into a product of maximal ideals (Theorem 3.4.10), and it suffices to show that $\mathrm{Nm}(\mathfrak{am}) = \mathrm{Nm}(\mathfrak{a})\,\mathrm{Nm}(\mathfrak{m})$ for $\mathfrak{m}$ maximal. Since $\mathfrak{am} \subset \mathfrak{a}$, we have $\mathrm{card}(A/\mathfrak{am}) = \mathrm{card}(A/\mathfrak{a})\,\mathrm{card}(\mathfrak{a}/\mathfrak{am})$. It thus suffices to show that $\mathrm{card}(\mathfrak{a}/\mathfrak{am}) = \mathrm{card}(A/\mathfrak{m})$. Now $\mathfrak{a}/\mathfrak{am}$ is an A-module annihilated by $\mathfrak{m}$, which means it may be considered as a vector space over $A/\mathfrak{m}$. Its subspaces are its A-submodules; and they are of the form $\mathfrak{q}/\mathfrak{am}$, where $\mathfrak{q}$ is an ideal such

that $\mathfrak{am} \subset \mathfrak{q} \subset \mathfrak{a}$. But formula (3.4.16) implies that there are no ideals between $\mathfrak{am}$ and $\mathfrak{a}$. Therefore, the vector space $\mathfrak{a}/\mathfrak{am}$ is of dimension one over $A/\mathfrak{m}$. This means that $\mathrm{card}(\mathfrak{a}/\mathfrak{am}) = \mathrm{card}(A/\mathfrak{m})$. □

Chapter 4

Ideal classes and the unit theorem

The present chapter is devoted to two important finiteness theorems. Some tools from analysis, (called Minkowsky's Geometry of Numbers and borrowed from topology and integration in $\mathbb{R}^m$) will be used.

4.1 Preliminaries concerning discrete subgroups of $\mathbb{R}^n$

A subgroup H of $\mathbb{R}^n$ is discrete if and only if, for any compact subset K of $\mathbb{R}^n$, the intersection $H \cap K$ is finite. A typical example of a discrete subgroup of $\mathbb{R}^n$ is $\mathbb{Z}^n$. We are going to show that it is almost the only one:

Theorem 4.1.1. *Let H be a discrete subgroup of $\mathbb{R}^n$. Then H is generated (as a $\mathbb{Z}$-module) by r vectors which are linearly independent over $\mathbb{R}$ (so $r \leq n$).*

Proof. Let $(e_1, \ldots, e_r)$ be a set of elements of H which are linearly independent over $\mathbb{R}$, where r is as large as possible (again, $r \leq n$). Let

$$P = \{x \in \mathbb{R}^n \mid x = \sum_{j=1}^{r} \alpha_i e_i, 0 \leq \alpha_i \leq 1\}, \tag{4.1.2}$$

the parallelotope constructed on these vectors. Clearly P is compact, so $P \cap H$ is finite. Take $x \in H$. From the maximality of the set $(e_1, \ldots, e_r)$ it follows that $x = \sum_{i=1}^{r} \lambda_i e_i, \lambda_i \in \mathbb{R}$. For $j \in \mathbb{Z}$ set

$$x_j = jx - \sum_{i=1}^{r} [j\lambda_i] e_i \tag{4.1.3}$$

(where $[\mu]$ denotes the largest integer less than or equal to $\mu \in \mathbb{R}$). Thus,

$$x_j = \sum_{i=1}^{r} (j\lambda_i - [j\lambda_i])e_i,$$

from which it follows that $x_j \in P$ and by (4.1.3) $x_j \in P \cap H$. If one notices that $x = x_1 + \sum_{i=1}^{r} [\lambda_i]e_i$ one sees that the $\mathbb{Z}$-module H is generated by $P \cap H$ and is thus of *finite type*.

On the other hand, since $P \cap H$ is finite and $\mathbb{Z}$ is infinite, there exist distinct integers j and k such that $x_j = x_k$. It follows from (4.1.3) that $(j-k)\lambda_i = [j\lambda_i] - [k\lambda_i]$, which implies that the λ_i's are *rational*. Thus the $\mathbb{Z}$-module H is generated by a *finite* number of elements which are linear combinations with rational coefficients of the e_i's. Let d be a common denominator ($d \in \mathbb{Z}, d \neq 0$) of these coefficients. Clearly, $dH \subset \sum_{i=1}^{r} \mathbb{Z}e_i$. Thus there exists a basis (f_i) of the $\mathbb{Z}$-module $\sum_{i=1}^{r} \mathbb{Z}e_i$ and integers α_i such that $(\alpha_1 f_1, \ldots, \alpha_r f_r)$ generates dH (Theorem 1.5.1). Since the $\mathbb{Z}$-module dH has the same rank as H and since $H \supset \sum_{i=1}^{r} \mathbb{Z}e_i$, the rank of dH is $\geq r$. Therefore, the rank of dH equals r and the α_i's are non-zero. We may conclude that the f_i's are, like the e_i's, linearly independent over $\mathbb{R}$. The module dH, and consequently H itself, is generated (over $\mathbb{Z}$) by r vectors linearly independent over $\mathbb{R}$. □

Example 4.1.4. Let $t = (\theta_1, \ldots, \theta_n) \in \mathbb{R}^n$ such that at least one of the θ_i's is *irrational*. Write $(e_1, \ldots, e_n)$ for the canonical basis of $\mathbb{R}^n$ and let H denote the subgroup of $\mathbb{R}^n$ generated by $(e_1, \ldots, e_n, t)$. The group H is not discrete; otherwise the methods employed in the proof of Theorem 4.1.1 would provide us with an expression for t as a rational linear combination of the e_i's, an absurdity. Therefore, for any $\epsilon > 0$ there exists a non-zero element of H whose distance from 0 is smaller than ϵ. Therefore, there exist integers $p_1 \in \mathbb{Z}, q \in \mathbb{N}, q \neq 0$ such that $|q\theta_i - p_i| \leq \epsilon$, which means that

$$\left|\theta_i - \frac{p_i}{q}\right| \leq \frac{\epsilon}{q} \quad \text{for all} \quad i = 1, \ldots, n.$$

Let us remark that, simply by picking the multiple n_i/q of $1/q$ nearest θ_i, we would obtain the cruder approximation

$$\left|\theta_i - \frac{n_i}{q}\right| \leq \frac{1}{2q}, (n_i \in \mathbb{Z}) \quad \text{for any} \quad q > 0$$

The result proved in the last paragraph is a basic theorem in the very rich theory of approximation of irrational numbers by rationals. The reader interested in learning more about this subject should consult Koksma, "Diophantische Approximation", Berlin (Springer), 1936.

Definition 4.1.5. A discrete subgroup of rank n of $\mathbb{R}^n$ is called a *lattice* in $\mathbb{R}^n$.

By Theorem 4.1.1 a lattice is generated over $\mathbb{Z}$ by a basis of $\mathbb{R}^n$, which is then a $\mathbb{Z}$-basis for the given lattice. For each $\mathbb{Z}$-basis $e = (e_1, \ldots, e_n)$ of a lattice

H we shall write P_e for the half open parallelotope

$$P_e = \{\sum_{i=1}^{n} \alpha_i e_i \mid 0 \leq \alpha_i < 1\}.$$

Thus every point of $\mathbb{R}^n$ is congruent modulo H to one and only one point of P_e for any fixed e (we say, in this case, that P_e is a *fundamental domain* for H). We shall write μ to denote the *Lebesgue measure* in $\mathbb{R}^n$; thus, if S is a measurable subset of $\mathbb{R}^n$, $\mu(S)$ will stand for its measure (which we will also call its volume).

Lemma 4.1.6. *The volume $\mu(P_e)$ is independent of the basis e chosen for H.*

Proof. Let $f = (f_1, \ldots, f_n)$ be another basis of H. Then

$$f_i = \sum_{j=1}^{n} \alpha_{ij} e_j \quad \text{with} \quad \alpha_{ij} \in \mathbb{Z}.$$

By calculus we know that $\mu(P_f) = |\det(\alpha_{ij})|\mu(P_e)$. The matrix (α_{ij}), being associated with a change of basis, is invertible with an integer inverse matrix, so $\det(\alpha_{ij}) = \pm 1$. Thus $\mu(P_f) = \mu(P_e)$. □

The volume of the parallelotope P_e associated with any basis e of H is called the *volume of the lattice* H and is denoted $v(H)$ (the word "volume" is here an abuse of language since $\mu(H) = 0$; would it perhaps be better to speak of the "mesh" of the lattice H?).

Theorem 4.1.7 (Minkowski)**.** *Let H be a lattice in $\mathbb{R}^n$ and let S be a measurable subset of $\mathbb{R}^n$ such that $\mu(S) > v(H)$. Then there exist two distinct points $x, y \in S$ such that $x - y \in H$.*

Proof. Let $e = (e_1, \ldots, e_n)$ be a $\mathbb{Z}$-base of H and let P_e be the parallelotope associated with e. Since P_e is a fundamental domain for H, S is the disjoint union of subsets of the form $S \cap (h + P_e), (h \in H)$. It follows that

$$\mu(S) = \sum_{h \in H} \mu[S \cap (h + P_e)] \tag{4.1.8}$$

Since μ is translation invariant,

$$\mu[S \cap (h + P_e)] = \mu[(-h + S) \cap P_e].$$

The sets $(-h + S) \cap P_e, (h \in H)$ cannot all be pairwise disjoint, otherwise $\mu(P_e) \geq \sum_{h \in H} \mu[(-h + S) \cap P_e]$, which contradicts (4.1.8) and the hypothesis $\mu(P_e) = v(H) < \mu(S)$. Consequently, there exist two distinct elements h and h' of H such that $P_e \cap (-h + S) \cap (-h' + S) \neq \varnothing$. Let x and y be elements of S such that $-h + x = -h' + y$. Then $x - y = h - h' \in H$ and $x \neq y$, since $h \neq h'$. □

Corollary 4.1.9. *Let H be a lattice in $\mathbb{R}^n$ and let S be a measurable subset of $\mathbb{R}^n$ which is symmetric with respect to 0 and convex. Assume that S satisfies at least one of the following two conditions:*

(a) $\mu(S) > 2^n v(H)$ or

(b) $\mu(S) \geq 2^n v(H)$ and S is compact.

Then $S \cap (H \setminus 0) \neq \varnothing$.

Proof. In case (a) apply Theorem 4.1.7 to the set

$$S' = \frac{1}{2}S \quad (\mu(S') = 2^{-n}\mu(S) > v(H)).$$

Let y and z be distinct points of S' such that $y - z \in H$. Then $y - z$ also belongs to S, because $y - z = \frac{1}{2}(2y + (-2z))$ and S is both symmetric and convex. Therefore, $y - z \in S^n(H \setminus 0)$. To prove that case (b) also implies the conclusion of the corollary apply case (a) to $(1 + \varepsilon)S$ for $\varepsilon > 0$. Thus, $(H \setminus 0) \cap (1 + \varepsilon)S$ is a nonempty compact set (it is even finite, since it is compact and discrete). Furthermore, $\cap_{\varepsilon > 0}[(H \setminus 0) \cap (1 + \varepsilon)S] \neq \varnothing$, since an intersection of non-empty, nested compact sets is never void. This means that there is a point of $H \setminus 0$ which belongs to $(1 + \varepsilon)S$ for all $\varepsilon > 0$, therefore, since S is compact, it belongs to S, too. □

Remark 4.1.10. The hypothesis of compactness is needed in (b). Consider, as a counter-example to (b) with compactness omitted, the open parallelotope

$$\{x \in \mathbb{R}^n \mid x = \sum_{i=1}^{n} \lambda_i e_i, \quad -1 < \lambda_i < 1\}$$

built on the basis $e = (e_1, \ldots, e_n)$ and the lattice having e as a $\mathbb{Z}$-basis.

4.2 The canonical imbedding of a number field

Let K be a number field and let n be its degree. We have seen (Theorem 2.4.4) that there are n distinct isomorphisms $\sigma_i \colon K \to \mathbb{C}$. There are exactly n, because the minimal polynomial for a primitive element of K over $\mathbb{Q}$, (Corollary 2.4.6) has only n roots in $\mathbb{C}$. Let $\alpha \colon \mathbb{C} \to \mathbb{C}$ be complex conjugation. Then, for any $i = 1, \ldots, n$, $\alpha \circ \sigma_i = \sigma_j, 1 < j < n$, and $\sigma_j = \sigma_i$ if and only if $\sigma_i(K) \subset \mathbb{R}$. Write r_1 for the number of indices such that $\sigma_i(K) \subset \mathbb{R}$. Then $n - r_1$ is an even number $2r_2$ so we may write

$$r_1 + 2r_2 = n. \tag{4.2.1}$$

Let us renumber the σ_i's so that $\sigma_i(K) \subset \mathbb{R}$ for $1 \leq i \leq r$ and so that $\sigma_{j+r_2}(x) = \overline{\sigma_j(x)}$ for $r_1 + 1 \leq j \leq r_1 + r_2$. Then the first $r_1 + r_2$ isomorphisms $(\sigma_i' s)$ determine the last r_2. For $x \in K$ we define

$$\sigma(x) = (\sigma_1(x), \ldots, \sigma_{r_1+r_2}(x)) \in \mathbb{R}^{r_1} \times \mathbb{C}^{r_2}. \tag{4.2.2}$$

We call σ the *canonical imbedding* of K in $\mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$; it is an injective ring homomorphism. We shall frequently identify $\mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$ with R^n (cf. (4.2.1)). The notations σ, K, n, r_1 and r_2 will be in use for the rest of this chapter.

Proposition 4.2.3. *If M is a free $\mathbb{Z}$-submodule of rank n of K, and if $(x_i)_{1\leq i\leq n}$ is a $\mathbb{Z}$-basis of M, then $\sigma(M)$ is a lattice in $\mathbb{R}^n$, whose volume is given by*

$$v(\sigma(M)) = 2^{-r_2} \left| \det_{1\leq i,j\leq n} (\sigma_i(x_j)) \right|. \tag{4.2.4}$$

Proof. For fixed i the coordinates of $\sigma(x_i)$ with respect to the canonical basis of $\mathbb{R}^n$ are given by

$$\sigma_1(x_i), \ldots \sigma_{r_1+r_2}(x_i), \Re(\sigma_{r_1+1}(x_i), \Im(\sigma_{r_1+1}(x_i)), \ldots, \Re(\sigma_{r_1+r2}(x_i), \Im(\sigma_{r_1+r_2}(x_i)). \tag{4.2.5}$$

Let us calculate the determinant D of the matrix whose ith column is given by (4.2.5). Making use of the formulas $\Re(z) = \frac{1}{2}(z + \overline{z})$ and $\Im(z) = \frac{1}{2i}(z - \overline{z})$ for $z \in \mathbb{C}$ and of the linearity of both $\Re$ and $\Im$, we obtain $D = \pm(2i)^{r_2} \det(\sigma_j(x_i))$. Since the x_i's form a basis for K over $\mathbb{Q}$, $\det(\sigma(x_i)) \neq 0$ (Proposition 2.7.6) and therefore $D \neq 0$. Thus the vectors $\sigma(x_i)$ are linearly independent in $\mathbb{R}^n$, so that the $\mathbb{Z}$-module which they generate (call it $\sigma(M)$) is a lattice in $\mathbb{R}^n$. The calculation of D given above shows that (4.2.4) does give its volume. □

Proposition 4.2.6. *Let d be the absolute discriminant of K, let A be the ring of integers in K, and let $\mathfrak{a}$ be a non-zero integral ideal of A. Then $\sigma(A)$ and $\sigma(\mathfrak{a})$ are lattices. Moreover,*

$$v(\sigma(A)) = 2^{-r_2}|d|^{1/2} \quad \textit{and} \quad v(\sigma(\mathfrak{a})) = 2^{-r_2}|d|^{1/2}\,\mathrm{Nm}(\mathfrak{a}). \tag{4.2.7}$$

Proof. We know that A and $\mathfrak{a}$ are free $\mathbb{Z}$-modules of rank n, so we may apply Proposition 4.2.3. On the other hand, if (x_i) is a $\mathbb{Z}$-basis for A, then $d = \det(\sigma_i(x_j)^2$ (Proposition 2.7.6). This proves the first formula in (4.2.7). The second formula follows from the first and the observation that $\sigma(\mathfrak{a})$ is a subgroup of $\sigma(A)$ of index $Nm(\mathfrak{a})$ (Definition 3.5.2). A fundamental domain for $\sigma(\mathfrak{a})$ may obviously be constructed as the disjoint union of $Nm(\mathfrak{a})$ copies of a fundamental domain for $\sigma(A)$. □

4.3 Finiteness of the ideal class group

Proposition 4.3.1. *Let K be a number field, n its degree, r_1 and r_2 the integers defined in the beginng of Section 4.2, d the absolute discriminant of K, and $\mathfrak{a}$ a non-zero integral ideal of K. Then $\mathfrak{a}$ contains a non-zero element x such that*

$$|\mathrm{Nm}_{K/\mathbb{Q}}(x)| \leq \left(\frac{4}{\pi}\right)^{r_2} \frac{n!}{n^n}|d|^{1/2}\,\mathrm{Nm}(\mathfrak{a}). \tag{4.3.2}$$

Proof. Let σ be the canonical imbedding of K into $\mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$ (Section 4.2). Let t be a positive real number and let B_t be the set of all elements

$$(y_1, \ldots, y_{r_1}, z_1, \ldots, z_{r_2}) \in \mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$$

such that

$$\sum_{i=1}^{r_1} |y_i| + 2 \sum_{j=1}^{r_2} |z_j| \leq t. \tag{4.3.3}$$

Then B_t is a set which is compact and convex and symmetric relative to $0 \in \mathbb{R}^n$. By a calculation given in the appendix B

$$\mu(B_t) = 2^{r_1} \left(\frac{\pi}{2}\right)^{r_2} \frac{t^n}{n!}. \tag{4.3.4}$$

Now choose t such that $\mu(B_i) = 2^n v(\sigma(\mathfrak{a}))$, i.e. such that

$$2^{r_1} \left(\frac{\pi}{2}\right)^{r_2} \frac{t^n}{n!} = 2^{n-r_2} |d|^{1/2} \operatorname{Nm}(\mathfrak{a}) \quad \text{(Proposition 4.2.6)}$$

or such that $t^n = 2^{n-r_1} \pi^{-r_2} n! |d|^{1/2} \operatorname{Nm}(\mathfrak{a})$. By Corollary 4.1.9, there exists a non-zero element $x \in \mathfrak{a}$ such that $\sigma(x) \in B_t$. Its norm has absolute value

$$|\operatorname{Nm}(x)| = \prod_{i=1}^{r_1} |\sigma_i(x)| \prod_{j=r_1+1}^{r_1+r_2} |\sigma_j(x)|^2.$$

By the fact that the geometric mean never exceeds the arithmetic mean we have

$$|\operatorname{Nm}(x)| \leq \left[\frac{1}{n} \sum_{i=1}^{r_1} |\sigma_i(x)| + \frac{2}{n} \sum_{j=r_1+1}^{r_1+r_2} |\sigma_j(x)| \right]^n \leq \frac{t^n}{n^n} \quad (by (4.3.3)).$$

Consequently,

$$|\operatorname{Nm}(x)| \leq \frac{1}{n^n} 2^{n-r_1} \pi^{-r_2} n! |d|^{1/2} \operatorname{Nm}(\mathfrak{a}),$$

which combined with the relation $r_1 + 2r_2 = n$, yields (4.3.2). □

Corollary 4.3.5. *With the same notations, every ideal class of K (Section 3.4) contains an integral ideal $\mathfrak{b}$ such that*

$$\operatorname{Nm}(\mathfrak{b}) \leq \left(\frac{4}{\pi}\right)^{r_2} \frac{n!}{n^n} |d|^{1/2}. \tag{4.3.6}$$

Proof. Let $\mathfrak{a}'$ be an ideal of the given class. By multiplying $\mathfrak{a}'$ by a principal ideal we may suppose that $\mathfrak{a} = \mathfrak{a}'^{-1}$ is an integral ideal. Take a non-zero element $x \in \mathfrak{a}$ for which (4.3.2) holds. Then $\mathfrak{b} = x\mathfrak{a}'^{-1}$ is an integral ideal in the same class as $\mathfrak{a}'$, and $\operatorname{Nm}(\mathfrak{b})$ satisfies (4.3.6) by virtue of the multiplicativity of norms (Proposition 3.5.3). □

Corollary 4.3.7. *Let K be a number field, let n be its degree, and let d be its absolute discriminant. Then, for $n \geq 2$,*

$$|d| \geq \frac{\pi}{3}\left(\frac{3\pi}{4}\right)^{n-1}$$

and $n/(\log|d|)$ is majorised by a constant independent of K.

Proof. Since there is always a non-zero integral ideal $\mathfrak{b}$ in K and $\mathrm{Nm}(\mathfrak{b}) \geq 1$, we obtain from (4.3.6) $|d|^{1/2} \geq (4/\pi)^{r_2} n!/n^n$. From $\pi/4 < 1$ and $2r_2 \leq n$ we conclude that $|d| \geq a_n$, where $a_n = (\pi/4)^n[n^{2n}/(n!)^2]$. We observe that

$$a_2 = \frac{\pi^2}{4} \quad \text{and} \quad \frac{a_{n+1}}{a_n} = \frac{\pi}{4}\left(1+\frac{2}{n}\right)^{2n} = \frac{\pi}{4} \quad (1 + 2 + \text{ positive terms})$$

(by use of the binomial formula), so $a_{n+1}/a_n \geq +3\pi/4$. Hence, for $n \geq 2$,

$$|d| \geq \frac{\pi^2}{4}\left(\frac{3\pi}{4}\right)^{n-2}$$

from which the inequality statement in the corollary is immediate. The uniform majoration of $n/\log|d|)$ follows by taking logarithms. □

Theorem 4.3.8 (Hermite-Minkowski)**.** *For any number field $K \neq \mathbb{Q}$, the absolute discriminant d of K is $\neq \pm 1$.*

Proof. Using Corollary 4.3.7 we see that $|d| \geq (\pi/3)(3\pi/4)^{n-1}$. Since $\pi/3 > 1$ and $3\pi/4 > 1$, we have $|d| > 1$. □

Theorem 4.3.9 (Dirichlet)**.** *For any number field K the ideal class group is finite (Section 3.4).*

Proof. By Corollary 4.3.5 it suffices to show that, for every positive integer q, the set of all integral ideals $\mathfrak{b}$ of K which have q as their norms is a finite set. For such an ideal $\mathfrak{b}$ we have $\mathrm{card}(A/\mathfrak{b}) = q$ (Section 3.5). It follows that $q \in \mathfrak{b}$, since (by Cauchy-Lagrange theorem) for any group the order of an element divides the order of the group. Thus our ideals $\mathfrak{b}$ are among those which contain Aq, and there can be only finitely many such ideals (formula 3.4.16; or the finiteness of A/Aq). □

Theorem 4.3.10 (Hermite)**.** *In $\mathbb{C}$ there are only finitely many number fields with a given discriminant d.*

Proof. By Corollary 4.3.7 the degree of such a field is bounded. We may suppose n and the integers r_1 and r_2 are given. Let K be such a field.

In $\mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$ consider the following set B:

(a) If $r_1 > 0$, B is the set of all elements $(y_1, \dots, y_{r_1}, z_1, \dots, z_{r_2}) \in \mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$ such that

$$\begin{aligned} |y_1| \leq 2^n \left(\frac{\pi}{2}\right)^{-r_2} |d|^{1/2}, \quad |y_i| \leq \frac{1}{2} \quad \text{for} \quad i = 2, \dots, r_1 \quad \text{and} \\ |z_j| \leq \frac{1}{2} \quad \text{for} \quad j = 1, \dots, r_2. \end{aligned} \tag{4.3.11}$$

(b) If $r_1 > 0$, B is the set of all elements $(z_1, \dots, z_{r_2}) \in \mathbb{C}^{r_2}$ such that

$$\begin{aligned} |z_1 - \overline{z}_1| \leq 2^n \left(\frac{\pi}{2}\right)^{1-r_2} |d|^{1/2}, \quad |z_1 + \overline{z}_1| \leq \frac{1}{2}, \quad \text{and} \\ |z_j| \leq \frac{1}{2} \quad \text{for} \quad j = 2, \dots, r_2. \end{aligned} \tag{4.3.12}$$

Clearly, B is a compact and convex set which is symmetric about the origin in $\mathbb{R}^n$ and which has volume $2^n 2^{-r_2} |d|^{1/2}$[1] Writing σ for the canonical imbedding of K (Section 4.2), we obtain by means of Proposition 4.2.6 and Corollary 4.1.9 an integer $x \neq 0$ of K for which $\sigma(x) \in B$.

Let us show that x is a *primitive* element of K over $\mathbb{Q}$.
Case (a): (4.3.11) shows that $|\sigma_i(x)| \leq 1/2$ for $i \neq 1$. Since

$$|\mathrm{Nm}(x)| = \prod_{i=1}^{n} |\sigma_i(x)|$$

is a positive integer (Corollary 2.6.8), we may conclude that $|\sigma_1(x)| > 1$, so $\sigma_1(x) \neq \sigma_i(x)$ for all $i \neq 1$. However, if x were not primitive, $\sigma_1(x)$ would coincide with $\sigma_i(x)$ for some $i \neq 1$ (Proposition 2.6.8).
Case (b): We see similarly that $|\sigma_1(x)| = |\overline{\sigma_1(x)}| \geq 1$ so $\sigma_1(x) \neq \sigma_j(x)$ when σ_j is not σ_1 or $\overline{\sigma_1}$. Now (4.3.12) implies that the real part $|\Re(\sigma_1(x))| < 1/4$. But this means that $\sigma_1(x)$ cannot be real, so $\sigma_1(x) \neq \overline{\sigma_1(x)}$. As in case (a) we conclude that x is primitive.

Formulae (a) and (b) imply that the conjugates $\sigma_i(x)$ of x are *bounded*. Therefore the elementary symmetric functions of the $\sigma_i(x)$'s are also bounded. In other words, the coefficients, as well as the degree, of the minimal polynomial of x are bounded. Since x is an integer, its minimal polynomial is a monic polynomial with coefficients in $\mathbb{Z}$ (Corollary 2.6.8). The degree and the coefficients of the minimal polynomial of x being bounded, there are only finitely many possibilities for the minimal polynomial of x, consequently only finitely many possible values for $x \in \mathbb{C}$. As x generates K, there are only finitely many possibilities for K. □

4.4 The unit theorem

Let K be a number field and let A be the ring of integers in K. By abuse of language we use the expression "units of K" to refer to the units in the

[1] One may calculate this volume by making use of the observation that B is a product of intervals, of discs, and of a rectangle in case (b).

ring A. We remind the reader that in any ring the units form a group under multiplication. We write $A^\times$ for the group of units in A.

The following result will be useful.

Proposition 4.4.1. *Let K be a number field and let $x \in K$. In order that x be a unit of K it is necessary and sufficient that x be an integer of K of norm ± 1.*

Proof. If x is a unit of K, then $\mathrm{Nm}(x)$ and $\mathrm{Nm}(x^{-1})$ belong to $\mathbb{Z}$. We have $\mathrm{Nm}(x)\,\mathrm{Nm}(x^{-1}) = 1$, so $\mathrm{Nm}(x) = \pm 1$. Conversely, let x be an integer of K with norm ± 1. Its characteristic equation has the form

$$x^n + a_{n-1}x^{n-1} + \cdots + a_1 x \pm 1 = 0 \quad \text{with} \quad a_i \in \mathbb{Z} \quad \text{(Section 2.6)}$$

Thus, $\pm(x^{n-1} + a_{n-1}x^{n-2} + \cdots + a_1) = x^{-1}$ and, since x^{-1} is an integer of K, x is a unit. □

Theorem 4.4.2 (Dirichlet)**.** *Let K be a number field, n its degree, and let r_1 and r_2 be the integers defined in Section 4.2. Set $r = r_1 + r_2 - 1$. The group $A^\times$ of units of K is isomorphic to $\mathbb{Z}^r \times G$, where G is a finite cyclic group comprised of the roots of unity contained in K.*

Proof. First we shall show that $A^\times$ is a commutative group of finite type. Then we shall calculate its rank. Consider the canonical imbedding (Section 4.2) $x \mapsto (\sigma_1(x), \ldots \sigma_{r_1+r_2}(x))$ of K into $\mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$ of K and the mapping

$$x \mapsto L(x) = (\log|\sigma_1(x)|, \ldots, \log|\sigma_{r_1+r2}(x)|) \tag{4.4.3}$$

of $K^\times$ to $\mathbb{R}^{r_1+r_2}$. (4.4.3) is a homomorphism (i e. $L(xy) = L(x) + L(y)$), called the *logarithmic imbedding* of $K^\times$. Let B be a compact subset of $\mathbb{R}^{r_1+r_2}$. Let us show that the set B' of units $x \in A^\times$ such that $L(x) \in B$ is a *finite* set. Indeed, since B is bounded, there exists a real number $\alpha > 1$ such that, for all $x \in B'$,

$$\frac{1}{\alpha} \leq |\sigma_i(x)| \leq \alpha \quad (i = 1, \ldots, n).$$

It follows that the elementary symmetric functions of the $\sigma_i(x)$s are bounded in absolute value. Since they belong to $\mathbb{Z}$ (because $x \in A$), the set of possible values for the symmetric functions of the $\sigma_i x$'s is a finite set. Therefore, there are only finitely many possible characteristic polynomials for elements $x \in B'$ and consequently only finitely many possible values for x. Thus B' is a finite set.

The finiteness of B' implies immediately the following statements:

(a) The kernel G of the restriction of L to $A^\times$ is a finite group. It consists, therefore, of roots of unity and is *cyclic* (Theorem 1.6.1). Clearly, every *root of unity* in K belongs to the kernel of L, for the roots of unity in K are integers and, if x is a root of unity in K, $|\sigma_i(x)|^q = |\sigma_i(x^q)| = |1| = 1$, so $|\sigma_i(x)| = 1$ for any i.

(b) The image $L(A^\times)$ is a discrete subgroup of $\mathbb{R}^{r_1+r_2}$ (Section4.1). Consequently, $L(A^\times)$ is a free $\mathbb{Z}$-module of rank $s \leq r_1 + r_2$ (Theorem 4.1.1). Since $L(A^\times)$ is free, $A^\times$ is isomorphic to $G \times L(A^\times) = G \times \mathbb{Z}^s$. It remains to show that the rank s of $L(A^\times)$ equals $r_1 + r_2 - 1$.

The inequality $s \leq r_1 + r_2 - 1$ is easy. Indeed, for $x \in A^\times$, the relation

$$\pm 1 = \mathrm{Nm}(x) = \prod_{i=1}^{n} \sigma_i(x) = \prod_{i=1}^{r_1} \sigma_i(x) \prod_{j=r_1+1}^{r_1+r_2} \sigma_j(x)\overline{\sigma_j(x)} \quad \text{(Proposition 4.4.1)}$$

implies that the vector $L(x) = (y_1, \ldots, y_{r_1+r_2})$ lies in the hyperplane W defined by the equation

$$\sum_{i=1}^{r_1} y_i + 2 \sum_{j=r_1+1}^{r_1+r_2} y_j = 0. \tag{4.4.4}$$

Since $L(A^\times)$ is a discrete subgroup of W, $s \leq r_1 + r_2 - 1$.

Now we show that $L(A^\times)$ contains $r = r_1 + r_2 - 1$ linearly independent vectors. This requires a more delicate argument. Wc are going to show that for any linear form $f \neq 0$ on W, there exists a unit u such that $f(L(u)) \neq 0$. As the projection of W on $\mathbb{R}^r$ is an isomorphism (by (4.4.4)), we may write, for any $y = (y_1, \ldots, y_{r+1}) \in W \subset \mathbb{R}^{r+1}$

$$f(y) = c_1 y_1 + \ldots + c_r y_r, \quad \text{with} \quad c_i \in \mathbb{R}. \tag{4.4.5}$$

Fix a real number α such that

$$\alpha \geq 2^n \left(\frac{1}{2\pi}\right)^{r_2} |d|^{l/2}.$$

For any set $\lambda = (\lambda_1, \ldots, \lambda_r)$ of r positive real numbers take $\lambda_{r+1} > 0$ such that

$$\prod_{i=1}^{r_1} \lambda_1 i \prod_{j=r_1+1}^{r_1+r_2} \lambda_j^2 = \alpha.$$

In $\mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$ the set B of elements

$$(y_1, \ldots, y_{r_1}, x_1, \ldots, z_{r_2}) \quad (y_i \in \mathbb{R} \quad \text{and} \quad z_j \in \mathbb{C})$$

such that

$$|y_i| \leq \lambda_i, \quad \text{and} \quad |z_j \leq \lambda_j|$$

is compact, convex, symmetric about 0, and of volume

$$\prod_{i=1}^{r_1} 2\lambda_i \prod_{j=r_1+1}^{r_2} \pi\lambda_j^2 = 2^{r_1}\pi^{r_2}\alpha \geq 2^n 2^{-r_1}|d|^{1/2}.$$

It follows from Proposition 4.2.6 and Corollary 4.1.9 that there exists an *integer* x_λ of K such that $\sigma(x_\lambda) \in B$. This means that $|\sigma_i(x_\lambda)| \leq \lambda_i$ for $i = 1, .., n$ (putting λ_{j+r_2}, for $j = r_1 + 1, \ldots, r_1 + r_2$). Since x_λ is an integer,

$$1 \leq |\mathrm{Nm}(x_\lambda)| = \prod_{i=1}^{n} |\sigma_i(x_\lambda)| \leq \prod_{i=1}^{r_1} \lambda_i \prod_{j=r_1+1}^{r_1+r_2} \lambda_j^2 = \alpha.$$

On the other hand, for any i

$$|\sigma_i(x_\lambda)| = |\mathrm{Nm}(x_\lambda)| \prod_{j \neq i} |\sigma_j(x_\lambda)|^{-1} \geq \prod_{j \neq i} |\lambda_j^{-1} = \lambda_i \alpha^{-1}.$$

Now we have $\lambda_i \alpha^{-1} \leq |\sigma_i(x_{lambda})| \leq \lambda_i$ for any i, so that

$$0 \leq \log \lambda_i - \log |\sigma_i(x_\lambda)| \leq \log \alpha. \tag{4.4.6}$$

Use of (4.4.5) entails

$$|f(L(x_\lambda)) - \sum_{i=1}^{r} c_i \log \lambda_i| \leq \left(\sum_{i=1}^{r} |c_i| \right) \log \alpha. \tag{4.4.7}$$

Let β be a constant which is strictly larger than the right-hand side of (4.4.7) and, for every positive integer h, select r positive real numbers $\lambda_{i,h}$ $(i = 1, \ldots, r)$ satisfying $\sum_{i=1}^{r} c_i \log \lambda_{i,h} = 2\beta h$. Put

$$\lambda(h) = (\lambda_{1,h}, \ldots, \lambda_{r,h}),$$

and let x_h be the corresponding integer $x_{\lambda(h)}$. By (4.4.7) we have

$$|f(L(x_h)) - 2\beta h| < \beta,$$

so

$$(2h-1)\beta < f(L(x_h)) < (2h+1)\beta. \tag{4.4.8}$$

It follows from (4.4.8) that the numbers $f(L(x_h))$ are all *distinct*. On the other hand, since $|\mathrm{Nm}(x_h)| \leq \alpha$, there are only *finitely many* distinct ideals of the form Ax_h, (cf. the proof of Theorem 4.3.9). Therefore, there exist two distinct indices h and k such that $A_{x_h} = A_{x_k}$ and, consequently, a *unit* $u \in A$ such that $x_k = ux_h$. We may conclude (since f is linear) that $f(L(u)) = f(L(x_k)) - f(L(x_h)) \neq 0$ and u is the unit sought for. □

Remark 4.4.9. Theorem 1 (called the "unit theorem") implies that there exist $r(= r_1 + r_2 - 1)$ units (u_i) of K such that any unit u of K may be uniquely expressed in the form

$$u = z u_1^{n_1} \cdots u_r^{n_r} \tag{4.4.10}$$

with $n_i \in \mathbb{Z}$ and z a root of unity. The set $(u_i), i = 1, \ldots, r$ is called a *system of fundamental units* of K.

Example 4.4.11 (cyclotomic fields). Let p be an odd prime number, let z be a primitive complex pth root of unity, and let K be the cyclotomic field $\mathbb{Q}[\zeta]$ (cf. Section 2.9). We know that $[K : \mathbb{Q}] = p - 1$ (ibid., Theorem 2.9.3). Since no conjugate of ζ in $\mathbb{C}$ is real, $r_1 = 0$ and $2r_2 = p - 1$, so $r = (p-3)/2$.

4.5 Units in imaginary quadratic fields

Let K be an imaginary quadratic field (Section 2.5). Then $r_1 = 0, 2r_2 = 2, r_2 = 1$, and $r_1 + r_2 - 1 = 0$. Thus the only units in K are the roots of unity contained in K (Theorem 4.4.2), a finite cyclic group. With a little calculation we shall prove this result directly and make it more precise.

Let $K = \mathbb{Q}[\sqrt{-m}]$, where m is a square-free positive integer. Recall that the units of K are integers of norm ± 1 (Proposition 4.4.1).

(1) If $m \equiv 1$ or $2 \bmod 4$, the ring of integers of K is $\mathbb{Z} + \mathbb{Z}\sqrt{-m}$ (Theorem 2.5.6). For $x = a + b\sqrt{-m}$ $(a, b \in \mathbb{Z})$ we have

$$\mathrm{Nm}(x) = a^2 + mb^2 \geq 0.$$

In order that x be a unit we must have $a^2 + mb^2 = 1$. If $m \geq 2$, this implies that $b = 0$ and $a = \pm 1$, so $x = \pm 1$. If $m = 1$, besides the solution $x = \pm 1$, there are the solutions $a = 0, b = \pm 1$, ie. $x = \pm i$ (with $i^2 = 1$).

(2) If $m \equiv 3 \bmod 4$, the ring of integers of K is $\mathbb{Z} + \mathbb{Z}\left(\frac{1+\sqrt{-m}}{2}\right)$ (Theorem 2.5.6). For $x = a + (b/2)(1 + \sqrt{-m})$ $(a, b \in \mathbb{Z})$, we have

$$\mathrm{Nm}(x) = (a + b/2)^2 + mb^2/4.$$

In order that x be a unit we must have $(2a + b)^2 + mb^2 = 4$. If $m \geq 7$, this implies that $b = 0$, so $(2a)^2 = 4, a = \pm 1$, and $x = \pm 1$. If $m = 3$, the relations $b = \pm 1$ and $(2a \pm l)^2 = \pm 1$ entail the additional solutions

$$x = \frac{1}{2}(\pm 1 \pm \sqrt{-3}) \quad \text{(the signs } \pm \text{ being independent).}$$

Summarising, we have proved the following result:

Proposition 4.5.1. *If K is a quadratic imaginary field, the group G of units in K is comprised of the square roots of unity, $+1$ and -1, except in the following two cases:*

(1) If $K = \mathbb{Q}[i]$ (where $i^2 = -1$), G is comprised of the fourth roots of unity: $i, -1, -i, 1$.

(2) If $K = \mathbb{Q}[\sqrt{-3}]$, G is comprised of the sixth roots of unity: $\left(\frac{1+\sqrt{-3}}{2}\right)^j, j = 0, 1, \ldots, 5$.

4.6 Units in real quadratic fields

This section is going to be considerably more interesting than the preceding one. Let K be a real quadratic field. With the usual notations, we have $r_1 = 1$ and $r_2 = 0$, so $r = r_1 + r_2 - 1 = 1$. The unit theorem (Theorem 4.4.2) implies

that the group of units of K is isomorphic to the product of $\mathbb{Z}$ with the group of roots of unity contained in K. As K admits an imbedding into $\mathbb{R}$, the only roots of unity are ± 1. Thus, assuming that K has been imbedded into $\mathbb{R}$, we have:

Proposition 4.6.1. *The positive units of a real quadratic field $K \subset \mathbb{R}$ form a (multiplicative) group isomorphic to $\mathbb{Z}$.*

This group contains one and only one generator larger than one, we call it the *fundamental unit* of K.

Let $K = \mathbb{Q}[\sqrt{d}]$, where $d \geq 2$ is a square-free integer, and let $x = a + b\sqrt{d}$ $(a, b \in \mathbb{Q})$ be a unit of K. The numbers $x, x^{-1}, -x$, and $-x^{-1}$ are units of K and, since $\mathrm{Nm}(x) = (a+b\sqrt{d})(a-b\sqrt{d}) = \pm 1$ (Proposition 4.4.1), these four numbers are $\pm a \pm b\sqrt{d}$. For $x \neq \pm 1$ only one of the four numbers $x, x^{-1}, -x, -x^{-1}$ is greater than one, and it is the largest of the four. Thus *the units greater than one of K are those of the form $a + b\sqrt{d}$ with $a > 0, b > 0$.*

(a) Suppose first that $d \equiv 2$ or $3 \bmod 4$. In this case the ring of integers of K is $\mathbb{Z} + \mathbb{Z}\sqrt{d}$ (Theorem 2.5.6). As the units of K are integers of norm ± 1 (Â§4, Proposition 4.4.1), the units greater than one of K are the numbers $a + b\sqrt{d}$ with $a, b \in \mathbb{Z}$ and $a > 0, b > 0$ such that

$$a^2 - db^2 = \pm 1. \tag{4.6.2}$$

We see that the solutions "in natural numbers" (a, b) of equation (4.6.2) (called the "equation of Pell-Fermat") are obtained as follows: take the fundamental unit $a_1 + b_1\sqrt{d}$ of K, and put

$$a_n + b_n\sqrt{d} = (a_1 + b_1\sqrt{d})^n \quad (n \geq 1). \tag{4.6.3}$$

The sequence (a_n, b_n) provides *all the solutions* of (4.6.2).

Remark 4.6.4. It follows from (4.6.3) that $b_{n+1} = a_1 b_n + b_1 a_n$. Since a_1, b_1, a_n and b_n are all positive, the sequence (b_n) is strictly increasing. Thus, in order to explicitly calculate the fundamental unit $a_1 + b_1\sqrt{d}$, it suffices to write down the sequence (db^2) for $b \in \mathbb{N}, b \geq 1$ and to stop at the first number db_1^2 of this sequence which differs by a square a_1^2 from ± 1. Then $a_1 + b_1\sqrt{d}$ is the fundamental unit of K. For instance, if $d = 7$, the sequence of (db^2) is $7, 28, 63 = 64 - 1 = 8^2 - 1$, so, taking $b_1 = 3$ and $a_1 = 8$, we see that $8 + 3\sqrt{7}$ is the fundamental unit of $\mathbb{Q}[\sqrt{7}]$. We see similarly that the fundamental units of $\mathbb{Q}[\sqrt{2}], \mathbb{Q}[\sqrt{3}]$, and $\mathbb{Q}[\sqrt{6}]$ are $1 + \sqrt{2}, 2 + \sqrt{3}$, and $5 + \sqrt{6}$. Using the theory of continued fractions, one can find other, more rapid, procedures for calculating the fundamental unit.

Remark 4.6.5. If the fundamental unit is of norm one, the sequence (a_n, b_n) gives solutions only for the equation $(1')$ $a^2 - db^2 = 1$; in this case the equation $(1'')$ $a^2 - db^2 = -1$ has no solution in natural numbers. If the fundamental unit has norm -1, the solutions of $(1')$ comprise the sequence (a_{2n}, b_{2n}) and those of $(1'')$ the sequence (a_{2n+1}, b_{2n+1}). The first case occurs when $d = 3, 6$, or 7, the second when $d = 2$ or 1 $(3 + \sqrt{10}$ is the fundamental unit in $\mathbb{Q}[\sqrt{10}])$.

(b) Assume now that $d \equiv 1 \bmod 4$. The integers of $K = \mathbb{Q}[\sqrt{d}]$ are the numbers $\frac{1}{2}(a + b\sqrt{d})$ with $, b \in \mathbb{Z}$ of the same parity (Theorem 2.5.6). Consequently, if $\frac{1}{2}(a + b\sqrt{d})$ is a unit of K (Proposition 4.4.1), we must have

$$a^2 - db^2 = \pm 4. \tag{4.6.6}$$

Conversely, if (a, b) is an integer solution of (4.6.6), then $\frac{1}{2}(a + b\sqrt{d})$ is an integer of K (its trace is a and its norm, by (4.6.6), is ± 1 and, hence, a unit of K. As in (a), writing $\frac{1}{2}(a_1 + b_1\sqrt{d})$ for the fundamental unit of K, we see that the solutions in pairs of natural numbers (a, b) of (4.6.6) comprise the values of the sequence (a_n, b_n) $(n \geq 1)$ defined by setting

$$a_n + b_n\sqrt{d} = 2^{1-n}(a_1 + b_1\sqrt{d})^n. \tag{4.6.7}$$

The calculation of $a_1 + b_1\sqrt{d}$ may be accomplished as in (a). For example, the fundamental units of $\mathbb{Q}[\sqrt{5}], \mathbb{Q}[\sqrt{13}]$, and $\mathbb{Q}[\sqrt{17}]$ are $\frac{1}{2}(1 + \sqrt{5})$, $\frac{1}{2}(3 + \sqrt{13})$, and $4 + \sqrt{17}$; these three units all have norm -1. For the choice of the sign $\pm$ in (4.6.6) we have results similar to those obtained in (a).

Remark 4.6.8. In the case $d \equiv 1 \bmod 4$ the solutions of the Pell-Fermat equation

$$a^2 - db^2 = \pm 1 \tag{4.6.9}$$

correspond to units $a + b\sqrt{d}$ $(a, b > 0)$ which belong to the ring $B = \mathbb{Z}[\sqrt{d}]$. This ring B is a subring of the ring A of integers of K and the positive units of B form a subgroup G of the group of positive units of A. Let $u = (a + b\sqrt{f})$ be the fundamental unit of K. If a and b are both even, then $a \in B$, so that G *consists of the powers of* u (this is the case, for instance, when $d = 17$). If a and b are *both odd*, then $u^3 \in B$. (To see this note that $8u^3 = a(a^2 + 3b^2d) + b(3a^2 + b^2d)\sqrt{d}$. Since $a^2 - b^2d = \pm 4$, $a^2 + 3b^2d = 4(b^2d \pm 1)$, which is a multiple of 8, since b and d are odd. Similarly $3a^2 + b^2d = 4(a^2 \pm 1)$, which is again a multiple of 8 because a is odd. In this case G is *comprised of the powers of* u^3 ($u^2 \notin B$, otherwise $u = u^3/u^2 \in B$). This happens, for instance, when $d = 5$ (respectively, $d = 13$), in which case $u^3 = 2 + \sqrt{5}$ (respectively, $u^3 = 18 + 5\sqrt{13}$).

4.7 A generalisation of the unit theorem

Proposition 4.7.1. *Let A be a ring which is a $\mathbb{Z}$-module of finite type. Then the multiplicative group $A^\times$ consisting of the units of A is a (commutative) group of finite type.*

Remark 4.7.2. For a commutative group G, "of finite type" means "of finite type with respect to the structure of $\mathbb{Z}$-*module* of G". A subgroup of a commutative group of finite type is of finite type (Corollary 3.1.5). Let us note that A is a *Noethenan* ring, for the ideals of A are $\mathbb{Z}$-submodules of A.

Proof. First we treat the case when A is an *integral domain*. If its field of fractions K is of characteristic 0, K is a finite-dimensional vector space over $\mathbb{Q}$, so K is a number field. On the other hand, A is integral over $\mathbb{Z}$ (since it is a $\mathbb{Z}$-module of finite type, cf. Theorem 2.1.1), and, therefore, A is a subring of B, the ring of integers of K. Thus $A^\times \subset B^\times$ and, since $B^\times$ is of finite type by the unit theorem (Theorem 4.4.2), so is $A^\times$. If K is of characteristic $p \neq 0$, K is a finite extension of $\mathbb{F}_p$, so K is a finite field and $A^\times$ is a finite group.

Now let us consider the case in which A is *reduced* (by definition, this means that 0 is the only nilpotent element in A). We shall need the following lemma.

Lemma 4.7.3. *In a reduced Noethenan ring A, the ideal (0) is expressible as the intersection of finitely many prime ideals.*

Proof. We know that, in a Noetherian ring, any ideal contains a product of prime ideals (Lemma 3.3.5). (0) is the smallest ideal, so (0) is a product of prime ideals $(0) = \mathfrak{p}_1^{n_1} \cdots \mathfrak{p}_q^{n_q}$. Let $x \in \mathfrak{p}_1 \cap \cdots \cap \mathfrak{p}_q$. Then $x^{n_1+\cdots n_q} \in \mathfrak{p}_1^{n_1} \cdots \mathfrak{p}_q^{n_q} = (0)$, so $x^{n_1+\cdots n_q} = 0$. Since A is reduced, this means that $x = 0$. Therefore, $\mathfrak{p}_1 \cap \cdots \cap \mathfrak{p}_q = (0)$. □

Now, returning to the proof of Proposition 4.7.1. We let $(0) = \mathfrak{p}_1 \cap \cdots \cap \mathfrak{p}_q$, the $\mathfrak{p}_i$ being prime ideals. It follows that the canonical homomorphism $\varphi\colon A \to \prod_{i=1}^q A/\mathfrak{p}_i$ is injective. An element of a ring product is invertible if and only if all of its components are invertible, so that $\left(\prod_{i=1}^q A/\mathfrak{p}_i\right)^\times = \prod_{i=1}^q (A/\mathfrak{p}_i)^\times$. By the integral domain case, each $(A/\mathfrak{p}_i)^\times$ is of finite type; therefore, $\prod (A/\mathfrak{p}_i)^\times$ is of finite type and so is any subgroup, e.g $\varphi(A^\times)$ (recall that $\mathbb{Z}$ is a Noetherian ring). Since *varphi* is injective, $A^\times$ is of finite type.

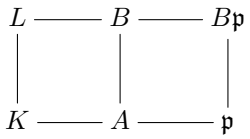
Let us finally consider the *general case*. Observe that the set $\mathfrak{n}$ of nilpotent elements of A is an *ideal*, since $x^p = 0, y^q = 0$, and $a \in A$ imply that $(x + y)^{p+q-1} = 0$ and $(ax)^p = 0$. On the other hand there exists an integer s such that $n^s = (0)$. (To see this, let $(x_1, \ldots, x_r)$ be a finite set of generators of the ideal $\mathfrak{n}$ in the Noetherian ring A. Assume $x_i^{r_i} = 0$ for $i = 1, \ldots, r$. Then, with $s = q_1 + \cdots + q_r$, it is clear that $\mathfrak{n}^s = 0$.) We proceed by induction on s. The case $s = 1$ is the reduced case which is already treated. Suppose $s > 1$ and write φ for the canonical homomorphism $\varphi\colon A \to A/\mathfrak{n}^{s-1}$. Then $\varphi(A^\times) \subset (A/\mathfrak{n}^{s-1})^\times$, so $\varphi(A^\times)$ is of finite type. The kernel of φ restricted to $A^\times$ belongs to $1 + \mathfrak{n}^{s-1}$; in fact, $\ker(\varphi) = 1 + \mathfrak{n}^{s-1}$, because for $s > 1$, $(\mathfrak{n}^{s-1})^2 \subset \mathfrak{n}^s = (0)$, which implies that any element $1 + x \in 1 + \mathfrak{n}^{s-1}$ has $1 - x$ as its inverse: $(1+x)(1-x) = 1 - x^2 = 1$. To prove that $1 + \mathfrak{n}^{s-1}$ is of finite type we need only observe that the mapping $x \mapsto 1 + x$ of the additive group $\mathfrak{n}^{s-1}$"1 to $1 + \mathfrak{n}^{s-1}$ is an isomorphism ($\mathfrak{n}^{s-1}$ is of finite type because it is a submodule of A). But this is obvious from the relation $(1+x)(1+y) = 1 + x + y$ for $x, y \in \mathfrak{n}^{s-1}$. That $A^\times$ is of finite type now follows from Proposition 3.1.3. □

Remark 4.7.4. Using arguments borrowed from algebraic geometry, one can show that, for anv reduced ring B of the form $B = \mathbb{Z}[x_1, \ldots, x_n]$ (i.e. finitely generated over $\mathbb{Z}$ as a ring), the group $B^\times$ of units in B is of finite type.

Chapter 5

The splitting of prime ideals in an extension field

Let K be a number field, A the ring of integers of K, L an extension of finite degree of K, and B the integral closure of A in L (i.e. the ring of integers of L). The ideal $B\mathfrak{p}$, generated in B by a non-zero prime ideal $\mathfrak{p}$ of A, is not prime in general.



It splits into a product of prime ideals (Theorem 3.4.10), i.e. $B\mathfrak{p} = \prod_i \mathfrak{P}_i^{e_i}$. In this chapter we propose to study this splitting. The case in which B is a *free* A-module (for example, when A is a PID; cf. Corollary 2.7.13) is particularly easy. In Section 5.1 we shall show how the general case may be reduced to this easier case.

5.1 Preliminaries concerning rings of fractions

Definition 5.1.1. Let A be an integral domain, let K be its field of fractions, and let S be a subset of $A \setminus (0)$ which is stable under multiplication and contains 1. We call the set of all elements of K which may be written in the form a/s with $a \in A$ and $s \in S$ the *ring of fractions of A with respect to S* (or the *localisation of A by S*) and denote it by $S^{-1}A$.

Clearly $S^{-1}A$ is a commutative ring (since $a/s + a'/s' = (s'a + sa')/ss'$ and $(a/s)(a'/s') = aa'/ss'$) which contains A (since $1 \in S$). If $S = A \setminus (0)$, then $S^{-1}A = K$. If S contains 1 alone, or if it contains only units of A, then $S^{-1}A = A$.

Proposition 5.1.2. *Let A be an integral domain and let S be a multiplicatively stable subset of $A \setminus (0)$ which contains 1. Set $A' = S^{-1}A$.*

(1) For any ideal $\mathfrak{b}'$ of A', we have $(\mathfrak{b}' \cap A)A' = \mathfrak{b}'$ so the mapping $b' \mapsto \mathfrak{b}' \cap A$ is an increasing (as to the inclusion) injection of the set of ideals of A' into the set of ideals of A.

(2) The mapping $\mathfrak{p}' \mapsto \mathfrak{p} \cap A$ is an isomorphism of the partially ordered set (under inclusion) of prime ideals of A' on the partially ordered set of prime ideals $\mathfrak{p}$ of A which satisfy $\mathfrak{p} \cap S = \varnothing$. The inverse mapping is $\mathfrak{p} \mapsto \mathfrak{p}A'$.

Proof. (1): If $\mathfrak{b}'$ is an ideal of A', then $\mathfrak{b}' \cap A \subset \mathfrak{b}'$ and $(\mathfrak{b}' \cap A)A' \subset \mathfrak{b}'$, since $\mathfrak{b}'$ is an ideal. To prove the reverse inclusion take $x \in \mathfrak{b}'$. Since $x = a/s$ ($a \in A$ and $s \in S$), $sx \in \mathfrak{b}'$ (for $A \subset A'$ and $\mathfrak{b}'$ is an ideal of A'). It follows that $a \in \mathfrak{b}'$ and thus $a \in \mathfrak{b}' \cap A$. Therefore, $x = 1/s \cdot a \in A'(\mathfrak{b}' \cap A)$, so $\mathfrak{b}' \subset A'(\mathfrak{b}' \cap A)$ and $\mathfrak{b}' = A'(\mathfrak{b}' \cap A)$. This formula assures the injectivity of the mapping $\varphi\colon \mathfrak{b}' \mapsto \mathfrak{b}' \cap A$, for there is a mapping $\theta\colon \mathfrak{b} \mapsto A'\mathfrak{b}$ such that $\theta \circ \varphi = \mathrm{id}$. It is clear that φ is an increasing mapping.
(2): If $\mathfrak{p}'$ is a prime ideal of A', then $\mathfrak{p} = \mathfrak{p}' \cap A$ is a prime ideal of A (Lemma 3.3.1). Furthermore, $\mathfrak{p} \cap S = \varnothing$, since, if $s \in \mathfrak{p} \cap S$, then $s \in \mathfrak{p}'$ and $1 = (1/s) \cdot s \in A'\mathfrak{p}' = \mathfrak{p}'$, a contradiction. Conversely, let $\mathfrak{p}$ be a prime ideal of A such that $\mathfrak{p} \cap S = \varnothing$. We are going to show that $\mathfrak{p}A'$ is a prime ideal of A' and that $\mathfrak{p}A' \cap A = \mathfrak{p}$. Note first that $\mathfrak{p}A'$ is the set of all elements of A' which are of the form p/s with $p \in \mathfrak{p}$ and $s \in S$; any element $x \in \mathfrak{p}A'$ may be written as

$$x = \sum_{i=1}^{n} \frac{a_i}{s_i} p_i \quad (a_i \in A, s_i \in S \quad \text{and} \quad p_i \in \mathfrak{p}),$$

so

$$x = \sum_{i=1}^{n} \frac{b_i}{s} p_i \quad (s = s_1 \cdots s_n \quad \text{and} \quad \frac{b_i}{s} = \frac{a_i}{s_i}).$$

Thus $x = p/s$ with $p = \sum b_i p_i \in \mathfrak{p}$. We may conclude that $1 \notin \mathfrak{p}A'$, since $\mathfrak{p} \cap S = \varnothing$ and since 1 cannot be written in the form p/s with $p \in \mathfrak{p}$ and $s \in S$. To show that the ideal $\mathfrak{p}A'$ is prime, let $a/s \in A'$ and $b/t \in A'$ with $(a/s) \cdot (b/t) \in \mathfrak{p}A'$. Then $(a/s)(b/t) = (p/u)$ with $p \in \mathfrak{p}$ and $u \in S$, thus $abu = pst \in \mathfrak{p}$. Since $\mathfrak{p} \cap S = \varphi$, we have $u \notin \mathfrak{p}$, so $ab \in \mathfrak{p}$ ($\mathfrak{p}$ is prime), which implies that either a or b belongs to $\mathfrak{p}$. Therefore, either a/s or b/t belongs to $\mathfrak{p}A'$, i.e. $\mathfrak{p}A'$ is prime. Let us show finally that $\mathfrak{p} = \mathfrak{p}A' \cap A$. Clearly, $\mathfrak{p} \subset \mathfrak{p}A' \cap A$. For the reverse inclusion take $x \in \mathfrak{p}A' \cap A$; then $x = p/s$ ($p \in \mathfrak{p}, s \in S$), since, by hypothesis, $x \in \mathfrak{p}A'$. Thus $sx = p \in \mathfrak{p}$; since $s \notin \mathfrak{p}$ ($\mathfrak{p} \cap S = \varnothing$) and since $\mathfrak{p}$ is prime, it follows that $x \in \mathfrak{p}$. Now we simply observe that the formulae $\mathfrak{p} = \mathfrak{p}A' \cap A$ and $\mathfrak{p}' = A'(\mathfrak{p} \cap A)$ entail that the mappings $\varphi\colon \mathfrak{p}' \mapsto \mathfrak{p}' \cap A$ and $\theta\colon \mathfrak{p}' \mapsto \mathfrak{p}A'$ (restricted to the prime ideals $\mathfrak{p}$ which do not intersect S) are inverse bijections, since $\theta \circ \varphi$ and $\varphi \circ \theta$ are both identity mappings. □

Corollary 5.1.3. *If A is a Noetherian integral domain, then every ring of fractions $S^{-1}A$ is Noethenan.*

Proof. By Proposition 5.1.2, (1) there is an injective mapping of the lattice of ideals in $S^{-1}A$ to a sublattice of the lattice of ideals in A. Therefore, the lattice of ideals in $S^{-1}A$ satisfies the maximal condition, so $S^{-1}A$ is a Noetherian ring. □

Proposition 5.1.4. *Let R be an integral domain, let A be a subring of R, let S be a multiplicatively stable subset of $A \setminus 0$ with $1 \in S$, and let B be the integral closure of A in R. Then the integral closure of $S^{-1}A$ in $S^{-1}R$ is $S^{-1}B$.*

Proof. Any element of $S^{-1}B$ may be written in the form b/s ($b \in B, s \in S$). By dividing an equation of integral dependence for b on A, e.g.

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

by s^n we obtain an equation

$$\left(\frac{b}{a}\right)^n + \frac{a_{n-1}}{s}\left(\frac{b}{s}\right)^{n-1} + \cdots + \frac{a_0}{s^n} = 0,$$

which shows that b/s is integral over $S^{-1}A$. Conversely, if x/s ($x \in R, s \in S$), an element of $S^{-1}R$, is integral over $S^{-1}A$, then there is an equation of the form

$$\left(\frac{x}{s}\right)^n + \frac{a_{n-1}}{t_{n-1}}\left(\frac{x}{s}\right)^{n-1} + \cdots + \frac{a_0}{t_0} = 0 \quad (a_i \in A, t_i \in S)$$

Multiplying through by $(t_0 t_1 \cdots t_{n-1})^n$ shows that $xt_0 \cdots t_{n-1}/s$ is integral over A. Therefore, $xt_0 \cdots t_{n-1}/s \in B$ and $x/s = (1/t_0 \cdots t_{n-1})(xt_0 \cdots t_{n-1}/s)$ belongs to $S^{-1}B$. □

Corollary 5.1.5. *If A is an integrally closed ring, then every ring of fractions $S^{-1}A$ is integrally closed.*

Proof. Take for R in Proposition 5.1.4 the field of fractions of A. □

Proposition 5.1.6. *If A is a Dedekind ring, every ring of fractions $S^{-1}A$ is a Dedekind ring.*

Proof. $S^{-1}A$ is Noetherian (Corollary 5.1.3) and integrally closed (Corollary 5.1.5). Furthermore, since one "loses" some prime ideals in passing from A to $S^{-1}A$ (Proposition 5.1.2, (2)), every non-zero prime ideal of $S^{-1}A$ is maximal. □

Proposition 5.1.7. *Let A be a Dedekind ring, let $\mathfrak{p}$ be a non-zero prime ideal of A, and let $S = A \setminus \mathfrak{p}$. Then ${}^{-1}A$ is a PID. More precisely, there exists a prime $p \in S^{-1}A$ such that the only non-zero ideals of $S^{-1}A$ are of the form $(p^n), n \geq 0$.*

Proof. Since $\mathfrak{p}$ is the only non-zero prime ideal of A disjoint from S, the only non-zero prime ideal of $S^{-1}A$ is $\mathfrak{P} = \mathfrak{p}S^{-1}A$ (Proposition 5.1.2, (2)). Since $S^{-1}A$ is a Dedekind ring (Proposition 5.1.6), its only non-zero ideals are of the form $\mathfrak{P}^n (n \geq 0)$. Take an element $p \in \mathfrak{P} \setminus \mathfrak{P}^2$. The ideal (p) is contained in $\mathfrak{P}$ but not in $\mathfrak{P}^2$. Therefore, $(p) = \mathfrak{P}$ and $(p)^n = \mathfrak{P}^n$ for all $n \geq 0$. Thus $S^{-1}A$ is principal and all its ideals are of the form $(p)^n, n \geq 0$. □

Proposition 5.1.8. *Let A be an integral domain, S a multiplicatively stable subset of $A \setminus (0)$ containing 1, and let $\mathfrak{m}$ be a maximal ideal of A which is disjoint from S. Then*

$$S^{-1}A/\mathfrak{m}S^{-1}A \cong A/\mathfrak{m}.$$

Proof. The composition of ring homomorphisms $A \to> S^{-1}A \to S^{-1}A/\mathfrak{m}S^{-1}A$ has kernel $\mathfrak{m}S^{-1}A \cap A = \mathfrak{m}$ (Proposition 5.1.2 (1)), so there is an injection $\varphi\colon A/\mathfrak{m} \to S^{-1}A/\mathfrak{m}S^{-1}A$. We must show that φ is surjective. Take $x = a/s \in S^{-1}A$ $(a \in A, s \in S)$ and let $\overline{x}$ denote its residue class in $S^{-1}A/\mathfrak{m}S^{-1}A$. Since $s \notin \mathfrak{m}$ (by hypothesis, $\mathfrak{m} \cap S = \varnothing$) and since $\mathfrak{m}$ is maximal, there exists $b \in A$ such that $bs \equiv 1 \bmod \mathfrak{m}$. Thus

$$\frac{a}{s} - ab = \frac{a}{s}(1 - bs) \in \mathfrak{m}S^{-1}A,$$

so $\varphi(ab) = \overline{x}$. □

5.2 The splitting of a prime ideal in an extension

In this section A denotes a Dedekind ring of characteristic 0, K its field of fractions, L a finite extension of K of degree n, and B the integral closure of A in L. We remind the reader that B is also a Dedekind ring (Theorem 3.4.2).

Let $\mathfrak{p}$ be a non-zero prime ideal of A. Then $B\mathfrak{p}$ is an ideal of B and it has an expression of the form

$$B\mathfrak{p} = \prod_{i=1}^{q} \mathfrak{P}_i^{e_i} \tag{5.2.1}$$

where the $\mathfrak{P}_i$'s are distinct prime ideals of B, the e_i's are positive integers, and the product sign denotes multiplication of ideals.

Proposition 5.2.2. *The $\mathfrak{P}_i$'s are precisely those prime ideals $\mathfrak{Q}$ of B such that $\mathfrak{Q} \cap A = \mathfrak{p}$.*

Proof. For a prime ideal $\mathfrak{Q}$ of B the relation $\mathfrak{Q} \cap A = \mathfrak{p}$ is equivalent to the relation $\mathfrak{Q} \supset \mathfrak{p}B$ ($\to$ is clear. $Leftarrow <$ follows from the fact that $\mathfrak{Q} \cap A$ is a prime ideal of A and $\mathfrak{p}$ is maximal). Clearly, $B\mathfrak{p} = \prod_{i=1}^{q} \mathfrak{P}_i^{e_i}$ implies $B\mathfrak{p} \subset \mathfrak{P}_i$ for each $i = 1, \ldots, q$, so $\mathfrak{P}_i$ appears in the product expression for $B\mathfrak{p}$ if and only if $\mathfrak{P}_i \cap A = \mathfrak{p}$. □

It is now clear that $A/\mathfrak{p}$ may be identified with a subring of $B/\mathfrak{P}_i$ for any $i = 1, \ldots, q$. Both rings are fields. Since B is an A-module of finite type

(Theorem 3.4.2), $B/\mathfrak{P}_i$ is a finite dimensional vector space over $A/\mathfrak{p}$. We shall write f_i for the dimension of $B/\mathfrak{P}_i$ over $A/\mathfrak{p}$ and call f_i the *residual degree* of $\mathfrak{P}_i$ over A. The exponent e_i in (5.2.1) is called the *ramification index* of $\mathfrak{P}_i$ over A. Let us remark finally that $B\mathfrak{p} \cap A = \mathfrak{p}$ ($\supset$ clear. $\subset$ follows from the fact that, for each $i = 1, \ldots, q$, $\mathfrak{P}_i \cap A = \mathfrak{p}$), so $B/B\mathfrak{p}$ is a vector space over $A/\mathfrak{p}$, also of finite dimension.

Theorem 5.2.3. *With the preceding notations*

$$\sum_{i=1}^{q} e_i f_i = [B/B\mathfrak{p} : A/\mathfrak{p}] = n. \tag{5.2.4}$$

Proof. The first equality is easy. Consider the sequence of ideals

$$B \supset \mathfrak{P}_1 \supset \mathfrak{P}_1^2 \supset \cdots \supset \mathfrak{P}_1^{e_1} \supset \mathfrak{P}_1^{e_1}\mathfrak{P}_2 \supset \cdots \supset \mathfrak{P}_1^{e_i}\mathfrak{P}_2^{e_2} \supset \mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_q^{e_q} = B\mathfrak{p}.$$

Two consecutive elements of this sequence are of the form $\mathfrak{B}$ and $\mathfrak{B}\mathfrak{P}_i$. Since there is no ideal strictly between $\mathfrak{B}$ and $\mathfrak{B}\mathfrak{P}_i$, $\mathfrak{B}/\mathfrak{B}\mathfrak{P}_i$ is a vector space of dimension one $B/\mathfrak{P}_\mathfrak{i}$ (cf. the proof of Proposition 3.5.3). Thus it is a vector space of dimension f_i over $A/\mathfrak{p}$. For a given i there are exactly e_i consecutive elements of the above sequence with associated residue class space of the form $\mathfrak{B}/\mathfrak{B}\mathfrak{P}_i$ i.e. of dimension f_i over $A/\mathfrak{p}$. The total dimension $[B/B\mathfrak{p} : A/\mathfrak{p}]$ equals the sum of the dimensions of the residue classes, so it is $\sum_{i=1}^{q} e_i f_i$.

The second equality is also easy in the case where B is a free A-module, in particular when A is a PID (Corollary 2.7.13). In this case a basis $(x_1, \ldots, x_n)$ of B as an A-module gives, by reduction mod $B\mathfrak{p}$, a basis for $B/B\mathfrak{p}$ over $A/\mathfrak{p}$. We are going to reduce the general case to this case by considering the multiplicatively stable subset $S = A \setminus \mathfrak{p}$ of A and the rings of fractions $A' = S^{-1}A$ and $B' = S^{-1}B$. We know that A' is a PID in which $\mathfrak{p}A'$ is the unique maximal ideal (Proposition 5.1.7), and that B' is the integral closure of A' in L (Proposition 5.1.4). By the special case when A is a PID,

$$[B'/\mathfrak{p}B' : A'/\mathfrak{p}A'] = n.$$

Now consider the factorisation of the ideal $\mathfrak{p}B'$ in the Dedekind ring B': from the fact that $\mathfrak{p}B = \prod_{i=1}^{q} \mathfrak{P}_i^{e_i}$ we conclude that $\mathfrak{p}B' = \prod_{i=1}^{q} (B'\mathfrak{P}_i)^{e_i}$. Since $\mathfrak{P}_i \cap A = \mathfrak{p}$ (Proposition 5.2.2), $\mathfrak{P}_i \cap S = \varnothing$ and $B'\mathfrak{P}_i$ is a non-zero prime ideal of B' (Proposition 5.1.2, (2)). From the first part of our proof we now obtain

$$[B'/\mathfrak{p}B' : A'/\mathfrak{p}A'] = \sum_{i=1}^{q} e_i [B'/B'\mathfrak{P}_i : A'/\mathfrak{p}A'].$$

However,

$$A'/\mathfrak{p}A' \cong A/\mathfrak{p} \quad \text{and} \quad B'/B'\mathfrak{P}_i \cong B/\mathfrak{P}_i \quad \text{(Proposition 5.1.8)}$$

Therefore,

$$n = [B'/\mathfrak{p}B' : A'/\mathfrak{p}A'] = \sum_{i=1}^{q} e_i f_i.$$

□

Proposition 5.2.5. *With the same notations, the ring $B/B\mathfrak{p}$ is isomorphic to the ring $\prod_{i=1}^{q} B/\mathfrak{P}_i^{e_i}$.*

Proof. $\mathfrak{P}_i$ is the only maximal ideal of B which contains $\mathfrak{P}_i^{e_i}$, so $\mathfrak{P}_i^{e_i} + \mathfrak{P}_j^{e_j} = B$ for $i \neq j$. The proposition now follows from (5.2.1) and Lemma 1.3.3. □

Example 5.2.6 (Cyclotomic fields). Let p be a prime number and let $\zeta \in \mathbb{C}$ be a primitive p^rth root of unity. In this ease, all the complex p^rth roots of unity are of the form ζ^j $(j = 1, \ldots, p^r)$. The primitive roots of unity are those for which j is not a multiple of p. The number of primitive roots is

$$\varphi(p^r) = p^r - p^{r-1} = p^{r-1}(p-1)$$

(cf. Section 1.6). The primitive p^rth roots of unity are the roots of the cyclotomic polynomial

$$F(X) = \frac{X^{p^r} - 1}{X^{p^{r-1}} - 1} = X^{p^{r-1}(p-1)} + X^{p^{r-1}(p-2)} + \cdots + X^{p^{r-1}} + 1. \qquad (5.2.7)$$

We intend to give another proof that $[\mathbb{Q}[\zeta] : \mathbb{Q}] = p^{r-1}(p-1)$ i.e. that F is irreducible (cf. Section 2.9). For this purpose put $e = p^{r-1}(p-1)$ and let $\zeta_1, \ldots, \zeta_e$ be all the primitive p^rth roots of unity. Since the constant term of $F(X+1)$ is p, we have

$$\prod_{j=1}^{e} (\zeta_j - 1) = \pm p.$$

LetB be the ring of integers of $\mathbb{Q}[\zeta]$. Clearly, $\zeta_j \in B$ and $\zeta_j - 1 \in B(\zeta_k - 1)$ for all j and k, since ζ_j is a power ζ_k^q of ζ_k and

$$\zeta_k^q - 1 = (\zeta_k - 1)(\zeta_k^{q-1} + \cdots + \zeta_K + 1).$$

Thus all the ideals $B(\zeta_k - 1)$ are the same. It follows that $B\mathfrak{p} = B(\zeta_1 - 1)^e$.

Now write $B\mathfrak{p} = \prod_{i=1}^{q} \mathfrak{P}_i^{e_i}$, where the $\mathfrak{P}_i$'s are prime ideals of B. The e_i's must, clearly, all be multiples of e. But we have $e \geq [\mathbb{Q}[\zeta] : \mathbb{Q}]$ (by (5.2.7)), so $e \geq \sum_{i=1}^{q} e_i f_i$ (Theorem 5.2.3). From these inequalities (they are really equalities) we may conclude that $q = 1, e = e_1, f_1 = 1$, and $[\mathbb{Q}[\zeta] : \mathbb{Q}] = e$. In summary:

(a) $[\mathbb{Q}[\zeta] : \mathbb{Q}] = e = p^{r-1}(p-1)$,

(b) $B(\zeta_1 - 1))$ is a prime ideal of B of residual degree 1, and

(c) $Bp = B(\zeta_1 - 1)^e$.

5.3 The discriminant and ramification

With the notations of Section 5.2 (let $B\mathfrak{p} = \prod_{i=1}^{q} \mathfrak{P}_i^{e_i}$) a prime ideal $\mathfrak{p}$ of A is said to *ramify* in B (or in L) if any one of its ramification indices e_i is larger

than one. In terms of the theory of the discriminant (Section 2.7) we are going to characterise those prime ideals of A which ramify in B. In particular we shall show that only finitely many prime ideals of A ramify in B. First we need some lemmas concerning the discriminant.

Lemma 5.3.1. *Let A be a ring, let $B_1, \cdots, B_q$ be rings containing A which are free A-modules of finite type, and let $B = \prod_{i=1}^{q} B_i$ be the product ring. Then $\mathfrak{D}_{B_i/A} = \prod_{i=1}^{q} \mathfrak{D}_{B_i/A}$ (cf. Definition 2.7.4).*

Proof. We formulate our proof for the case $q = 2$. The general statement follows by induction on q. Let $(x_1, \ldots, x_m)$ and $(y_1, \ldots, y_n)$ be bases for B_1 and B_2 as modules over A. With the usual identifications of B_1 with $B_1 \times (0)$ and B_2 with $(0) \times B_2$, we may consider $(x_1, \ldots, x_m, y_1, \ldots, y_n)$ as a basis for $B = B_1 \times B_2$ over A. By definition of the product ring structure $x_i y_j = 0$, from which it follows that $\mathrm{Tr}(x_i, y_j) = 0$. As a consequence the determinant $D(x_1, \ldots, y_1, \ldots, y_n)$ is the determinant of the matrix

$$\begin{bmatrix} \mathrm{Tr}(x_i x_{i'}) & 0 \\ 0 & \mathrm{Tr}(y_j y_{j'}) \end{bmatrix}$$

The value of this determinant is

$$\det(\mathrm{Tr}(x_i x_{i'})) \det(\mathrm{Tr}(y_i y_{j'})),$$

so

$$D(x_1, \ldots, x_m, y_1, \ldots, y_n) = D(x_1, \ldots, x_m) D(y_1, \ldots, y_n).$$

□

Lemma 5.3.2. *Let B be a ring, A a subring of B, and $\mathfrak{a}$ an ideal of A. Assume that B is a free module over A with the basis $(x_1, \ldots, x_n)$. For $x \in B$ write $\overline{x}$ for the residue class of x in $B/\mathfrak{a}B$.*

Then $(\overline{x_1}, \ldots, \overline{x_n})$ is a basis of $B/\mathfrak{a}B$ over $A/\mathfrak{a}$ and we have

$$D(\overline{x_1}, \ldots, \overline{x_n}) = \overline{D(x_1, \ldots, x_n)}. \tag{5.3.3}$$

Proof. Let $x \in B$. If the matrix for multiplication by x, with respect to the basis $(x_1, \ldots, x_n)$ is (a_{ij}) $(a_{ij}) \in A)$, then the matrix for multiplication by $\overline{x}$ with respect to the basis $(\overline{x_1}, \ldots, \overline{x_n})$ is $(\overline{a_{ij}})$. Thus, $\mathrm{Tr}(\overline{x}) = \overline{\mathrm{Tr}(x)}$. Taking $x = x_i x_j$, we obtain

$$\mathrm{Tr}(\overline{x_i} \cdot \overline{x_j}) = \overline{\mathrm{Tr}(x_i x_j)},$$

and (5.3.3) follows by taking determinants. □

Lemma 5.3.4. *Let K be afield which is finite or of characteristic 0. Let L be a finite dimensional (commutative) K-algebra. In order that L be reduced it is necessary and sufficient that $\mathfrak{D}_{L/K} \neq (0)$.*

Proof. Suppose first that L is not reduced and let x be a non-zero nilpotent element of L. Let $(x_1, \ldots, x_n)$ be a basis for L over K such that $x = x_1$. Then $x_i x_j$, is nilpotent and multiplication by $x_i x_j$ is a nilpotent endomorphism of the vector space L over K. Thus all the characteristic values of this endomorphism are zero, so $\mathrm{Tr}(x_i x_j) = 0$. The matrix $(\mathrm{Tr}(x_i x_j))$ has a row comprised entirely of zeroes, which implies that $D(x_1, \ldots, x_n) = 0$, i.e. $\mathfrak{D}_{L/K} = (0)$.

Conversely, suppose that L is reduced. Then the ideal (0) of L is expressible as a finite intersection of prime ideals, $(0) = \cap_{i=1}^{q} \mathfrak{P}_i$ (Lemma 4.7.3). Since $L/\mathfrak{P}_i$ is an integral domain and a finite dimensional algebra over K, it is a field (Proposition 2.1.10). It follows that $\mathfrak{P}_i$ is a maximal ideal of L, and consequently $\mathfrak{P}_i + \mathfrak{P}_j = L$ for $i \neq j$. Therefore L is isomorphic to the ring product $\prod_{i=1}^{q} L/\mathfrak{P}_i$ (Lemma 1.3.3). By Lemma 5.3.1 $\mathfrak{D}_{L/K} = \prod_{i=1}^{q} \mathfrak{D}_{(L/\mathfrak{P}_i)/K}$. But $\mathfrak{D}_{(L/\mathfrak{P}_i)/K} \neq (0)$ since K is finite or of characteristic 0 (Proposition 2.7.6). Therefore, $\mathfrak{D}_{L/K} \neq (0)$. □

Definition 5.3.5. Let K and L be number fields with $K \subset L$ and A and B be the rings of integers of K and L, respectively.

$$\begin{array}{ccc} L & \text{——} & B \\ | & & | \\ K & \text{——} & A \end{array}$$

The *discriminant (ideal)* of B over A (or of L over K) is the ideal of A generated by the discriminants of bases of L over K which are contained in B. Notation: $\mathfrak{D}_{B/A}$ or $\mathfrak{D}_{L/K}$.

Remark 5.3.6. If $(x_1, \ldots, x_n)$ is a basis of L over K contained in B, then $\mathrm{Tr}_{L/K}(x_i x_j) \in A$ (Corollary 2.6.8), so $D(x_1, \ldots, x_n) \in A$. Thus $\mathfrak{D}_{B/A}$ is an *integral* ideal of A. It is non-zero by Proposition 2.7.6.

Remark 5.3.7. When B is a *free* A-module (for example if A is a PID) we have already defined the discriminant $\mathfrak{D}_{B/A}$ as the ideal generated by $D(e_1, \ldots, e_n)$ where $(e_1, \ldots, e_n)$ is an A-module basis for B (Definition 2.7.4). Our old definition coincides with the one given above, since, given any basis (x_i) of L over K contained in B, one sees that $x_i = \sum_i a_{ij} e_j$ with $a_{ij} \in A$. Therefore, by Proposition 2.7.3 we have

$$D(x_1, \ldots, x_n) = \det(a_{ij})^2 D(e_1, \ldots, e_n)$$

Theorem 5.3.8. *Let the notations be as in Definition 5.3.5. In order that a prime ideal $\mathfrak{p}$ of A ramify in B, it is necessary and sufficient that it contain the discriminant $\mathfrak{D}_{B/A}$. There are only finitely many prime ideals of A which ramify in B.*

Proof. The second assertion follows from the first, since $\mathfrak{D}_{B/A} \neq (0)$. Let us prove the first. Since $B/\mathfrak{p}B \cong \prod_{i=1}^{q} B/\mathfrak{P}i^{e_i}$ (Proposition 5.2.5), the assertion "$\mathfrak{p}$ ramifies" is equivalent to the statement "$B/\mathfrak{p}B$ is not reduced", i.e. equivalent

to $\mathfrak{D}_{(B/\mathfrak{P}_i)/(A/\mathfrak{p})} = (0)$" (by Lemma 5.3.4 and the fact that $A/\mathfrak{p}$ is a finite field). Now put $S = A \setminus \mathfrak{p}, A' = S^{-1}A, B' = S^{-1}B$, and $\mathfrak{p}' = \mathfrak{p}A'$. Then A' is a PID (Proposition 5.1.7), B' is a free A'-module, $A/\mathfrak{p} \cong A'/\mathfrak{p}'$, and $B/\mathfrak{p}B \cong B'/\mathfrak{p}'B'$ (Proposition 5.1.8). Therefore, writing $(e_1, \ldots, e_n)$ for an A'-module basis of B', we know that $\mathfrak{D}_{B/A} = (0)$ if and only if $D(e_1, \ldots, e_n) \in \mathfrak{p}'$ (Lemma 5.3.2). If $D(e_1, \ldots, e_n) \in \mathfrak{p}'$ and if $(x_1, \ldots, x_n)$ is a basis for L over K contained in B, then $x_i = \sum a'_{ij} e_j$ with $a'_{ij} \in A'$ (for $B \subset B'$), so

$$D(x_1, \ldots, x_n) = \det(a'_{ij})^2 D(e_1, \ldots, e_n) \in \mathfrak{p}'$$

Since $\mathfrak{p}' \cap A = \mathfrak{p}$ (Proposition 5.1.2 (2)), we may conclude that $D(x_1, \ldots, x_n) = \mathfrak{p}$ and $\mathfrak{D}_{B/A} \subset \mathfrak{p}$. Conversely, if $\mathfrak{D}_{B/A} \subset \mathfrak{p}$ then $D(e_1, \ldots, e_n) \in \mathfrak{p}'$, for one may write $e_i = y_i/s$ with $y_i \in B$ and $s \in S$, for $1 \leq i \leq n$. Consequently,

$$D(e_1, \ldots, e_n) = s^{-2n} D(x_1, \ldots, x_n) \in A'\mathfrak{D}_{B/A} \subset A'\mathfrak{p} = \mathfrak{p}'$$

□

Example 5.3.9 (Quadratic fields). Let $K = \mathbb{Q}$ and $L = \mathbb{Q}[\sqrt{d}]$, where d is a square-free integer (Section 2.5).

1. If $d \equiv 2$ or $3 \bmod 4$, then $(1, \sqrt{d})$ is a basis for the ring of integers of L. As $\mathrm{Tr}(1) = 2, \mathrm{Tr}(\sqrt{d}) = 0$, and $\mathrm{Tr}(d) = 2d$, it follows that $D(1, \sqrt{d}) = 4d$. The prime numbers which ramify in L therefore include 2 and the prime divisors of d.

2. If $d \equiv l \bmod 4$, $(1, (1 + \sqrt{d})/2)$ is a basis for the ring of integers of L. We see that
$$\mathrm{Tr}(1) = 2, \mathrm{Tr}\left(1, \frac{1+\sqrt{d}}{2}\right) = 1$$
and
$$\mathrm{Tr}\left(\left(\frac{1+\sqrt{d}}{2}\right)^2\right) = \mathrm{Tr}\left(\frac{d+1}{4} + \frac{1}{2}\sqrt{d}\right) = \frac{d+1}{2}.$$
thus
$$D\left(1, \frac{1+\sqrt{d}}{2}\right) = 2 \cdot \frac{d+1}{2} - 1 = d.$$
The only prime numbers which ramify in L are the divisors of d.

We remark that a quadratic field $\mathbb{Q}[\sqrt{d}]$ is uniquely determined by its discriminant. In fact,

$D \equiv 0 \bmod 4$ implies $d = \frac{D}{4}$ (we must have $d \equiv 2$ or $3 \bmod 4$),

$D \equiv 1 \bmod 4$ implies $d = D$, and

$D \equiv 2$ **or** $3 \bmod 4$ is impossible.

We also note that the discriminant of a quadratic field is not an arbitrary integer.

Example 5.3.10 (Cyclotomic fields). Let p be an odd prime number, let ζ be a primitive complex pth root of unity, and let $L = \mathbb{Q}[\zeta]$ be the corresponding cyclotomic field. We know that $(1, \zeta, \ldots, \zeta^{p-2})$ is a $\mathbb{Z}$-basis for the ring of integers B of L (Theorem 2.9.9), and that the minimal polynomial F of ζ over $\mathbb{Q}$ satisfies the relation $(X-1)F(X) = X^p - 1$ (Theorem 2.9.3). We are going to calculate the discriminant $\mathfrak{D}_{B/\mathbb{Z}}$ by making use of the formula

$$D(1, \zeta, \ldots, \zeta^{p-2}) = (-1)^{\frac{1}{2}(p-1)(p-2)} \operatorname{Nm}(F'(\zeta)) \quad \text{(Formula 2.7.15)}.$$

By taking the derivative of both sides of the relation $(X-1)F(X) = X^p - 1$, we obtain $(\zeta - 1)F'(\zeta) = p\zeta^{p-1}$ (since $F(\zeta) = 0$). We know that $\operatorname{Nm}(p) = p^{p-1}, \operatorname{Nm}(\zeta) = \pm 1$, and $\operatorname{Nm}(\zeta - 1) = \pm p$ (Section 2.9). Therefore,

$$D(1, \zeta, \ldots, \zeta^{p-2}) = \pm p^{p-2}. \tag{5.3.11}$$

It follows that p is the only prime number which ramifies in $\mathbb{Q}[\zeta]$,

The following result is sometimes useful for determining the ring of integers of a number field.

Proposition 5.3.12. *Let L be a number field of degree n over $\mathbb{Q}$ and let $(x_1, \ldots, x_n)$ be a $\mathbb{Q}$-basis for L contained in the ring B of integers of L. If the discriminant $D(x_1, \ldots, x_n)$ is square-free, then $(x_1, \ldots, x_n)$ is a $\mathbb{Z}$-basis for B.*

Proof. If $(e_1, \ldots, e_n)$ is a $\mathbb{Z}$-basis for B, then $x_i = \sum_{j=1}^n a_{ij} e_j$ with $a_{ij} \in \mathbb{Z}$, whence

$$D(x_1, \ldots, x_n) = \det(a_{ij})^2 D(e_1, \ldots, e_n).$$

Since $D(x_1, \ldots, x_n)$ is square-free, $\det(a_{ij})$ must be ± 1, so $(x_1, \ldots, x_n)$ is also a $\mathbb{Z}$-basis for B. □

Remark 5.3.13. The cyclotomic fields (for $p \geq 5$), or quadratic fields, provide examples which show that the sufficient condition of Proposition 5.3.12 is not a necessary condition.

Example 5.3.14. The polynomial $X^3 - X - 1$ (respectively, $X^3 + X + 1, X^3 + 10X + 1$) is *irreducible* over $\mathbb{Q}$. Otherwise it would have a linear factor, i.e. a rational root $x \in \mathbb{Q},$. But, the polynomial is monic, so $x \in \mathbb{Q}$, implies $x \in \mathbb{Z}$. The constant term of the polynomial is 1, so $x = \pm 1$ (x has to divide the constant term). Checking that neither ± 1 satisfies the polynomial, we may conclude that the polynomial is irreducible. Now let x be a complex root of the given polynomial. The field $L = \mathbb{Q}[x]$ is a *cubic field* (i.e. of degree 3). Thus, $(1, x, x^2)$ is a basis for L over $\mathbb{Q}$, and x is, clearly, an integer of L. By formula 2.7.16, $D(1, x, x^2) = 4 - 27 = -23$ (respectively $-31, -4027$), the negative of a prime number. Therefore, $(1, x, x^2)$ is a $\mathbb{Z}$-basis for the ring of integers of L.

5.4 The splitting of a prime number in a quadratic field

Let $d \in \mathbb{Z}$ be square-free, let L be the quadratic field $\mathbb{Q}[\sqrt{d}]$, write B for the ring of integers of L, and let p be a prime number. We are going to study the factorisation of the ideal pB into a product of prime ideals of B.

The formula $\sum_{i=1}^{q} e_i f_i = 2$ (Theorem 5.2.3) shows that $q \leq 2$ and the following three are possible:

(a) $q = 2, e_1 = e_2 = 1, f_1 = f_2 = 1$;
in this case we say that p *splits* in L.

(b) $q = 1, e_1 = 1, f_1 = 2$;
in this case we say that f *is inert* (or *remains prime*) in L.

(c) $q = 1, e_1 = 2, f_1 = 1$;
this means that p *ramifies* in L.

Remark 5.4.1. Before starting the investigation, let us remark that there are situations in which things work differently according to the *parity* of the prime numbers in question. Thus we consider the following two cases separately:

1. the prime p is odd,
2. the prime $p = 2$.

The *case in which p is odd*: We know (Section 2.5) that $B = \mathbb{Z} + \mathbb{Z}\sqrt{d}$ or $B = \mathbb{Z} + \mathbb{Z}((1 + \sqrt{d})/2)$ depending upon the value of d. But, if wc pass to the residue classes of B mod Bp, we see in the second case that $a + b((1 + \sqrt{d})/2)$ (with b odd) is congruent to $a + (b + p)((2 + \sqrt{d})/2)$, which belongs to $\mathbb{Z} + \mathbb{Z}\sqrt{d}$. Thus for any d, we have

$$B/Bp \cong (\mathbb{Z} + \mathbb{Z}\sqrt{d})/p(\mathbb{Z} + \mathbb{Z}\sqrt{d}).$$

Also we see that

$$\mathbb{Z} + \mathbb{Z}\sqrt{d} \cong \mathbb{Z}[X]/(X^2 - d)\mathbb{Z}[X].$$

So

$$\begin{aligned} B/Bp &\cong \mathbb{Z}[X]/(p, X^2 - d)\mathbb{Z}[X] \\ &\cong (\mathbb{Z}[X]/p\mathbb{Z}[X])/(X^2 - d)\mathbb{Z}[X] \\ &\cong \mathbb{F}_p[X]/(X^2 - \overline{d})\mathbb{F}_p[X], \end{aligned}$$

where $\overline{d}$ denotes the residue class of d mod p. Now the assertion that p splits (respectively, remains prime, ramifies) in B has the interpretation B/Bp is the product of two fields (respectively, is a field, contains nilpotent elements) (cf. Proposition 5.2.5). In other words, the polynomial $X^2 - \overline{d} \in \mathbb{F}_p[X]$ is the product of two distinct linear polynomials (respectively, is irreducible, is a square). This

happens if $\overline{d}$ is a non-zero square in $\mathbb{F}_p$ (respectively, is not a square in $\mathbb{F}_p$, is zero in $\mathbb{F}_p$). When $\overline{d}$ is a non-zero square in $\mathbb{F}_p$ (respectively, is not a square in $\mathbb{F}_p$), we say that d is a *quadratic residue* (respectively, *non-residue*) modulo p.

Let us now consider the *case* $p = 2$.
If $d \equiv 2$ or $3 \bmod 4$, then $B = \mathbb{Z} + \mathbb{Z}\sqrt{d}$, so, as above, $B/2B \cong \mathbb{F}_2[X]/(X^2 - 1)\mathbb{F}_2[X]$. In this case $X^2 - 2$ equals X^2 or $X^2 - 1 = (X + 1)^2$, in either case a square. Thus 2 ramifies in B.
If $d \equiv 1 \bmod 4$, $(1 + \sqrt{d})/2$ has $X^2 - X - (d - 1)/4$ as its minimal polynomial, so, as above, $B/2B \cong \mathbb{F}_2[X]/(X^2 - X - \delta)\mathbb{F}_2[X]$, where δ is the residue class mod 2 of $(d - 1)/4$.
For $d \equiv 1 \bmod 8$, we have $\delta = 0$ and $X^2 - X - \delta = X(X - 1)$, so that 2 splits.
For $d \equiv 5 \bmod 8$, $\delta = 1$ and $X^2 - X - \delta = X^2 + X + 2$, which is irreducible in $\mathbb{F}_2[X]$, so 2 remains prime.

In summary, we have proved the following:

Proposition 5.4.2. *LeT $L = \mathbb{Q}[\sqrt{d}]$ the quadratic field associated with the square-free integer d.*

(a) The odd primes p for which d is a quadratic residue mod p split in L. So does 2 if $d \equiv 1 \bmod 8$.

(b) The odd primes p for which d is not a quadratic residue mod p remain prime in L. So does 2, if $d \equiv 5 \bmod 8$.

(c) The odd prime divisors of d ramify in L. So does 2, if $d \equiv 2$ or $3 \bmod 4$.

Part (c) was proved earlier in Example 5.3.9.

5.5 The quadratic reciprocity law

Given an odd prime p and an integer d relatively prime to p we introduced in Section 5.4 the statement "d is a *quadratic residue* mod p" (respectively, "d is a non-residue mod p") as meaning that the residue class of d mod p is a square (respectively, not a square) in $\mathbb{F}_p^\times$. Now we define the *Legendre symbol* (d/p) as follows:

$$\left(\frac{d}{p}\right) = \begin{cases} +1 & \text{if } d \text{ is a quadratic residue mod } p, \\ -1 & \text{if } d \text{ is a non-residue mod } p \end{cases} \tag{5.5.1}$$

It is understood that (d/p) is defined only for integers d which are relatively prime to p, i.e. for $d \in \mathbb{Z} \setminus p\mathbb{Z}$. The multiplicative group $\mathbb{F}_p^\times$ being cyclic of even order $p - 1$ (Theorem 1.7.3), the squares in $\mathbb{F}_p^\times$ form a subgroup $\mathbb{F}_p^{\times 2}$ of index 2, and $\mathbb{F}_p^\times/\mathbb{F}_p^{\times 2}$ is isomorphic to $\{+1, -1\}$. Clearly, the Legendre symbol stands for the composition of the following homomorphisms

$$\mathbb{Z} \setminus p\mathbb{Z} \to \mathbb{F}_p^\times \to \mathbb{F}_p^\times/\mathbb{F}_p^{\times 2} \xrightarrow{\sim} \{+1, -1\}.$$

As a consequence there is the formula:

$$\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right). \tag{5.5.2}$$

Proposition 5.5.3 (Euler's criterion). *If p is an odd prime and if $a \in \mathbb{Z} \setminus p\mathbb{Z}$, then we have*

$$\left(\frac{a}{p}\right) \equiv a^{(p-1)/2} \bmod p.$$

Proof. Write w for a primitive root mod p (Section 1.7). Then $a \equiv w^j \bmod p$, with $0 \leq j \leq p-2$, since the residue class $\overline{w}$ of w generates $\mathbb{F}_p^\times$. Clearly, a is a quadratic residue if and only if j is even. Therefore, $(a/p) = (-1)^j$. On the other hand, $\mathbb{F}_p^\times$ contains only one element of order 2: this element can be written either as $\overline{w}^{(p-1)/2}$ or -1 as its square is 1. In $\mathbb{Z}$, we have $-1 \equiv w^{(p-1)/2} \bmod p$. Thus

$$\left(\frac{a}{p}\right) = (-1)^j \equiv w^{j\cdot(p-1)/2} \equiv a^{(p-1)/2} \bmod p.$$

□

Now we are going to prove a famous theorem, which provides us with a relation between the Legendre symbols for distinct odd primes.

Theorem 5.5.4 (The quadratic reciprocity law of Legendre-Gauss). *If p and q are distinct odd prime numbers, then*

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

Proof. Let us consider, in a suitable extension of $\mathbb{F}_p$, a primitive pth root of unity w. Since $w^p = 1$, the expression w^x is well defined for $x \in \mathbb{F}_p$. We shall also consider the Legendre symbol (x/p) as defined on $x \in \mathbb{F}_p^\times$, for (d/p) clearly depends only on the residue class of d mod p. For $a \in \mathbb{F}_p^\times$ consider the "Gaussian sum"

$$\tau(a) = \sum_{x \in \mathbb{F}_p^\times} \left(\frac{x}{p}\right) w^{ax}. \tag{5.5.5}$$

It is an element of an extension field of $\mathbb{F}_q$, Putting $ax = y$, we have

$$\tau(a) = \sum_{y \in \mathbb{F}_p^\times} \left(\frac{ya^{-1}}{p}\right) w^y = \left(\frac{a^{-1}}{p}\right) \sum_{y \in \mathbb{F}_p^\times} \left(\frac{y}{p}\right) w^y \quad \text{(by 5.5.2)}$$

so

$$\tau(a) = \left(\frac{a}{p}\right) \tau(1). \tag{5.5.6}$$

On the other hand, since we are working in a field of characteristic q and since $(x/p) \in \mathbb{F}_q^\times$, we have $\tau(1)^q = \sum_{x \in \mathbb{F}_p^\times} (x/p)^q w^{qx}$, so, identifying q with its residue class mod p, we obtain

$$\tau(1)^q = \tau(q). \tag{5.5.7}$$

Let us calculate $\tau(1)^2$. We have

$$\tau(1)^2 = \sum_{x,y \in \mathbb{F}_p^\times} \left(\frac{x}{p}\right)\left(\frac{y}{p}\right) w^{x+y}.$$

Putting $y = tx$, we see that

$$\begin{aligned}\tau(1)^2 &= \sum_{x,y\in\mathbb{F}_p^\times} \left(\frac{x}{p}\right)^2 \left(\frac{t}{p}\right) \\ &= \sum_{x,t} \left(\frac{t}{p}\right) w^{x(1+t)} \\ &= \sum_{t\in\mathbb{F}_p^\times} \left[\left(\frac{t}{p}\right) \sum_{x\in\mathbb{F}_p^\times} w^{x(1+t)}\right]\end{aligned}$$

If $w^{1+t} \neq 1$, then $\sum_{j=0}^{p-1}(w^{1+t})^j = 0$ by the formula for summing a geometric series. Since $(w^{1+t})^0 = 1$, we have

$$\sum_{x\in\mathbb{F}_p^\times} w^{x(1+t)} = -1 \quad \text{if} \quad w^{1+t} \neq 1.$$

If $w^{1+t} = 1$, then $\sum_{x\in\mathbb{F}p^\times} = p - 1$; and this happens if and only if $t = -1$, since w is a primitive pth root of unity. Therefore,

$$\tau(1)^2 = \left(\frac{-1}{p}\right)(p-1) - \sum_{t\in\mathbb{F}_p^\times, t\neq -1} \left(\frac{t}{p}\right).$$

As there are as many squares as non-squares in $mathbbF_p^\times$, we have

$$\sum_{t\in\mathbb{F}_p^\times} \left(\frac{t}{p}\right) = 0, \quad \text{so}$$

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

Using Euler's criterion (Proposition 5.5.3), wc obtain

$$\tau(1)^2 = (-1)^{(p-1)/2}p. \tag{5.5.8}$$

Finally, using (5.5.6) and (5.5.7), we see that

$$\tau(1)^q = \tau(q) = \left(\frac{q}{p}\right)\tau(1).$$

By (5.5.8), $\tau(1) \neq 0$, so we may simplify

$$\tau(1)^{q-1} = \left(\frac{q}{p}\right).$$

Use of (5.5.8) again yields

$$\left(\frac{q}{p}\right) = (\tau(1)^2)^{(q-1)/2} = (-1)^{(p-1)(q-1)/4}p^{(q-1)/2}.$$

Since $p^{(q-1)/2} = (q/p)$ (Proposition 5.5.3) and since $(p/q) = (p/q)^{-1}$, we have proved the quadratic reciprocity law. □

Proposition 5.5.9 (The complementary formulae)**.** *If p is an odd prime, then we have*

(a) $\left(\frac{-1}{p}\right) = (-1)^{(p-1)/2}$

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

Proof. Relation (a) is a special case of Euler's criterion (Proposition 5.5.3). We need only prove (b). Note first that, since the squares of $1, 3, 5$, and 7 mod 8 are $1, 1, 1$, and 1, we have $p^2 \equiv 1 \bmod 8$, so formula (b) makes sense. Let us remark next that, in the group $H = \{1, 3, 5, 7\}$ of units in the ring $\mathbb{Z}/8\mathbb{Z}$, $\{1, 7\}$ is a subgroup H' of index 2. Put $\theta(x) = 1$ for $x \in H'$ and $\theta(x) = -1$ for $x \in H \setminus H'$, so that $\theta(xy) = \theta(x)\theta(y)$ for $x, y \in H$. Let w be a primitive eighth root of unity in an extension of $\mathbb{F}_p$. As in Theorem 5.5.4 consider, for $a \in H$, the "Gaussian sum"

$$\tau(a) = \sum_{x \in H} \theta(x) w^{ax}. \tag{5.5.10}$$

As in Theorem 1 we see that $\tau(a) = \theta(a)\tau(1)$ and $\tau(1)^p = \tau(p)$ (identifying p with its residue class mod 8). From the definition of $\theta(x)$ we obtain

$$\begin{aligned} \tau(1)) &= w - w^2 - w^5 + w^7 = (a - w^2)(w - w^5) \\ &= w(1 - w^2)(1 - w^4) = 2w(1 - w^2), \end{aligned}$$

since $w^8 = 1$ and $w^4 = -1$. Consequently,

$$\tau(1)^2 = 4w^2(1 - 2w^2 + w^4) = -8w^4 = 8.$$

As in Theorem 5.5.4 we show that

$$\tau(1)^p = \tau(p) = \theta(p)\tau(1).$$

Next we see that

$$\begin{aligned} \theta(p) = (\tau(1)^2)^{(p-1)/2} = 8^{(p-1)/2} &= \left(\frac{8}{p}\right) \quad \text{(Proposition 5.5.3)} \\ &= \left(\frac{2}{p}\right)^3 = \left(\frac{2}{p}\right). \end{aligned}$$

Therefore $(2/p) = \theta(p)$. Now, by a direct calculation involving $x = 1, 3, 5, 7$ (or more easily, $x = 1, 3, -3, -1$), we haven that $\theta(x) = (-1)(x^2 - 1)/8$ and that $(x^2 - 1)/8$ depends only on the residue class of x mod 8. □

Example 5.5.11 (An application of the reciprocity law). The law of quadratic reciprocity and the complementary formulae make it possible to calculate the

Legendre symbol by successive reductions. Let us calculate (23/59) without computing squares modulo 59.

$$\begin{aligned}\left(\frac{23}{59}\right) &= (-1)^{11\cdot 29}\left(\frac{59}{23}\right) = -(-1)^{6\cdot 11}\left(\frac{23}{13}\right)\\ &= -\left(\frac{10}{13}\right) = -\left(\frac{-3}{13}\right) = -\left(\frac{-1}{13}\right)\left(\frac{3}{13}\right)\\ &= -(-1)^6\left(\frac{3}{13}\right) = -(-1)^{6\cdot 1}\left(\frac{13}{3}\right) = -\left(\frac{1}{3}\right) = -1.\end{aligned}$$

Thus 23 is not a square modulo 59.

5.6 The two-squares theorem

We are going to apply Proposition 5.4.2 to the field $L = \mathbb{Q}[i]$ where $i^2 = -1$. Since $-1 = 3 \bmod 4$ the ring B of integers of L is $\mathbb{Z} + \mathbb{Z}i$. This ring is called the *ring of Gaussian integers*. Its discriminant is -4 Example 5.3.9). If p is an odd prime number and if u is a generator of the cyclic group $\mathbb{F}_p^\times$, then $-1 = u^{(p-1)/2}$. Therefore, -1 is a square in $\mathbb{F}_p$ if and only if $(p-1)/2$ is even. We have the following classification for prime numbers:

- 2 ramifies in $\mathbb{Q}[i]$;
- the primes of the form $4k+1$ split; and
- the primes of the form $4k+3$ remain prime

The following result will prove useful.

Proposition 5.6.1. *The ring $B = \mathbb{Z} + \mathbb{Z}i$ of Gaussian integers is a PID.*

Proof. We use the full force of an earlier result to prove this easy proposition. With the notations of Section 4.3, we have $n = 2, r_1 = 0, r_2 = 1$, and $d = -4$. Therefore (Proposition 4.3.5), every ideal class of B contains an integral ideal of norm $\leq \frac{4}{\pi}\cdot\frac{2}{4}|4|^{1/2} = \frac{4}{\pi}$. Therefore, every ideal class contains the unit ideal, B itself, which is the only integral ideal of norm 1 (note that $4/\pi < 2$). Thus every ideal of B is equivalent to the principal ideal $B\cdot 1$, so B is a PID. □

Remark 5.6.2 (A sketch of an elementary proof). The points of B may be identified with $\mathbb{Z}^2 \subset \mathbb{R}^2 = \mathbb{C}$. With the usual identification of R^2 with the plane (the square of Euclidean distance is the norm in $\mathbb{Q}[i]$) the points of $\mathbb{Z}^2$ become the vertices of squares covering the plane. A little geometry shows that, for any $x \in \mathbb{Q}[i]$, there exists $z \in B$ such that $\mathrm{Nm}(x-z) = |x-z|^2 \leq (1/\sqrt{2})^2 = 1/2 < 1$. Now in $\mathfrak{a}$, a non-zero ideal of B, choose a non-zero element u of minimum norm (NB. the norm is a positive integer-valued function on $\mathbb{Z}[i]\setminus(0)$). For any $v \in \mathfrak{a}$ there is a $z \in B$ such that $\mathrm{Nm}(v/u - z) < 1$. Therefore, $\mathrm{Nm}(v - zu) < \mathrm{Nm}(u)$, so $v - zu = 0$ (since $v - zu \in \mathfrak{a}$). Consequently, $v \in Bu$ and $\mathfrak{a} = Bu$. The reader will observe the analogy with the proof that $\mathbb{Z}$ is a PID (Section 1.1).

Proposition 5.6.3 (Fermat)**.** *Any prime number $p \equiv 1 \bmod 4$ may be represented as the sum of two squares (i.e. is of the form $p = a^2 + b^2$ with $a, b \in \mathbb{N}$).*

Proof. In fact we have the decomposition $Bp = \mathfrak{p}_1\mathfrak{p}_2$ into a product of distinct prime ideals. Clearly $p^2 = \mathrm{Nm}(Bp) = \mathrm{Nm}(\mathfrak{p}_1)\,\mathrm{Nm}(\mathfrak{p}_2)$ (by Proposition 3.5.3). As the norms of $\mathfrak{p}_1$ and $\mathfrak{p}_2$ are larger than 1, necessarily $\mathrm{Nm}(\mathfrak{p}_1) = \mathrm{Nm}(\mathfrak{p}_2) = p$. Now, $\mathfrak{p}_1$ is a principal ideal $B \cdot (a + bi)$ (where $a, b \in \mathbb{Z}$) (Proposition 5.6.1), so $p = \mathrm{Nm}(a + bi) = a^2 + b^2$. □

Theorem 5.6.4. *Let x be a natural number and let $x = \prod_p p^{v_p(x)}$ be its expression as a product of powers of primes. For x to be a sum of two squares it is necessary and sufficient that, for every $p \equiv 3 \bmod 4$, the exponent $v_p(x)$ be even.*

Proof. In order to prove sufficiency we note that a sum of two squares $a^2 + b^2$ is the norm $\mathrm{Nm}(a + bi)$ of an element of B. By the multiplicativity of norms, the set S of sums of two squares is itself stable under multiplication. Since $2 = 1^2 + 1^2 \in S$ and since any square is also an element of S ($x^2 = x^2 + 0^2$), sufficiency follows from Proposition 5.6.3.

Conversely let $x = a^2+b^2 = (a+bi)(a-bi)$ be a sum of two squares ($a, b \in \mathbb{N}$) and let p be a prime number $\equiv 3 \bmod 4$. We have seen that the ideal Bp of B is prime (Proposition 5.4.2). Let n be the exponent of Bp in the expression for $B \cdot (a + bi)$ as a product of primes. As Bp is stable under the automorphism $\sigma\colon u + iv \mapsto u - iv$ of B, and since $\sigma(a + bi) = a - bi$, the exponent of Bp in the expression for $B(a - bi)$ is also n. Therefore, in the expression for $B(a^2 + b^2)$, the exponent for Bp is $2n$. As no prime number besides p belongs to Bp (for $Bp \cap \mathbb{Z} = p\mathbb{Z}$), we see that $v_p(x) = 2n$ and $v_p(x)$ is even. □

5.7 The four-squares theorem

In this section we intend to prove the following theorem:

Theorem 5.7.1 (Lagrange)**.** *Every natural number may be represented as the sum of four squares.*

The idea behind this proof is analogous to that of Section 5.6: in place of the ring of Gaussian integers, we will work in a suitably chosen ring of *quaternions*.

Let us begin with a definition of quaternions. Given a ring A, we will write $(1, i, j, k)$ for the canonical basis of the A-module A^{4*} and define a multiplication on A^4 as follows:

$$\begin{aligned} &1 \text{is the unit element,} \\ &i^2 =_j^2= k^2 = -1. \\ &ij = -ji = k, \quad jk = -kj = i, \quad \text{and} \quad ki = -ik = j. \end{aligned} \tag{5.7.2}$$

We extend this multiplication to elements $a + bi + cj + dk$ of A^4 by linearity. Distributivity is then clear. It suffices to verify associativity for elements of the

basisi, e.g. $i(jk) = i^2 = -1 = k^2 = (ij)k$. The formulae in which 1 appears being clear, there remain $3^3 - 1 = 26$ formulae to check. The patient and incredulous reader will reduce the number of formulas by the use of permutations and check those which remain. Others will accept the author's claim that the given multiplication is associative. Provided with this multiplication, A^4 is a *not necessarily commutative* ring, and even an A-*algebra*, which we call the *algebra of quaternions* over A, denoted by $\mathbb{H}(A)$ ($\mathbb{H}$ in honor of W. R. Hamilton, the inventor of quaternions).

Given a quaternion$z = a+bi+cj+dk$ over A (we write a in place of $a\cdot 1$), we define the conjugate quaternion of $\overline{z}$ to be the quaternion $\overline{z} = a - bi - cj - dk$.

Lemma 5.7.3. *For any z and $z' \in \mathbb{H}(A)$, we have $\overline{z+z'} = \overline{z} + \overline{z'}, \overline{zz'} = \overline{z'}\overline{z}$, and $\overline{\overline{z}} = z$. In other words, $z \mapsto \overline{z}$ is an involutive antiautomorphism of $\mathbb{H}(A)$.*

Proof. The first and the third formulae are clear. By linearity we see that to prove the second it suffices to check that $\overline{xy} = \overline{y} \cdot \overline{x}$ for $x, y \in \{1, i, j, k\}$. This is clear if $x = 1$ or $y = 1$. If $x = y = i$, then

$$\overline{xy} = 1\overline{1} \quad \text{and} \quad \overline{yx} = (-i)(-i) = i^2 = -1.$$

If $x = i$ and $y = j$, then

$$\overline{xy} = \overline{k} = -k \quad \text{and} \quad \overline{yx} = (-j)(-i) = ji = -k.$$

The others follow by a permutation argument. □

Given a quaternion z over A, we call the quaternion $\mathrm{Nm}(z) = z\overline{z}$ the *reduced norm* of z.

Lemma 5.7.4. *(a) For $z = a+bi+cj+dk \in \mathbb{H}(A)$, $\mathrm{Nm}(z) = a^2+b^2+c^2+d^2$ (four squares!), an element of A.*

(b) For $z, z' \in \mathbb{H}(A)$, we have $\mathrm{Nm}(zz') = \mathrm{Nm}(z)\,\mathrm{Nm}(z')$.

Proof. (a): We observe that, in the expansion of $(a+bi+cj+dk)(a-bi-cj-dk)$, the cross-product terms cancel, leaving $a^2 + b^2 + c^2 + d^2$.
(b): Observe that

$$\mathrm{Nm}(zz') = zz' \cdot \overline{zz'} = zz'\overline{z'}\overline{z} = z\,\mathrm{Nm}(z')\overline{z} = z\overline{z}\,\mathrm{Nm}(z')$$

(since $\mathrm{Nm}(z') \in A$ and any element of A commutes with every quaternion), so $\mathrm{Nm}(zz') = \mathrm{Nm}(z)\,\mathrm{Nm}(z')$. □

Remark 5.7.5. Lemma 5.7.4 implies that, for a (commutative) ring A, the set of reduced norms of quaternions, i.e. sums of four squares, is stable under multiplication.

Now we shall study in greater detail the quaternion algebra $\mathbb{H}(\mathbb{Q})$, the non-commutative subring $H(\mathbb{Z})$, and the subset $\mathbb{H}$ of "quaternions of Hurwitz", i e the quaternions of the form $a + bi + cj + dk$, where either a, b, c, and d belong to Z or all four coefficients belong to $\frac{1}{2} + \mathbb{Z}$.

Lemma 5.7.6. *(a) The set $\mathbb{H}$ of Hurwitz quaternions is a non-commutative subring of $\mathbb{H}(\mathbb{Q})$ containing $\mathbb{H}(\mathbb{Z})$ and stable under conjugation $z \mapsto \overline{z}$.*

(b) For any $z \in \mathbb{H}$, $z + \overline{z} \in \mathbb{Z}$ and $\mathrm{Nm}(z) = z\overline{z} \in \mathbb{Z}$.

(c) In order that $z \in \mathbb{H}$ be invertible, it is necessary and sufficient that $\mathrm{Nm}(z) = 1$.

(d) Every left ideal (respectively, right ideal) $\mathfrak{a}$ of $\mathbb{H}$ is principal, i.e. of the form $\mathbb{H}z$ (respectively, $z\mathbb{H}$).

Proof. (a): All assertions are clear except the stability of $\mathbb{H}$ under multiplication. To complete the proof of (a) it suffices to show that, for

$$u = \frac{1}{2}(1 + i + j + k),$$

we have $u \cdot 1, u \cdot i, u \cdot j, u \cdot k$, and $u^2 \in \mathbb{H}$. We have

$$\begin{aligned} u \cdot 1 &= \frac{1}{2}(1 + i + j + k), \\ u \cdot i &= \frac{1}{2}(-1 + i + j - k), \\ u \cdot j &= \frac{1}{2}(-1 - i + j + k), \quad \text{and} \\ u \cdot k &= \frac{1}{2}(-1 + i - j + k); \end{aligned}$$

all elements of $\mathbb{H}$. By addition, $2u^2 = \frac{1}{2}(-2 + 2i + 2j + 2k)$, so $u^2 \in \mathbb{H}$, too.
(b): Let

$$z = \frac{1}{2} + a + (i + b)i + (i + c)j + (i + d)k, \quad \text{with} \quad a, b, c, d \in \mathbb{Z}.$$

Then

$$z + \overline{z} = 1 + 2a \in \mathbb{Z}$$

and

$$Z\overline{z} = \left(\frac{1}{2} + a\right)^2 + \left(\frac{1}{2} + b\right) + \left(\frac{1}{2} + c\right)^2 + \left(\frac{1}{2} + d\right)^2 \in \frac{4}{4} + \mathbb{Z} \subset \mathbb{Z}.$$

The preceding formula follows from Lemma 5.7.4.
(c) ($\Rightarrow$): If z is invertible in $\mathbb{H}$ and if $z' = z^{-1}$, then

$$\mathrm{Nm}(z)\,\mathrm{Nm}(z') = \mathrm{Nm}(zz') = 1.$$

Since $\mathrm{Nm}(z)$ and $\mathrm{Nm}(z')$ are both positive integers (b) and Lemma 5.7.4, (a), $\mathrm{Nm}(z)) = 1$.
($\Leftarrow$): If $z \in mathbbH$ and if $\mathrm{Nm}(z) = 1$, then

$$z\overline{z} = \overline{z}z = \mathrm{Nm}(z) = 1,$$

so, since $\overline{z} \in \mathbb{H}$ by (a), z is invertible in $\mathbb{H}$. This proves (c).
(d): Take $x = a + bi + cj + dk \in \mathbb{H}(\mathbb{Q})$. There exist $a', b', c', d' \in \mathbb{Z}$ such that

$$|a - a'| \leq \frac{1}{2}, \quad |b - b'| \leq \frac{1}{2}, \quad |c - c'| \leq \frac{1}{2}, \quad \text{and} \quad |d - d'| \leq \frac{1}{2}.$$

Put $z = a' + b'i + c'j + d'k$. Then

$$\mathrm{Nm}(x - z) = (a - a')^2 + (b - b')^2 + (c - c')^2 + (d - d')^2 \leq 4 \cdot \frac{1}{4} = 1.$$

The inequality is even strict, except when a, b, c, and d all belong to $\frac{1}{2} + \mathbb{Z}$. But in this case $x \in \mathbb{H}$. Thus, for any quaternion $x \in \mathbb{H}(\mathbb{Q})$, there exists a Hurwitz quaternion $z \in \mathbb{H}$ such that $\mathrm{Nm}(x - z) < 1$ (it is precisely because we must have strict inequality that we work with the Hurwitz quaternions; $\mathbb{H}(\mathbb{Z})$ would not be sufficient). Now let $\mathfrak{a}$ be a left ideal of $\mathbb{H}$. To show that $\mathfrak{a}$ is principal we may assume $\mathfrak{a} \neq (0)$. Choose in $\mathfrak{a}$ a non-zero element u for which $\mathrm{Nm}(u)$ is a minimum (such u exists, since the reduced norm is a positive integer-valued function on $\mathbb{H} \setminus (0)$, by (b)). Clearly, u is invertible in $\mathbb{H}(\mathbb{Q})$ with inverse $\overline{u}\,\mathrm{Nm}(u)^{-1}$ (this shows that $\mathbb{H}(\mathbb{Q})$ is a skew field). For $y \in \mathfrak{a}$ form $yu^{-1} \in \mathbb{H}(\mathbb{Q})$ and take an element $z \in \mathbb{H}$ such that $\mathrm{Nm}(yu^{-1} - z) < 1$. Then, by Lemma 5.7.4, (b), we have

$$\mathrm{Nm}(y - zu) = \mathrm{Nm}((yu^{-1} - z)u) < \mathrm{Nm}(u).$$

Since $y - zu \in \mathfrak{a}$ and since $\mathrm{Nm}(u)$ is as small as possible, it follows that $y - zu = 0, y \in \mathbb{H}u$, and $\mathfrak{a} = \mathbb{H}u$. □

Now we are ready to prove Theorem 5.7.1. Since the set of elements of $\mathbb{Z}$ which are sums of four squares is multiplicatively stable (cf. Lemma 5.7.4), Theorem 5.7.1 follows from the following proposition.

Proposition 5.7.7. *Any prime number is the sum of four squares.*

Proof. Since $2 = 1^2 + 1^2 + 0^2 + 0^2$, we may suppose that p is odd. Since p commutes with any quaternion, the left ideal $\mathbb{H}p$ is two-sided. Consider the residue class ring $\mathbb{H}/\mathbb{H}p$. Since p is odd, any $z \in \mathbb{H}$ is congruent mod $\mathbb{H}p$ to an element of $\mathbb{H}(\mathbb{Z})$ (if the components of z all belong to $\frac{1}{2} + \mathbb{Z}$, form $z + p \cdot \frac{1}{2}(1 + i + j + k)$). Therefore, H/Hp is isomorphic to the corresponding residue class ring of $\mathbb{H}(\mathbb{Z})$, i.e. $\mathbb{H}(\mathbb{F}_p)$.

Since the quadratic form $a^2 + b^2 + c^2 + d^2$ represents 0 in $\mathbb{F}_p$, (Theorem 1.7.6; see the remark below for a direct proof), $\mathbb{H}(\mathbb{F}_p)$ contains a non-zero element of reduced norm zero. Such an element is not invertible (Lemma 5.7.4, (b)), so it generates a non-trivial left ideal. It follows that $\mathbb{H}p$ is properly contained in a left ideal $\mathbb{H}z$ distinct from $\mathbb{H}$. Consequently, $p = z'z$ for some $z, z' \in \mathbb{H}$ both non-units. Thus,

$$p^2 = \mathrm{Nm}(p) = \mathrm{Nm}(z)\,\mathrm{Nm}(z')$$

and, since $\mathrm{Nm}(z)$ and $\mathrm{Nm}(z')$ are both integers strictly larger than one (Lemma 5.7.6, (b) and (c)), $\mathrm{Nm}(z) = \mathrm{Nm}(z') = p$.

Put $z = a + bi + cj + dk$ ($a, b, c, d \in \mathbb{Z}$ or in $\frac{1}{2} + \mathbb{Z}$). If $a, b, c, d \in \mathbb{Z}$, then $p = \mathrm{Nm}(z) = a^2 + b^2 + c^2 + d^2$ and we are finished. It suffices to show that, if $a, b, c, d \in \frac{1}{2} + \mathbb{Z}$, we may make a reduction to the preceding case by multiplying z by an element of $\mathbb{H}$ of reduced norm 1, more precisely by an element of the form $\frac{1}{2}(\pm 1 \pm i \pm j \pm k)$. To see this consider the residue class η associated with $2z$ in $\mathbb{H}(\mathbb{Z})/4\mathbb{H}(\mathbb{Z}) \cong \mathbb{H}(\mathbb{Z}/4\mathbb{Z})$. Since $\mathrm{Nm}(z) \in \mathbb{Z}$, we have $\mathrm{Nm}(2z) \in 4\mathbb{Z}$, so $\mathrm{Nm}(\eta) = 0$ and $\eta\overline{\eta} = 0$. We observe that $\overline{\eta}$ is the residue class of a quaternion z' of the form $\pm 1 \pm i \pm j \pm k$. Set $u = \frac{1}{2}z' \in \mathbb{H}$; then u is of reduced norm 1 and, inasmuch as $(2z) \cdot (2u) \equiv 0 \bmod 4$, we have $zu \in \mathbb{H}(\mathbb{Z})$. Now $p = \mathrm{Nm}(z) = \mathrm{Nm}(zu)$, so we are finished. □

Remark 5.7.8. Here is a very elementary proof of the fact that, over a finite field K, the quadratic form $a^2 + b^2 + c^2 + d^2$ represents 0 (i.e. has a non-trivial zero in K^4).

Proof. It suffices to take $c = 1$ and $d = 0$ and to show that the equation $a^2 + b^2 + 1 = 0$ has a solution in K^2. Write this equation in the form $b^2 + 1 = -a^2$. In characteristic 2, we may take $4 = 0$ and $a = 1$. If $\mathrm{card}(K) = q$ is odd, there are $(q+1)/2$ squares in K (0 and the $(q-1)/2$ non-zero squares). Thus the set T (respectively, T') of elements of K of the form $b^2 + 1$ with $b \in K$ (respectively, of the form $-a^2$ with $a \in K$) consists of $(q+1)/2$ elements. Since $(q+q)/2 + (q+2)/2 > q$, we have $T \cap T' \neq \varnothing$, so $b^2 + 1 = -a^2$ has a solution. □

Chapter 6

Galois extensions of number fields

6.1 Galois theory

This section is a supplement to the general theory of commutative fields presented in Sections 2.3, 2.4, 2.6 and 2.7. Given a field L and a set G of automorphisms of L, one sees immediately that the set of all $x \in L$ such that $\sigma(x) = x$ for all $\sigma \in G$ is a *subfield* of L, called the *fixed field* of G, written $\mathrm{Fix}_G(L)$. It is also clear that, for an extension L of a field K, the set of K-automorphisms of L is a *group* under composition of mappings.

Theorem 6.1.1. *Let L be an extension of finite degree n of a field K, where K is finite or of characteristic 0. The following conditions are equivalent:*

(a) K is the fixed field of the group G of K-automorphisms of L: $K = \mathrm{Fix}_G(L)$.

(b) For every $x \in L$, the minimal polynomial of x over K has all its roots in L.

(c) L is generated by the roots of a polynomial with coefficients in K.

Under the above conditions the group G of K-automorphisms of L is of order n.

Proof. (a) implies (b): Observe that, for x$\in$ L, the polynomial $\prod_{\sigma \in G}(X - \sigma(x)) = P(X)$ is invariant under G (since any element of G permutes the factors).[1] Therefore, the coefficients of $P(X)$ belong to K. Since x is a root of $P(X)$ (G contains an identity element), the minimal polynomial of x divides $P(X)$ (2.3.7). Therefore, (a) implies (b).
(b) implies (c): Take a primitive element x of L over K (Corollary 2.4.6). Its minimal polynomial over K has all its roots in L by (b). Clearly, these roots generate L over K (since any one of them does).

[1] The finiteness of G follows from Theorem 2.4.4.

(c) implies (a): By hypothesis L is generated over K by a finite number of elements $(x^1, \ldots, x^q)$ and by all their conjugates (x^i_j) (Section 2.4). It is clear that any K-isomorphism σ of L into an extension of L sends each of these generators to another element of the same set. Therefore, $\sigma(L) \subset L$. Moreover, by linear algebra, $\sigma(L) = L$, since a is K-linear and injective. In other words, σ is a K-*automorphism* of L. It follows from Theorem 2.4.4 that the group G of K-automorphisms of L has precisely n elements. Let $x \in L$ be invariant under G. Then every $\sigma \in G$ is a $K[x]$-automorphism of L. By Theorem 2.4.4 there are exactly $[L : K[x]]$ $K[x]$-isomorphisms of L into an extension field of L. Thus, $n < [L : K[x]]$, from which we may conclude that $n = [L : K[x]]$, $K[x] = K$, and $x \in K$. This proves that (c) implies (a). That the order of G is n has been proved along the way. □

Definition 6.1.2. If the conditions of Theorem 6.1.1 are satisfied, L is called a *Galois extension* of K and G is called the *Galois group* of L over K and denoted by $\mathrm{Gal}(L, K)$. If G is abelian (respectively, cyclic), L is called an *abelian* (respectively, *cyclic*) extension of K.

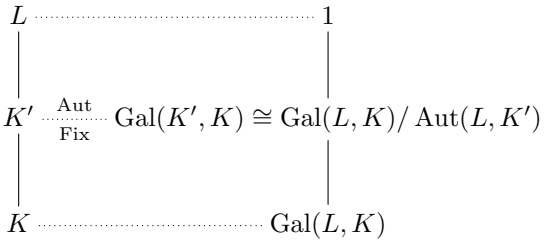
Corollary 6.1.3. *Let K be a finite field or a field of characteristic 0, let L be an extension of finite degree n of K, and let H be a group of automorphisms of L such that K is the fixed field of H, i.e. $K = \mathrm{Fix}_H(L)$. Then L is a Galois extension of K and H is the Galois group of L over K, i.e. $H = \mathrm{Gal}(L, K)$.*

Proof. For $x \in L$ the polynomial $\prod_{\sigma \in H}(X - \sigma(x)) = P(X)$ is invariant under H. Therefore, $P(X)$ has its coefficients in K. Since x is a root of $P(X)$, the minimal polynomial of x over K divides $P(X)$. By Theorem 6.1.1, (b) L is a Galois extension of K. Let G be the Galois group of L over K. We have $H \subset G$ and $\mathrm{card}(G) = n$ (Theorem 6.1.1). Now let x be a primitive element of L over K (Corollary 2.4.6) and let $P(X)$ be the polynomial constructed above. Since $n \leq \deg P$ and $\deg P = \mathrm{card}(H) \leq \mathrm{card}(G) = n$, we see that $H = G$. □

Theorem 6.1.4 (Fundamental theorem of Galois theory)**.** *Let K be a field which is finite or of characteristic 0, let L be a Galois extension of K with $G = \mathrm{Gal}(L, K)$. To any subgroup G' of G let us associate the fixed field $\mathrm{Fix}_{G'}(L)$, and to any subfield K' of L containing K let us associate the subgroup $\mathrm{Aut}(L, K') \subset G$ consisting of all K'-automorphisms of L.*

(a) The correspondences Fix *and* Aut *are bijections and are inverses of one another. They are both inclusion reversing on G and on L. The field L is a Galois extension of any intermediate field K' (i.e. $K \subset K' \subset L$).*

(b) In order that an intermediate field K' be a Galois extension of K, it is necessary and sufficient that $\mathrm{Aut}(L, K')$ be a normal subgroup of $G = \mathrm{Gal}(L, K)$. In this case we have $\mathrm{Gal}(K', K) \cong \mathrm{Gal}(L, K)/\mathrm{Aut}(L, K')$.



Proof. (a): For any intermediate field K' and any $x \in L$ the minimal polynomial of x over K' divides the minimal polynomial of x over K. Thus, all its roots belong to L by Theorem 6.1.1, (b), so L is a Galois extension of K', also by Theorem 6.1.1, (b). K' is the fixed field of the group $\mathrm{Aut}(L, K')$ of all K'-automorphisms of L (Theorem 6.1.1, (a)); in other words, $\mathrm{Fix}_{\mathrm{Aut}(L,K')}(L) = K'$. Let G' be a subgroup of $G = \mathrm{Gal}(L, K)$. Then G' is the Galois group of L over $\mathrm{Fix}_{G'}(L)$ (Corollary 6.1.3); this means $G' = \mathrm{Aut}(L, \mathrm{Fix}_{G'}(L))$. The relations $\mathrm{Fix}_{\mathrm{Aut}(L,K')}(L) = K'$ and $\mathrm{Aut}(L, \mathrm{Fix}_{G'}(L)) = G'$ imply that Fix and Aut are bijections and inverses of one another. It is clear that they reverse inclusions. This proves (a).
(b): Let K' be an intermediate field ($K \subset K' \subset L$). For $x \in K'$ the roots of the minimal polynomial of x over K are the elements of L of the form $\sigma(x)$, for $\sigma \in G$. According to Theorem 6.1.1 (b), in order that K' be a Galois extension of K, it is necessary and sufficient that $\sigma(x) \in K'$ for all $x \in K'$ and all $\sigma \in G$, i.e. that $\sigma(K') \subset K'$ for all $\sigma \in G$. But, if $\sigma(K') \subset K'$, if $\tau \in \mathrm{Aut}(L, K')$, and if $x \in K'$, then we have $\sigma^{-1}\tau\sigma(x) = \sigma^{-1}\sigma(x) = x$, so $\sigma^{-1}\tau\sigma \in \mathrm{Aut}(L, K')$. In other words, "$K'$ is a Galois extension over K" implies $\mathrm{Aut}(L, K')$ is normal in G. Conversely, suppose that $\mathrm{Aut}(L, K')$ is normal in G. If $x \in K'$, $\sigma \in G$, and $\tau \in \mathrm{Aut}(L, K')$, then $\tau\sigma(x) = \sigma\sigma^{-1}\tau\sigma(x) = \sigma(x)$, since $\sigma^{-1}\tau\sigma \in \mathrm{Aut}(L, K')$. Thus $\sigma(x)$ is invariant under every element of $\mathrm{Aut}(L, K')$, so $\sigma(x) \in K'$. Consequently, $\mathrm{Aut}(L, K')$ normal in G implies $\sigma(K') \subset K'$ and so K' is Galois over K.

Finally, let us determine $H = \mathrm{Gal}(K', K)$, the Galois group of K' over K. Since $\sigma(K') \subset K'$ for all $\sigma \in G$ (and even $\sigma(K') = K'$ by linear algebra), the restriction $\sigma \mid K'$ of σ to K' is a K-automorphism of K'. Restriction $\sigma \mapsto \sigma \mid K'$ is a homomorphism of G to the Galois group $H = \mathrm{Gal}(K', K)$. Clearly, its kernel is $\mathrm{Aut}(L, K')$. Since

$$\begin{aligned}\mathrm{card}(H) &= [K' : K] = [L : K][L : K']^{-1} = \mathrm{card}(G) \cdot \mathrm{card}(\mathrm{Aut}(L, K'))^{-1} \\ &= \mathrm{card}(G/\mathrm{Aut}(L, K')),\end{aligned}$$

we may conclude that the restriction homomorphism is surjective. Therefore, $H \cong G/\mathrm{Aut}(L, K')$. □

Example 6.1.5 (Quadratic extensions). Let K be a field of characteristic 0, and let L be a quadratic extension (i.e. of degree 2) of K. As in the beginning of Section 2.5 one sees that L is of the form $K[x]$, where x is a root of a polynomial

$X^2 - d$ ($d \in K$ and d non-square). Since the other root of this polynomial is $-x$, there is a non-trivial K-automorphism σ defined by $\sigma(x) = -x$, i.e.

$$\sigma(a + bx) = a - bx \quad (a, b \in K).$$

Clearly $\sigma^2 = 1$ and K is the fixed field for σ. Thus L is a Galois extension of K with the cyclic Galois group $\{1, \sigma\}$ (by Theorem 6.1.1 and Corollary 6.1.3).

Example 6.1.6 (Cyclotomic extensions). Let K be a field of characteristic 0, let ζ be a primitive nth root of unity in an extension of K, and let $L = K(\zeta)$. The field L is called a *cyclotomic extension* of K. The minimal polynomial of ζ over K divides $X^n - 1$ (2.3.7), so its roots are nth roots of unity and, consequently, powers of ζ (Section 1.6). Thus L is a *Galois extension* of K by Theorem 6.1.1, (c).

Let G be the Galois group of L over K. Any $\sigma \in G$ is determined by its effect on ζ. More precisely $\sigma(\zeta)$ is a power $\zeta^{j(\sigma)}$ of ζ where $j(\sigma)$ is uniquely determined modulo n. For $\sigma, \tau \in G$ one sees that

$$\sigma\tau(\zeta) = \sigma(\zeta)^{j(\sigma)} = \sigma(\zeta)^{j(\tau)} = \zeta^{j(\sigma)j(\tau)},$$

so $j(\sigma\tau) \equiv j(\sigma)j(\tau) \bmod n$. In other words $\sigma \mapsto j(\sigma)$ defines a homomorphism $G \to (\mathbb{Z}/n\mathbb{Z})^\times$. Since $j(\sigma)$ uniquely determines σ, this homomorphism is *injective*, and G is abelian. Thus *any cyclotomic extension is abelian.* If n is prime, this extension is even *cyclic*, for G is isomorphic to a subgroup of $(\mathbb{Z}/n\mathbb{Z})^\times = \mathbb{F}_n^\times$ (Theorem 1.7.3, (b)).

Remark 6.1.7. As any subgroup of an abelian group is normal, any intermediate field K' in a cyclotomic extension is a Galois extension (and an abelian extension) of K (Theorem 6.1.4, (b)). In particular, any subfield of a cyclotomic field is an abelian extension of $\mathbb{Q}$. Conversely, it can be shown, using (the theorem of Kronecker and Weber) that any abelian extension of $\mathbb{Q}$ is a subfield of a cyclotomic field.

The reader will observe that, with the preceding notations, the automorphism σ *raises every nth root of unity to its* $j(\sigma)$ *power*, for all the nth roots of unity are powers of ζ. Thus $\sigma \mapsto j(\sigma)$ is independent of the choice of ζ.

Example 6.1.8 (Finite fields). Let $\mathbb{F}_q$ be a finite field ($q = p^s$ with p prime). Any extension of finite degree of $\mathbb{F}_q$, is of the form $\mathbb{F}_{q^n}$. Its degree is n (Section1.7). The mapping $\sigma\colon x \mapsto x^q$ is an automorphism of $\mathbb{F}_{q^n}$ (Proposition 1.7.2) with $\mathbb{F}_q$ as its fixed field (Theorem 1.7.3, (c)). For any $x \in \mathbb{F}_{q^n}$, we have $\sigma^j(x) = x^{q^j}$, and $\sigma^n = 1$, since $x \in \mathbb{F}_{q^n}$ satisfies the relation $x^{q^n} = x$ (Theorem 1.7.3, (c)). On the other hand, for $1 \leq j \leq n-1$, we have $\sigma^j \neq 1$ since, if $j < n$, there exists $x \in \mathbb{F}_{q^n}$ such that $x^{q^n} \neq x$. Thus $\{1, \sigma, \ldots, \sigma^{n-1}\}$ is a cyclic group of order n. According to Corollary 6.1.3, $\mathbb{F}_{q^n}$ is a *cyclic extension of degree* n *of* $\mathbb{F}_q$. *Its Galois group has a canonical generator, the mapping* $x \mapsto x^q$. This mapping is called the *Frobenius automorphism.*

6.2 The decomposition and inertia groups

In this section A denotes a Dedekind ring, K its field of fractions (which is assumed to be of characteristic 0), K' is a Galois extension of K of degree n, G is the Galois group of K' over K, and A' is the integral closure of A in K'.

$$\begin{array}{ccc} K' & \text{——} & A' \\ | & & | \\ K & \text{——} & A \end{array}$$

By applying $\sigma \in G$ to an equation of integral dependence (over A) of an element $x \in A'$, one sees that $\sigma(x) \in A'$. Therefore,

$$A' \quad \text{is stable under} \quad G, \quad \text{i.e.} \quad \sigma(A') = A' \quad \text{for all} \quad \sigma \in G. \tag{6.2.1}$$

Remark 6.2.2. We have shown only that $\sigma(A') \subset A'$. But we also have $\sigma^{-1}(A') \subset A'$, so $A' = \sigma\sigma^{-1}(A') \subset \sigma(A')$. From now on we shall leave the details of reasoning of this sort to the reader

On the other hand, if $\mathfrak{p}$ is a maximal ideal of A and $\mathfrak{p}'$ a maximal ideal of A' such that $\mathfrak{p}' \cap A = \mathfrak{p}$ (i.e. $\mathfrak{p}'$ appears in the factorisation of $A'\mathfrak{p}$ into a product of prime ideals in A'; cf. Proposition 5.2.2), then, clearly $\sigma(\mathfrak{p}') \cap A = \mathfrak{p}$, so $\sigma(\mathfrak{p}')$ also appears in the expression for $A'\mathfrak{p}$ as a product of prime ideals of A' and with the *same* exponent as $\mathfrak{p}'$. We shall say that $\mathfrak{p}'$ and $\sigma(\mathfrak{p}')$ arc *conjugate* prime ideals of A'. We are going to show that all the prime ideals in the prime factorisation of $A'\mathfrak{p}$ in A' are conjugate.

Proposition 6.2.3. *If $\mathfrak{p}$ is a maximal ideal of A, then the maximal ideals $\mathfrak{p}'$ of A' which appear in the expression for $A'\mathfrak{p}$ as a product of prune ideals in A' (i.e. the maximal ideals $\mathfrak{p}'$ are characterised by the property $\mathfrak{p}' \cap A = \mathfrak{p}$) are all conjugate. They have the same residual degree f and the same ramification index e. Thus $A'\mathfrak{p} = (\prod_{i=1}^{g} \mathfrak{p}_i')^e$ and $n = efg$.*

Proof. The assertion concerning the ramification index and the residual degree is obvious, because an automorphism preserves *all* algebraic relations. The formula $n = efg$ is thus a special case of the relation $\sum e_i f_i = n$ (Theorem 5.2.3). Now let $\mathfrak{p}'$ be one of the $\mathfrak{p}_i'$'s and assume that another of the $\mathfrak{p}_i'$'s, which we shall denote $\mathfrak{q}'$, is not conjugate to $\mathfrak{p}'$. Since $\mathfrak{q}'$ and $\sigma(\mathfrak{p}')$ ($\sigma \in G$) are maximal and distinct, $\sigma(\mathfrak{p}') \not\subset \mathfrak{q}'$. We need the following lemma.

Lemma 6.2.4 (Prime avoidance lemma)**.** *Let R be a ring, $\mathfrak{p}_1, \ldots, \mathfrak{p}_q$ a finite set of prime ideals of R, and let $\mathfrak{b}$ be an ideal of R such that $\mathfrak{b} \not\subset \mathfrak{p}_i$ for any index i. Then there exists $b \in \mathfrak{b}$ such that $b \notin \mathfrak{p}_i$ for any i.*

Proof. Without loss of generality we may assume $\mathfrak{p}_j \not\subset \mathfrak{p}_i$ for $i \neq j$ (Just cast out non-maximal ideals $\mathfrak{p}_i$ from the list $\mathfrak{p}_1, \ldots, \mathfrak{p}_q$.) Let $x_{ij} \in \mathfrak{p}_j \setminus \mathfrak{p}_i$ for $i \neq j, 1 \leq i, j \leq q$. Since $\mathfrak{b} \not\subset \mathfrak{p}_i$, there exists $a_i \in \mathfrak{b}$ such that $a_i \notin \mathfrak{p}_i$. Put $b_i = a_i \prod_{j \neq i} x_{ij}$. Then $b_i \in \mathfrak{b}$, $b_i \in \mathfrak{p}_j$ for $j \neq i$, and $b_i \notin \mathfrak{p}_i$ (since $\mathfrak{p}_i$ is prime).

Thus $b = b_1 + \cdots + b_q \in \mathfrak{b} \setminus \cup_{i=1}^{q} \mathfrak{p}_i$, since clearly $b \in \mathfrak{b}$ and $b \equiv b_i \bmod \mathfrak{p}_i$ (so $b \notin \mathfrak{p}_i$ for any i). □

Returning to the proof of the proposition, we see, from the lemma, that there is an element $x \in \mathfrak{q}'$ such that $x \notin \sigma(\mathfrak{p}_i)$ for all $\sigma \in G$. Consider the norm of x, $\mathrm{Nm}(x) = \prod_{\tau \in G} \tau(x)$ (Proposition 2.6.6). Since $\tau(x) \in A'$ for all $\tau \in G$ (by (6.2.1) we see that $\mathrm{Nm}(x) \in \mathfrak{q}'$, so

$$\mathrm{Nm}(x) \in \mathfrak{q}' \cap A = p.$$

On the other hand $x \notin \tau^{-1}(\mathfrak{p}')$, so $\tau(x) \notin \mathfrak{p}'$ for any $\tau \in G$. Since $\mathfrak{p}'$ is prime, we see that $\mathrm{Nm}(x) \notin \mathfrak{p}'$, and this contradicts $\mathrm{Nm}(x) \in \mathfrak{p}$. □

Now let $\mathfrak{p}'$ be a maximal ideal of A' such that $\mathfrak{p}' \cap A = \mathfrak{p}$. Those $\sigma \in G$ for which $\sigma(\mathfrak{p}') = \mathfrak{p}'$ form a subgroup D of G, called the *decomposition group of* $\mathfrak{p}'$. If g denotes the number of conjugates of $\mathfrak{p}'$, then

$$g = \mathrm{card}(G) \cdot \mathrm{card}(D)^{-1} \quad \text{or} \quad \mathrm{card}(D) = n/g = ef. \tag{6.2.5}$$

For $\sigma \in D$, the relations $\sigma(A') = A'$ and $\sigma(\mathfrak{p}') = \mathfrak{p}'$ imply that σ induces an automorphism $\overline{\sigma}$ of $A'/\mathfrak{p}'$ ($x \equiv y \bmod \mathfrak{p}'$ entails $\sigma(x) \equiv \sigma(y) \bmod \mathfrak{p}'$). It is clear that $\overline{\sigma}$ is an $(A/\mathfrak{p})$-automorphism. The mapping $\sigma \mapsto \overline{\sigma}$ is a group homomorphism, whose *kernel* is the sub-group $I \subset D$ consisting of those $\sigma \in D$ which satisfy the relation $\sigma(x) - x \in \mathfrak{p}'$ for all $x \in A'$. Thus I is a *normal subgroup* of D, called the *inertia subgroup of* $\mathfrak{p}'$.

Proposition 6.2.6. *With the same notations as above, assume that $A/\mathfrak{p}$ is finite or of characteristic 0. Then $A'/\mathfrak{p}'$ is a Galois extension of degree f of $A/\mathfrak{p}$, and the mapping $\sigma \mapsto \overline{\sigma}$ is an epimorphism of D on the Galois group of $A'/\mathfrak{p}'$ over $A/\mathfrak{p}$. Moreover,* $\mathrm{card}(I) = e$.

Proof. Let K_D be the fixed field of D, let $A_D = A' \cap K_D$ be the integral closure of A in K_D, and let $\mathfrak{p}_D$ be the prime ideal $\mathfrak{p}' \cap A_D$. According to Proposition 6.2.3 and the definition of D, $\mathfrak{p}'$ is the only prime factor of $A'\mathfrak{p}_D$. Put $A'\mathfrak{p}_D = \mathfrak{p}'^{e'}$ and write f' for the residual degree $[A'/\mathfrak{p}' : A_D/\mathfrak{p}_D]$. According to Theorem 5.2.3, Theorem 6.1.4, and 6.2.5 we have

$$e'f' = [K'/K_D] = \mathrm{card}(D) = ef.$$

Since $A/\mathfrak{p} \subset A_D/\mathfrak{p}_D \subset A'/\mathfrak{p}'$, we have $f' \leq f$. Since $\mathfrak{p}A_D \subset \mathfrak{p}_D$, we have $e' \leq e$. Therefore, since $e'f' = ef$, $e = e'$ and $f = f'$. Thus

$$A/\mathfrak{p} \cong A_D/\mathfrak{p}_D. \tag{6.2.7}$$

Now let $\overline{x}$ be a primitive element for $A'/\mathfrak{p}'$ over $A/\mathfrak{p}$ and let $x \in A'$ be a representative for $\overline{x}$. Let $X^r + a_{r-1}X^{r-1} + \cdots + a_0 = P(X)$ be the minimal polynomial for x over K_D. We know that $a_i \in A_D$ (Corollary 2.6.8). The roots of $P(X)$ arc all of the form $\overline{\sigma}(x)$ with $\sigma \in D$. The "reduced polynomial" $\overline{P}(X) = X^r + \overline{a}_{r-1}X^{r-1} + \cdots + \overline{a}_0$ has its coefficients in $A/\mathfrak{p}$ (by 6.2.7)) and

the roots of $\overline{P}(X)$ are all of the form $\overline{\sigma}(x)$ with $\sigma \in D$. Consequently, $A'/\mathfrak{p}'$ contains all the conjugates of $\overline{x}$ over $A/\mathfrak{p}$, and $A'/\mathfrak{p}'$ is a *Galois extension* of $A/\mathfrak{p}$ (Theorem 6.1.1, (c)). Furthermore, since every conjugate of $\overline{x}$ over $A/\mathfrak{p}$ of the form $\overline{\sigma}(x)$, every $(A/\mathfrak{p})$-automorphism of $A'/\mathfrak{p}'$ is of the form $\overline{\sigma}$ for some $\sigma \in D$. Thus, the Galois group of $A'/\mathfrak{p}'$ over $A/\mathfrak{p}$ may be identified with D/I. Since its order is $[A'/\mathfrak{p}' : A/\mathfrak{p}] = f$, we have $\operatorname{card}(D)/\operatorname{card}(I) = f$, so $\operatorname{card}(I) = e$, by (6.2.5). □

Corollary 6.2.8. *In order that $\mathfrak{p}$ not ramify in A' it is necessary and sufficient that the inertia group I of $\mathfrak{p}'$ for any $\mathfrak{p}'$ over $\mathfrak{p}$ (i.e. such that $\mathfrak{p}' \cap A = \mathfrak{p}$) be trivial.*

Remark 6.2.9. Write $D_{\mathfrak{p}'}$ and $I_{\mathfrak{p}'}$ for the decomposition and inertia groups of the maximal ideal $\mathfrak{p}' \in A'$. For a *conjugate* ideal $\sigma(\mathfrak{p}')$ $(\sigma \in G)$

$$D_{\sigma(\mathfrak{p}')} = \sigma D_{\mathfrak{p}'} \sigma^{-1}, \quad I_{\sigma(\mathfrak{p}')} = \sigma I_{\mathfrak{p}'} \sigma^{-1}. \tag{6.2.10}$$

To prove (6.2.10) note that, for $\tau \in D_{\sigma(\mathfrak{p}')}$, we have

$$\sigma\tau\sigma^{-1}\dot{\sigma}(\mathfrak{p}') = \sigma\tau(\mathfrak{p}') = \sigma(\mathfrak{p}'), \quad \text{and} \quad \sigma D_{\mathfrak{p}'}\sigma^{-1} \subset D_{\sigma(\mathfrak{p}')}.$$

The reverse inclusion follows by an argument analogous to that of the remark following (6.2.1). Similarly, for $\tau \in I_{\mathfrak{p}'}$ and $x \in A'$, we have

$$\sigma\tau\sigma^{-1}(x) - x = \sigma\tau(\sigma^{-1}(x)) - \sigma\sigma^{-1}(x) = \sigma(\tau(\sigma^{-1}(x)) - \sigma^{-1}(x)) \in \sigma(\mathfrak{p}'),$$

so $\sigma I_{\mathfrak{p}'}\sigma^{-1} \subset I_{\sigma(\mathfrak{p}')}$, the reverse inclusion being proved as before. When K' is an *abelian* extension of K. the groups $D_{\sigma(\mathfrak{p}')}$ (respectively, $I_{\sigma(\mathfrak{p}')}$) $(\sigma \in G)$ are all *equal*. They depend only on the ideal $\mathfrak{p}$ of the ring A (Proposition 6.2.3).

6.3 The number field case. The Frobenius automorphism

The preceding will now be applied to number fields and their rings of integers. This application is possible because number fields are of characteristic 0 and their residual fields are finite.

Let us keep our earlier notations ($K \subset K'$, both number fields, K' a Galois extension of K with Galois group G, the respective rings of integers A and A').

$$\begin{array}{ccc} K' & \text{——} & A' \\ | & & | \\ K & \text{——} & A \end{array}$$

Let $\mathfrak{p}$ be a maximal ideal of A which *does not ramify* in A', and let $\mathfrak{p}'$ be a prime factor of $A'\mathfrak{p}$. The inertia group of $\mathfrak{p}'$ consists of the identity of G alone (Corollary 6.2.8); its decomposition group D is canonicallv isomorphic

to the Galois group of $A'/\mathfrak{p}'$ over $A/\mathfrak{p}$ (Proposition 6.2.6). But the Galois group of $A'/\mathfrak{p}'$ over $A/\mathfrak{p}$ is cyclic with a canonical generator $\overline{\sigma}\colon \overline{x} \mapsto \overline{x}^q$ where $q = \mathrm{card}(A/\mathfrak{p})$ (Example 6.1.8). Therefore, D itself is *cyclic* with a canonical generator σ defined by the relation $\sigma(x) \equiv x^q \bmod \mathfrak{p}'$) for any $x \in A'$. This generator is called the *Frobenius automorphism* of $\mathfrak{p}'$. We denote it $(\mathfrak{p}', K'/K)$.

For $\tau \in G$ we have, as in Remark 6.2.9.

$$(\tau(\mathfrak{p}'), K'/K) = \tau \cdot (\mathfrak{p}', K'/K) \cdot \tau^{-1}. \tag{6.3.1}$$

In particular, if K' is an abelian extension, $(\mathfrak{p}', K'/K)$ depends only on the ideal $\mathfrak{p}$ of A. In this case we write $(\frac{K'/K}{\mathfrak{p}})$.

Proposition 6.3.2. *With the preceding hypotheses and notations, let F be an intermediate field $(K \subset F \subset K')$ and write f for the residual degree of $\mathfrak{p}' \cap F$ over K. Then*

(a) $(\mathfrak{p}', K'/F) = (\mathfrak{p}', K'/K)^f$;

(b) if F is Galois over K, the restriction of $(\mathfrak{p}', K'/K)$ to F equals $(\mathfrak{p}' \cap F, F/K)$.

Proof. (a): Put $\sigma = (\mathfrak{p}', K'/K)$. By definition $\sigma(\mathfrak{p}') = \mathfrak{p}'$ and $\sigma(x) \equiv x^q \bmod \mathfrak{p}'$ for every $x \in A'$ (here $q = \mathit{card}(A/\mathfrak{p})$). Thus

$$\sigma(\mathfrak{p}') = \mathfrak{p}' \quad \text{and} \quad \sigma^f(x) \equiv x^{q^f} \bmod \mathfrak{p}'$$

for all $x \in A'$. By definition of f, q^f is the cardinality of the residual field $(A' \cap F)/(\mathfrak{p}' \cap F)$. Furthermore, the decomposition group of $\mathfrak{p}'$ over F is obviously a subgroup of the decomposition group D of $\mathfrak{p}'$ over K. It is of order

$$[A'/\mathfrak{p}' : (A' \cap F)/(\mathfrak{p} \cap F)] = f^{-1}[A'/\mathfrak{p}' : A/\mathfrak{p}] = f^{-1}\,\mathrm{card}(D),$$

by (6.2.5). Since D is cyclic and generated by σ, the only subgroup of D of order $f^{-1}\,\mathrm{card}(D)$ is generated by σ^f. This proves (a)
(b): Suppose F is Galois over K and write σ' for the restriction of σ to F (Theorem 6.1.1, (b)). Since $\sigma(\mathfrak{p}') = \mathfrak{p}'$, it follows that $\sigma'(\mathfrak{p}' \cap F) = \mathfrak{p}' \cap F$ and σ' belongs to the decomposition group of $\mathfrak{p}' \cap F$ over K. Moreover, it is clear that $\sigma'(x) \equiv x^q \bmod \mathfrak{p}'$ for all $x \in A' \cap F$, with $q = \mathrm{card}(A/\mathfrak{p})$. □

6.4 An application to cyclotomic fields

We are going to utilise the theory which we have just developed to present a third proof of the irreducibility of the cyclotomic polynomial (cf. Theorem 2.9.3 and Example 5.2.6).

Theorem 6.4.1. *Let ζ be a primitive complex nth root of unity. Then*

(a) No prime number which does not divide n ramifies in $\mathbb{Q}[\zeta]$;

(b) $\mathbb{Q}[\zeta]$ is an abelian extension of $\mathbb{Q}$ of degree $\varphi(n)$ and with Galois group isomorphic to $(\mathbb{Z}/n\mathbb{Z})^\times$.

Proof. (a): Let $F(X)$ be the minimal polynomial of ζ over $\mathbb{Q}$, and let d be its degree (so $d = [\mathbb{Q}[\zeta] : \mathbb{Q}]$). The polynomial F divides $X^n - 1$; let $X^n - 1 = F(X)G(X)$. We know that $D(1, \zeta, \ldots, \zeta^{d-1}) = \mathrm{Nm}(F'(\zeta))$ (2.7.15). From the relation $nX^{n-1} = F'(X)G(X) + F(X)G'(X)$, we may prove, by substitution, $n\zeta^{n-1} = F'(\zeta)G(\zeta)$. Since ζ is a unit of $\mathbb{Q}[\zeta]$, it is of norm ± 1. Taking norms, we may conclude that $\mathrm{Nm}(F'(\zeta))$ divides n^d. Finally, since ζ is an integer in $\mathbb{Q}[\zeta]$, the absolute discriminant of $\mathbb{Q}[\zeta]$ divides $D(1, \zeta, \ldots, z^{d-1})$ and, therefore also, n^d. By Theorem 5.3.8, no prime number which does not divide n ramifies in $\mathbb{Q}[\zeta]$. This proves (a).
(b): Recall (Example 6.1.6) that $\mathbb{Q}[\zeta]$ is an abelian extension of $\mathbb{Q}$, and that there is an monomorphism j of the Galois group G of $\mathbb{Q}[\zeta]$ over $\mathbb{Q}$ into $(\mathbb{Z}/n\mathbb{Z})^\times$. More precisely, the element $\sigma \in G$ raises all the nth roots of unity to the power $j(\sigma)$. Let p be a prime number which docs not divide n. By (a) the Frobenius automorphism

$$\left(\frac{\mathbb{Q}[\zeta]/\mathbb{Q}}{p}\right)$$

is defined; denote it σ_p. Writing A for the ring of integers of $\mathbb{Q}[\zeta]$ and $\mathfrak{p}$ for an arbitrary prime factor of Ap, we obtain, from the definition of the Frobenius automorphism, the relation $\sigma_p(x) \equiv x^p \bmod \mathfrak{p}$ for all $x \in A$. In particular, putting $j = j(\sigma_p$, we have $\zeta^j \equiv \zeta^p \bmod \mathfrak{p}$. Recall that

$$\prod_{0 \le r \le n-1 r \not\equiv p \bmod n} (\zeta^p - \zeta^r) = P'(\zeta^p) = n\zeta^{p(n-1)},$$

where $P(X) = X^n - 1 = \prod_{0 \le r \le n-1}(X - \zeta^r)$. Since n is relatively prime to p, since $\mathfrak{p} \cap \mathbb{Z} = p\mathbb{Z}$, and since ζ is a unit in the integers of $\mathbb{Q}[\zeta]$, we may conclude from the relation $P'(\zeta^p) = n\zeta^{p(n-1)}$ that

$$\prod_{0 \le r \le n-1 r \not\equiv p \bmod n} (\zeta^p - \zeta^r) \notin \mathfrak{p}.$$

The relation $\zeta^j \equiv z^p \bmod \mathfrak{p}$ thus implies that j represents the residue class of $p \bmod n$. Hence $j(G)$ contains the residue classes mod n of all the prime numbers p; which do not divide n. But this means that $j(G) = (\mathbb{Z}/n\mathbb{Z})^\times$, which proves (b). □

6.5 Another proof of the quadratic reciprocity law

Let q be an odd prime. Let K be the cyclotomic field generated by a primitive qth root of unity in $\mathbb{C}$. The Galois group G of K over $\mathbb{Q}$ is isomorphic to $\mathbb{F}_q^\times$ (Theorem 6.4.1, (b)); it is cyclic of even order $q - 1$. There is a unique

subgroup H of index 2, which corresponds to the subgroup of squares $(\mathbb{F}_q^\times)^2$. Thus K contains a unique quadratic subfield F (Theorem 6.1.4, (b)). No prime number $p \neq q$ ramifies in F, for, if it did, it would ramify in K; and this would contradict Theorem 6.4.1, (a). The calculation of the discriminant of a quadratic field (Example 5.3.9) implies that $F = \mathbb{Q}[\sqrt{q}]$, if $q \equiv 1 \bmod 4$, and $F = \mathbb{Q}[\sqrt{-q}]$, if $q \equiv 3 \bmod 4$. Putting $q^* = (-1)^{(q-1)/2}q$, we have, in either case, $F = \mathbb{Q}[\sqrt{q^*}]$.

Let p be a prime distinct from q. Write σ_p for the Frobenius automoiphism $(\frac{K/\mathbb{Q}}{p})$ (cf. Section 6.4). Its restriction to F is $(\frac{F/\mathbb{Q}}{p})$ (Proposition 6.3.2, (b)). It is the identity if $\sigma_p \in H$, i.e if the exponent $j(\sigma_p) =$ the residue class of $p \bmod q$ (cf. Section 6.4) is a square in $\mathbb{F}_p^\times$. Otherwise it is the non-trivial automorphism of F. In other words, identifying the Galois group G/H of F over $\mathbb{Q}$ with $\{+1, -1\}$, we have

$$\left(\frac{F/\mathbb{Q}}{p}\right) = \left(\frac{p}{q}\right) \tag{6.5.1}$$

by definition of the Legcndre symbol (p/q) (Section 5.5).

On the other hand, the results concerning the decomposition of the prime p in $F = \mathbb{Q}[\sqrt{q^*}]$ (Section 5.4) give further information regarding $(\frac{F/\mathbb{Q}}{p})$. By definition it is the identity if p splits in F, and it is the non-trivial automorphism if p remains prime. Using Proposition 5.4.2, we may conclude that, if p is odd,

$$\left(\frac{F/\mathbb{Q}}{p}\right) = \left(\frac{q^*}{p}\right). \tag{6.5.2}$$

Comparing (6.5.1) and (6.5.2) we obtain

$$\left(\frac{p}{q}\right) = \left(\frac{q^*}{p}\right) = \left(\frac{-1}{p}\right)^{(q-1)/2} \left(\frac{q}{p}\right).$$

But

$$\left(\frac{-1}{p}\right) = (-1)^{(q-1)/2} \left(\frac{q}{p}\right)$$

by Euler's criterion (Proposition 5.5.3). Consequently,

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

This completes our second proof of the quadratic reciprocity law (Theorem 5.5.4). To take care of the case $p = 2$, recall that 2 splits in F if $q^* = 1 \bmod 8$ and 2 remains prime if $q^* = 5 \bmod 8$ (Proposition 5.4.2). However,

$$(-1)^{(q^2-1)/8} = (-1)^{(q^*-1)/8} = \begin{cases} 1 & \text{if} \quad q^* \equiv 1 \bmod 8 \\ -1 & \text{if} \quad q^* \equiv 5 \bmod 8. \end{cases}$$

Thus,

$$\left(\frac{F/\mathbb{Q}}{2}\right) = (-1)^{(q^2-1)/8}. \tag{6.5.3}$$

Putting (6.5.1) and (6.5.3) together, we obtain $(2/q) = (-1)^{(q^2-1)/8}$. This is the difficult "complementary formula" (Proposition 5.5.9, (b)).

Appendix A

The field of complex numbers is algebraically closed

Let K be a field and consider the following statements:

(a) Any polynomial of posiuve degree over K is a product of polynomials of degree one (linear polynomials).

(b) Any polynomial of positive degree has a root in K.

Clearly (a) implies (b). Conversely, if (b) is true, if P is a polynomial of degree $d \geq 1$ over K, and if $a \in K$ is a root of P, then P is a multiple of $X - a$, and induction on the degree d of P shows that (aa is true. A field K which satisfies the equivalent conditions (a) and (b) is said to be *algebraically closed.*

We are going to show, by a method essenually due to Lagrange, that $\mathbb{C}$ $(= \mathbb{R}[i], i^2 = -1)$ is algebraically closed. We shall make use of only the following facts:

1. Any polynomial of odd degree over $\mathbb{R}$ has a root in $\mathbb{R}$; this is a special case of Weierstrass's theorem on intermediate values.

2. Any quadratic polynomial over $\mathbb{C}$ has its roots in $\mathbb{C}$. The elementary "formula" for a root of $aX^2 + bX + c = 0$ reduces the question to that of showing that any $z = a + ib \in \mathbb{C}$ $(a, b \in \mathbb{R})$ has a square root in $\mathbb{C}$. But $(x + iy)^2 = a + ib$ $(x, y \in \mathbb{R})$ is equivalent to $x^2 - y^2 = a$ and $2xy = b$. It follows that $a^2 + b^2 = (x^2 + y^2)^2$ and $x^2 + y^2 = \sqrt{a^2 + b^2}$. Clearly, one may find x^2 and y^2, hence x and y, satisfying these equations.

3. Given a non-constant polynomial $P \in K[X]$, there exists an extension K' of K such that P factors into a product of linear polynomials in $K'[X]$. There was an easy proof of this fact in Proposition 2.3.11 (a proof almost independent of other results in this chapter; it suffices to know that, if F is irreducible, $K[X]/F(X)K[X]$ is a field. Then, use an induction).

4. The relations between coefficients and roots of a polynomial.

5. The fact that a symmetric polynomial $G \in K[X_1, \ldots, X_n]$ is a polynomial in the elementary symmetric functions $\sum X_i, \sum X_i X_j, \ldots, \sum X_1 \cdots X_n$ of the X_i's.

Theorem A.0.1. *The field $\mathbb{C}$ of complex numbers is algebraically closed.*

Proof. We shall prove property (b), that any non-constant polynomial has a root in $\mathbb{C}$. Observing that $F(X) = P(X)\overline{P}(X)$ ($\overline{P}$: the polynomial whose coefficients are the complex conjugates of the coefficients of P) has roots in $\mathbb{C}$ if and only if P does, we see that we need consider only polynomials with real coefficients.

Now we write the degree of T ($\in \mathbb{R}[X]$) in the form $d = 2^n q$ where q is odd. We argue by induction on the *exponent* n of 2. For $n = 0$, d is odd and F has a root in $\mathbb{R}$ (cf (1)). Suppose $n \geq 1$. By (3) there exists an extension K' of $\mathbb{C}$ and $x_1, \ldots, x_d \in K'$ such that $F(X) = \prod_{i=1} d(X - x_i)$ (assuming, without loss of generality, that F is monic).

Let c be an arbitrary element of $\mathbb{R}$ and consider the elements $y_{ij} = x_i + x_j + cx_i x_j$, of K' ($i \leq j$). The cardinality of $(y_{ij}, 1 \leq i \leq j \leq d$, is $\frac{1}{2}d(d+1) = 2^{n-1}q(d+1)$, where $q(d+q)$ is odd. The polynomial $G(X) = \prod_{i \leq j}(X - y_{ij})$ has as coefficients symmetric polynomials in the x_i's with real coefficients. By (5) the coefficients are polynomials in the elementary symmetric functions of the x_i's; these polynomials themselves have real coefficients. Therefore, the coefficients of G are real (by 4)). As its degree is of the form $2^{n-1} \times x$ (x odd), the induction hypothesis implies that it has a root $z_c \in \mathbb{C}$. One of the y_{ij}'s, say $y_{i(c),j(c)} = x_{i(c)} + y_{j(c)} + cx_{i(c)}x_{j(c)}$ is therefore equal to z_c.

Now, since $\mathbb{R}$ is infinite and since the set of pairs $(i, j), (i \leq j)$ is finite, there exist two distinct real numbers c and c' such that $i(c) = i(c')$ and $j(c) = j(c')$. Denote these indices by r and s respectively. Then $x_r + x_s + cx_r x_s = z_c \in \mathbb{C}$ and $x_r + x_s + c'x_r x_s = z_{c'} \in \mathbb{C}$. Taking linear combinations, we may conclude that $x_r + x_s \in \mathbb{C}$ and $x_r x_s \in \mathbb{C}$. Therefore, by 4), x_r and x_s are roots of a quadratic equation with coefficients in $\mathbb{C}$. We may conclude that $x_r, x_s \in \mathbb{C}$ (by (2)). Thus F) has a root in $\mathbb{C}$ and the theorem is proved $\square$

Appendix B

The calculation of a volume

Proposition B.0.1. *Let $r_1, r_2 \in \mathbb{N}$, $n = r_1 + 2r_2$, $t \in \mathbb{R}$, and let B_t be the set of all elements*

$$(y_1, \ldots, y_{r_1}, z_1, \ldots, z_{r_2}) \in \mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$$

such that

$$\sum_{i=1}^{r_1} |y_i| + 2 \sum_{j=1}^{r_2} |z_j| \leq t. \tag{B.0.2}$$

Let μ denote the Lebesgue measure in $\mathbb{R}^n$. Then

$$\mu(B_t) = 2^{r_1} \left(\frac{\pi}{2}\right)^{r_2} \frac{t^n}{n!} \quad \textit{for any} \quad t \geq 0. \tag{B.0.3}$$

Proof. We set $\mu(B_t) = V(r_1, r_2, t)$ and argue by double induction on r_1 and r_2. Clearly $V(1, 0.t) = 2t$ (the segment $[-t, +t]$) and $V(0, 1, t) = \pi t^2/4$ (the disc of radius $t/2$). These results verify (B.0.3) in the special cases considered.

Now assume (B.0.3) gives $V(r_1, r2, t)$. First we compute $V(r_1+1, r_2, t)$. The set $B_t \subset \mathbb{R} \times \mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$, which corresponds to $r_1 + 1$ and r_2, is defined by the relation

$$|y| + \sum_{i=1}^{r_1} |y_i| + 2 \sum_{j=1}^{r_2} |z_j| \leq t \quad (y \in \mathbb{R})$$

Integrating "in strips" and observing that for $|y| > t$, $B_t = \varnothing$, we see that

$$V(r_1 + 1, r_2, t) = \int_{-t}^{+t} V(r_1, r_2, t - |y|) dy.$$

Use of the induction hypothesis gives

$$V(r_1 + 1, r_2, t) = 2 \int_0^t 2^{r_1} \left(\frac{\pi}{2}\right)^{r_2} \frac{(t-y)^n}{n!} dy = 2^{r_1+1} \left(\frac{\pi}{2}\right)^{r_2} \frac{t^{n+1}}{(n+1)!},$$

which agrees with (B.0.3). It remains to compute $V(r_1, r_{2+1}, t)$. We keep the induction hypothesis that $V(r_1, r_2, t)$ satisfies (B.0.3). The set $B_t \subset \mathbb{R}^{r_1} \times \mathbb{C}^{r_2} \times$

$\mathbb{C}$ which corresponds to r_1 and $r_2 + 1$ is defined by the relation

$$\sum_{i=1}^{r_1} |y_i| + 2\sum_{j=1}^{r_2} |z_j| + 2|z| \leq t \quad (z \in \mathbb{C})$$

Again integrating in strips, we obtain

$$V(r_1, r_2 + 1, t) = \int_{|z| \leq t/2} V(r_1, r_2, t - 2|z|) d\mu(z),$$

where $d\mu(z)$ denotes Lebesgue measure on $\mathbb{C}$. Putting $z = \rho e^{i\theta}$ ($\rho \in \mathbb{R}, 0 \leq \theta \leq < 2\pi$), we have $d\mu(z) = \rho d\rho d\theta$. Use of the induction hypothesis gives

$$\begin{aligned} V(r_1, r_2 + 1, t) &= \int_0^{t/2} \int_0^{2\pi} 2^{r_1} \left(\frac{\pi}{2}\right)^{r_2} \frac{(t - 2\rho)^n}{n!} \rho d\rho d\theta \\ &= 2^{r_1} \left(\frac{\pi}{2}\right)^{r_2} \frac{2\pi}{n!} \int_0^{t/2} (t - 2\rho)^n \rho d\rho. \end{aligned}$$

Calculating $\int_0^{t/2} (t - 2\rho)^n \rho d\rho$ by putting $2\rho = x$ and integrating bv parts, we find that this integral has the value $t^{n+2}/[4(n + 1)(n + 2)]$. Thus,

$$V(r_1, r_2 + 1, t) = 2^{r_1} \left(\frac{\pi}{2}\right)^{r_2+1} \frac{t^{n+2}}{(n + 2)!}$$

which agrees with (B.0.3) since $r_1 + 2(r_2 + 1) = n + 2$. □