Algebraic Number Theory with Elementary Galois Theory

Rodney Coleman, Laurent Zwald

Algebraic Number Theory with Elementary Galois Theory

Rodney Coleman, Laurent Zwald

February 2, 2023

Preface

Our aim in writing this book is to present a clear introduction to algebraic number theory at the upper undergraduate/graduate level. The first chapters are devoted to elementary Galois theory, which plays a fundamental role in algebraic number theory. Usually the Galois theory needed in algebraic number theory is confined to a reference or a brief appendix. We feel it is useful to have a good traitment of this material at hand. Naturally, there are important parts of Galois theory, for example radical extensions and inverse Galois theory, which we do not handle, as they do not concern the main subject of this text.

After this preliminary work we turn to the study of algebraic number fields, i.e., finite field extensions of the rationals, presenting basic results such as the Kronecker-Weber theorem, Dedekind's different theorem, Dirichlet's unit theorem, Hermite's theorem and Dedekind's factorization theorem. We also introduce and study the class group of a number ring and establish the class number formula. In general, our proofs are detailed and we do not leave important parts of proofs to the reader. This avoids tedious reading and frustration when faced with gaps which the reader is often unable to fill in.

As for required reading, we assume a good background in elementary algebra: semigroups, groups, rings and modules over rings; in particular, the basic isomorphism theorems for groups, rings and modules. We also assume a basic knowledge of Lebesgue integration and complex analysis. Finally, we suppose that the reader is acquainted with fundamental number theory, for example the rings of integers $\mathbf{Z}_n$ and the finite fields $\mathbf{F}_p$. All this material is generally covered in the first years of a mathematics program. Of course, where necessary, we give reminders; however, as our aim is to reach a relatively high level in a moderately short text, we do not spend too much time on elementary notions.

Unless otherwise mentioned, we will suppose that all rings are commutative with identity, although we will often recall these assumptions.

Contents

Part I

Elementary Galois Theory

Chapter 1

Field Extensions

If E and F are rings, in particular fields, then we say that E is an *extension* of F, or F is included in E, if there is a an injective ring homomorphism ϕ, or monomorphism, from F into E. The following result justifies these terms.

Theorem 1.1 *Let ϕ be a monomorphism of the ring A into the ring B. Then there is an extension $\bar{A}$ of A and of ϕ to an isomorphism of $\bar{A}$ onto B.*

PROOF If $\phi : A \longrightarrow B$ is an isomorphism, then there is nothing to prove, so we can suppose that this is not the case. We set $\bar{A} = A \cup B \setminus \phi(A)$ and then define $\psi : B \longrightarrow \bar{A}$ by

$$\psi(y) = \begin{cases} \phi^{-1}(y) & \text{if } y \in \phi(A), \\ y & \text{if } y \notin \phi(A). \end{cases}$$

ϕ is clearly a bijection. We define an addition $\bar{+}$ and a multiplication $\bar{\cdot}$ on $\bar{A}$ by

$$x_1 \bar{+} x_2 = \psi(\psi^{-1}(x_1) + \psi^{-1}(x_2)) \qquad \text{and} \qquad x_1 \bar{\cdot} x_2 = \psi(\psi^{-1}(x_1) \cdot \psi^{-1}(x_2)).$$

It is easy to check that

$$\psi(y_1 + y_2) = \psi(y_1) \bar{+} \psi(y_2) \qquad \text{and} \qquad \psi(y_1 \cdot y_2) = \psi(y_1) \bar{\cdot} \psi(y_2).$$

In addition $\psi(1) = 1$. Thus $\bar{A}$ with the operations just defined is a ring which is isomorphic to B. What remains to be shown is that the operations $\bar{+}$ and $\bar{\cdot}$ restricted to A are the ring operators $+$ and $\cdot$ of A. If $\phi(x_1) = y_1$ and $\phi(x_2) = y_2$, then

$$x_1 \bar{+} x_2 = \psi(y_1 + y_2) = \psi(\phi(x_1) + \phi(x_2)) = \psi(\phi(x_1) + \phi(x_2)) = x_1 + x_2.$$

A similar calcuation gives $x_1 \bar{\cdot} x_2 = x_1 \cdot x_2$. Hence $\bar{A}$ is an extension of A and $\bar{\phi} = \psi^{-1}$ is an isomorphism from $\bar{A}$ onto B. □

When the ring B is an extension of the ring A as defined above we will often write B/A.

We recall that, if F is a field, then the ring $F[X]$ of polynomials with coefficients in F is a PID (principal ideal domain). For $f \in F[X]$ we write (f) for the ideal generated by f, i.e.,

$$(f) = \{gf : g \in F[X]\},$$

and R_f for the quotient ring $F[X]/(f)$. The zero element of the quotient ring is (f). Using the euclidean algorithm we see that, if $f \neq 0$, then every coset has a unique element r with $\deg r < \deg f$. A nonconstant polynomial f is irreducible if there is no pair of nonconstant polynomials g and h such that $f = gh$; if such a pair exists, then we say that f is reducible.

Proposition 1.1 *The following statements are equivalent:*

- **a.** *R_f is a field;*
- **b.** *R_f is an integral domain;*
- **c.** *f is irreducible.*

PROOF **a.** $\Longrightarrow$ **b.** It is sufficient to observe that a field has no zero divisors.
b. $\Longrightarrow$ **c.** Suppose that f is reducible. If $f = gh$, then $(f) = (g + (f))(h + (f))$. As neither $(g + (f)) = (f)$ nor $(h + (f)) = (f)$ we have a pair of zero divisors, a contradiction. Therefore f is irreducible.
c. $\Longrightarrow$ **a.** If $g + (f) \neq (f)$, then $g \notin (f)$ and, from what we have said above, we may suppose that $\deg g < \deg f$. If $\gcd(g, f) \neq 1$, then $1 \leq \deg \gcd(g, f) < \deg f$, a contradiction to the irreducibility of f. Hence $\gcd(g, f) = 1$ and so there are polynomials s and t such that $sg + tf = 1$. It follows that $(s + (f))(g + (f)) = 1 + (f)$, i.e., $g + (f)$ is invertible. □

If E is an extension of F, then we may consider E as a vector space over F. The dimension of E over F, which we write $[E : F]$, is called the degree of the extension. If $[E : F] < \infty$, then we say that the extension is finite, otherwise we say that it is infinite.

Exercise 1.1 *If $f : F \longrightarrow E$ is a ring homomorphism, with F and E fields, then show that f is a monomorphism.*

The next result is fundamental.

Theorem 1.2 *If $f \in F[X]$, with $\deg f \geq 1$, then there is an extension E of F which contains a root of f.*

PROOF Let g be an irreducible factor of f. From the previous proposition we know that $E = R_g$ is a field. As the mapping $\phi : F \longrightarrow R_g, a \longmapsto a + (g)$ is a monomorphism, E is an extension of F. If $g = \sum_{k=0}^{s} a_k X^k$ and $\alpha = X + (g)$, then in E

$$g(\alpha) = \sum_{k=0}^{s} (a_k + (g))\alpha^k = g + (g) = 0.$$

As $g(\alpha) = 0$ in E and g divides f, $f(\alpha) = 0$ in E. □

Exercise 1.2 *Let $f, g \in F[X]$. Show that gcd$(f, g) = 1$ if and only if f and g have no common root in an extension of F. Deduce that if $f \neq g$ are nonconstant polynomials in $F[X]$, which are monic and irreducible, then f and g have no common root in an extension of F.*

If E is an extension of F and $\alpha \in E$, then we write $F(\alpha)$ for the smallest subfield of E containing F and α, i.e., the intersection of all subfields of E containing F and α. In fact, $F(\alpha)$ is the collection of all fractions of the form $\frac{f(\alpha)}{g(\alpha)}$, where $f, g \in F[X]$ and $g(\alpha) \neq 0$. We also say that $F(\alpha)$ is the subfield of E generated by F and α.

1.1 Prime fields

In this section we will show that every field can be considered as an extension of the rational numbers $\mathbf{Q}$ or of a field $\mathbf{F}_p$, for a certain prime number p. We begin with a preliminary result.

Proposition 1.2 *Let R be a subring of a field F and K the intersection of all the subfields of F which contain R. Then $K = Frac(R)$, the field of fractions of R.*

PROOF As R is is a subring of F, R is an integral domain and so $Frac(R)$ is a field. We can define a monomorphism ϕ from $Frac(R)$ into F in the following way:

$$\phi(a) = a \quad \forall a \in R \qquad \text{and} \qquad \phi\left(\frac{a}{b}\right) = \phi(a)\phi(b)^{-1}.$$

We set $L = \operatorname{Im}\phi$. Then L is a subfield of F containing R, hence $K \subset L$. In addition, if G is a subfield of F which contains R, then G contains any element of the form $\phi(a)\phi(b)^{-1}$, with $b \neq 0$, because G is a field and $\phi(R) = R$. Therefore $L \subset G$. It follows that $L \subset K$. Thus $K = L \equiv Frac(R)$. □

The intersection of all the subfields of a given field F is itself a subfield of F, called the *prime field* of F. Clearly F is an extension of its prime subfield.

Theorem 1.3 *The prime subfield of a field F is isomorphic to $\mathbf{Q}$ or to $\mathbf{F}_p$ for some prime number p.*

PROOF Let ϕ be the mapping of $\mathbf{Z}$ into F defined by $\phi(n) = n.1$, where 1 is the identity for the multiplication in F. It is easy to see that ϕ is a ring homomorphism. We write $I = \operatorname{Ker}\phi$. Then I is an ideal of $\mathbf{Z}$ and the factor ring $\mathbf{Z}/I$ is isomorphic to a subring of F, therefore $\mathbf{Z}/I$ is an integral domain, which implies that I is a prime ideal in $\mathbf{Z}$. As ϕ is not the zero mapping, $I = (0)$ or $I = (p)$, where p is a prime number.

In the first case ϕ is injective and the subring $\phi(\mathbf{Z})$ of F is included in P, the prime field of F. From Proposition 1.2 above, P is isomorphic to $Frac(\phi(\mathbf{Z}))$, which is clearly isomorphic to $\mathbf{Q}$.

If $I = (p)$, then $\phi(\mathbf{Z})$ is isomorphic to $\mathbf{Z}/(p)$, which is $\mathbf{F}_p$. However, $\phi(\mathbf{Z})$ is included in every subfield of F and so $\phi(\mathbf{Z}) \subset P$; but $\phi(\mathbf{Z})$ is a subfield of F, hence $P \subset \phi(\mathbf{Z})$. Thus P is isomorphic to $\mathbf{F}_p$. □

This theorem has an important corollary, namely

Corollary 1.1 *If F is a finite field, then the cardinal of F is p^k, where p is a prime number and k a positive integer.*

PROOF The prime subfield P of F must be finite, hence of the form $\mathbf{F}_p$, for some prime number p. If $[F : \mathbf{F}_p] = k$, then $|F| = p^k$. □

Some final remarks before closing this section. It should be clear that, if one field is an extension of another, then they both have the same prime field. Also, if $\mathbf{Q}$ is the prime field of a given field F, then the characteristic of F is 0. On the other hand, if the prime field is $\mathbf{F}_p$, then the characteristic of F is p.

1.2 Algebraic extensions

If E is an extension of F and $\alpha \in E$ is a root of a nonconstant polynomial $f \in F[X]$, then we say that α is *algebraic* over F. If α is not algebraic, then we say it is *transcendental*. If every element of E is algebraic, then we say that E is an *algebraic extension*. An extension which is not algebraic is said to be a *transcendental extension*.

Proposition 1.3 *If $[E : F] < \infty$, then E is an algebraic extension of F.*

PROOF Let $\alpha \in E$ and $[E : F] = n$. The vectors $1, \alpha, \ldots, \alpha^n$ are dependant and so we can find $a_0, a_1, \ldots, a_n \in F$ not all equal to 0 such that $\sum_{i=0}^{n} a_i\alpha^i = 0$. Hence α is a root of the polynomial $f(X) = \sum_{i=0}^{n} a_i X^i$. □

Corollary 1.2 *If an extension is not algebraic, then it is infinite-dimensional.*

PROOF Let E/F be an extension which is not algebraic. By hypothesis, there exists $\alpha \in E$ which is not algebraic over F. If $[E : F] < \infty$, then, from Proposition 1.3, E is an algebraic extension of F, so α is algebraic over F, a contradicition. It follows that E/F is infinite-dimensional. □

Remark We will see below that the converse of Proposition 1.3 is false (example after Corollary 1.5).

If E is an extension of F and $\alpha \in E$ is algebraic over F, then the collection of polynomials $f \in F[X]$ such that $f(\alpha) = 0$ form an ideal I in $F[X]$. The unique monic generator of I, which we note $m(\alpha, F)$, or simply m if the field F is understood, is called the *minimal polynomial of α over F*. A minimal polynomial is clearly irreducible. It should also be noticed that if K/F, E/K and $\alpha \in E$ is algebraic over F, then α is also algebraic over K, since $m(\alpha, F) \in K[X]$.

Proposition 1.4 *If E is an extension of F, $\alpha \in E$ and $\deg m(\alpha, F) = n$, then $[F(\alpha) : F] = n$.*

PROOF We will first show that $F_{n-1}[\alpha]$, the set of polynomials in α of degree strictly less than n is a field and thus is equal to $F(\alpha)$. If $f \in F[X]$ then we may find $g, r \in F[X]$, with $\deg r < n$ such that

$$f(X) = g(X)m(X) + r(X) \Longrightarrow f(\alpha) = g(\alpha)m(\alpha) + r(\alpha) = r(\alpha).$$

Now if $f_1, f_2 \in F[X]$ and we set $f = f_1 f_2$, then we may find $r \in F_{n-1}[X]$ such that $f(\alpha) = r(\alpha)$; therefore $F_{n-1}[\alpha]$ is closed under multiplication. Clearly $F_{n-1}[\alpha]$ is closed under addition. It follows that $F_{n-1}[\alpha]$ is a subring of $F(\alpha)$. To show that it is a field we only need to find an inverse for every nonzero element. If $f \in F_{n-1}(X)$ and $f \neq 0$, then $\deg f < \deg m$. As m is irreducible we may find $g, h \in F[X]$ such that

$$f(X)g(X) + m(X)h(X) = 1 \Longrightarrow f(\alpha)g(\alpha) = 1.$$

However, we have seen that there is $s \in F_{n-1}[X]$ such that $s(\alpha) = g(\alpha)$, hence $f(\alpha)$ has an inverse. We have shown that $F_{n-1}[\alpha] = F(\alpha)$. As the vectors $1, \alpha, \ldots, \alpha^{n-1}$ are independant and α^n is a linear combination of smaller powers of α, these vectors form a basis of $F_{n-1}[\alpha]$; it follows that $[F(\alpha) : F] = n$. □

Corollary 1.3 *If α is algebraic over F, then $F(\alpha)$ is an algebraic extension of F.*

Remark In the course of the proof of Proposition 1.4 we have shown that, if α is algebraic, then $F(\alpha) = F[\alpha]$.

As examples of algebraic extensions we will consider quadratic number fields. We say that a finite extension E of $\mathbf{Q}$ in $\mathbf{C}$ is a *number field*. It is quadratic if the degree of the extension is 2. Suppose that $d \in \mathbf{Z}$ is not a square and let α be a square root of d. If $d > 0$, then we usually suppose that α is the positive root and, if $d < 0$, then α is the product of i and the positive root of $-d$. In both cases we write $\sqrt{d}$ for α. If $\sqrt{d} = \frac{a}{b} \in \mathbf{Q}$, then $b^2 d = a^2$, which is impossible because d is not a square. It follows that $\deg m(\sqrt{d}, \mathbf{Q}) > 1$. As $\sqrt{d}$ is a root of the polynomial $P(X) = -d + X^2$, we have $P(X) = m(\sqrt{d}, \mathbf{Q})$. It follows that $[\mathbf{Q}(\sqrt{d}) : \mathbf{Q}] = 2$ and that $(1, \sqrt{d})$ is a basis of $\mathbf{Q}(\sqrt{d})$ over $\mathbf{Q}$.

If d is a square, then $\sqrt{d} \in \mathbf{Z}$ and so $\mathbf{Q}(\sqrt{d}) = \mathbf{Q}$, so we exclude this case. On the other hand, if $d = u^2 v$, where v is square-free, then $\mathbf{Q}(\sqrt{d}) = \mathbf{Q}(\sqrt{v})$, so we can limit our attention to square-free integers d. The following result is a little unexpected.

Theorem 1.4 *If m and n are square-free integers and $m \neq n$ then $\mathbf{Q}(\sqrt{m})$ is not isomorphic to $\mathbf{Q}(\sqrt{n})$.*

PROOF Suppose that there is un isomorphism ϕ from $\mathbf{Q}(\sqrt{m})$ onto $\mathbf{Q}(\sqrt{n})$. As $\phi(1) = 1$, ϕ must fix all elements of $\mathbf{Q}$. Let $\phi(\sqrt{m}) = a + b\sqrt{n}$. If $b = 0$, we have a $\phi(a) = a = \phi(\sqrt{m})$, which contadicts the fact that ϕ is injective, so $b \neq 0$. Also

$$m = \phi(m) = \phi((\sqrt{m})^2) = (\phi\sqrt{m})^2 = (a + b\sqrt{n})^2 = a^2 + 2ab\sqrt{n} + b^2 n.$$

If $a \neq 0$, then $\sqrt{n} = \frac{m-a^2-b^2n}{2ab} \in \mathbf{Q}$, a contradiction. Hence $a = 0$ and $m = b^2 n$. If $b = \frac{e}{f}$, with $(e, f) = 1$, then we have $e^2 m = f^2 n$, which is only possible if $e^2 = f^2$, because m and n are square-free. It follows that $b^2 = 1$ and so $m = n$. $\square$

A little later we will see that all quadratic number fields are of the form we have seen here.

Suppose that F, K and E are fields with K an extension of F and E an extension of K. We now consider the relation between the degrees of the extensions. We recall that any vector space over a field has a basis which may be infinite.

Proposition 1.5 *If $(\beta_j)_{j \in J}$ is a basis of K over F and $(\alpha_i)_{i \in I}$ a basis of E over K, then $(\alpha_i \beta_j)_{i \in I, j \in J}$ is a basis of E over F.*

PROOF If $\gamma \in E$, then γ is a linear combination of α_i, with coefficients $a_i \in K$. As each a_i is a linear combination of β_j, with coefficients $b_j \in F$, γ is a linear combination of $\alpha_i \beta_j$, with coefficients in F. Thus the set $(\alpha_i \beta_j)_{i \in I, j \in J}$ generates E. To show that it is a basis of E over F, we must show that it is independant. To do so, let us consider a (finite) linear combination $\sum \lambda_{ij} \alpha_i \beta_j$, with $\lambda_{ij} \in F$, whose value is 0. Adding some terms $\lambda_{ij} \alpha_i \beta_j$, with $\lambda_{ij} = 0$ if necessary, we may write

$$0 = \sum_{i,j} \lambda_{ij} \alpha_i \beta_j = \sum_i \left(\sum_j \lambda_{ij} \beta_j \right) \alpha_i.$$

As the α_i are independant, $\sum_j \lambda_{ij} \beta_j = 0$ for every i. However, the β_j are independant and so $\lambda_{ij} = 0$, for each pair (i, j). Hence the elements $\alpha_i \beta_j$ form an independant collection. We have shown that $(\alpha_i \beta_j)_{i \in I, j \in J}$ is a basis of E over F. $\square$

This leads to the following statement, often referred to as the *multiplicativity of the degree*:

Corollary 1.4 *If K/F and E/K, then*

$$[E : F] = [E : K][K : F].$$

Suppose now that E is an extension of F and that $\alpha_1, \ldots, \alpha_n \in E$. We denote $F(\alpha_1, \ldots, \alpha_n)$ the subfield of E generated by F and the α_i, i.e., the smallest subfield of E containing F and the α_i. (We have already seen this notion when there is only one α_i.) In fact, this field is the collection of all fractions of the form $\frac{f(\alpha_1,\ldots,\alpha_n)}{g(\alpha_i,\ldots,\alpha_n)}$, where $f, g \in F[X_1, \ldots, X_n]$ and the denominator is nonzero. We may generalize Corollary 1.3.

Corollary 1.5 *If $\alpha_1, \ldots, \alpha_n$ are algebraic over F, then $F(\alpha_1, \ldots, \alpha_n)$ is a finite extension of F, hence an algebraic extension of F. Moreover, $F(\alpha_1, \ldots, \alpha_n) = F[\alpha_1, \ldots, \alpha_n]$.*

PROOF Let us set

$$E_0 = F, E_1 = F(\alpha_1), E_2 = F(\alpha_1, \alpha_2), \ldots, E_n = F(\alpha_1, \alpha_2, \ldots, \alpha_n).$$

Then $E_k = E_{k-1}(\alpha_k)$ and α_k is algebraic over E_{k-1}. Now $[E_k : E_{k-1}] = \deg m(\alpha_k, E_{k-1})$ and

$$[E_n : F] = \prod_{k=0}^{n-1} [E_{k+1} : E_k] < \infty,$$

the result we were looking for.

To prove the second statement we use a simple induction argument. We have aleady seen that it is true for $n = 1$. (See the remark after Corollary 1.3). If we suppose that the statement is true up to $n - 1$, then we have

$$\begin{aligned} F(\alpha_1, \ldots, \alpha_n) &= F(\alpha_1, \ldots, \alpha_{n-1})(\alpha_n) \\ &= F[\alpha_1, \ldots, \alpha_{n-1}](\alpha_n) \\ &= F[\alpha_1, \ldots, \alpha_{n-1}][\alpha_n] \\ &= F[\alpha_1, \ldots, \alpha_{n-1}, \alpha_n], \end{aligned}$$

which concludes the induction step and hence the proof. □

Example Consider the extension $E = \mathbf{Q}(\sqrt[n]{2} : n \in \mathbf{N}^*)$ of $\mathbf{Q}$. Any element $\alpha \in E$ is algebraic over $\mathbf{Q}$, because $\alpha \in \mathbf{Q}(\sqrt[n]{2} : n = 1, \ldots, N)$, for some $N \in \mathbf{N}^*$, and $\sqrt[n]{2}$ is algebraic over $\mathbf{Q}$. Hence E is an algebraic extension of $\mathbf{Q}$. For any $n \in \mathbf{N}^*$, by the Eisenstein criterion, $f_n(X) = -2 + X^n$ is irreducible and hence the minimal polynomial of $\sqrt[n]{2}$. However, $E_n \subset E$, where $E_n = \mathbf{Q}(\sqrt[n]{2})$, and, from Proposition 1.4, $[E_n : \mathbf{Q}] = n$. This implies that $[E : \mathbf{Q}] \geq n$, for all $n \in \mathbf{N}^*$. Thus we have found an algebraic extension of $\mathbf{Q}$, which is not finite.

We will see later that we may partially rectify this situation by imposing conditions on the algebraic extension.

If E is an extension of F then we will write $A(E/F)$ (or simply A when the fields E and F are understood) for the collection of elements of E which are algebraic over F.

Proposition 1.6 *$A(E/F)$ is a subfield of E.*

PROOF It is sufficient to show that if $\alpha, \beta \in A$, then α, $-\alpha$, $\alpha+\beta$, $\alpha\beta$ and β^{-1}, with $\beta \neq 0$, belong to A. However, $F(\alpha,\beta)$ is an algebraic extension of F, therefore $F(\alpha,\beta) \subset A$. As $\alpha, -\alpha, \alpha+\beta, \alpha\beta, \beta^{-1} \in F(\alpha,\beta)$, these elements belong to A. □

Remark Proposition 1.6 ensures that $A(\mathbf{C}/\mathbf{Q})$ is an algebraic extension of $\mathbf{Q}$. It contains all the algebraic extensions of $\mathbf{Q}$ and is an infinite extension, after the example following Corollary 1.5.

Exercise 1.3 *We have seen that if α and β are algebraic, then $\alpha+\beta$ and $\alpha\beta$ are algebraic. Prove the converse, namely, if $\alpha+\beta$ and $\alpha\beta$ are algebraic, then α and β are algebraic.*

We may define a relation $\mathcal{R}$ on the collection of fields by $F\mathcal{R}E$ if E is an algebraic extension of F. This relation is in fact a partial order. Clearly $\mathcal{R}$ is reflexive and antisymmetric, so we only need to show that it is transitive. To do so we need the following preliminary result.

Proposition 1.7 *If K is an algebraic extension of F, E/K and $\alpha \in E$ is algebraic over K, then α is algebraic over F.*

PROOF Let $m(\alpha, K) = \sum_{k=0}^{n} a_i X^i$, with $a_i \in K$, for $i = 0, \ldots, n$, and $a_n = 1$. As the a_i, for $i = 0, \ldots, n$, are algebraic over F, $A = F(a_0, a_1, \ldots, a_{n-1})$ is a finite extension of F, by Corollary 1.5. Now, α is algebraic over A, therefore $A(\alpha)$ is a finite extension of A, by Proposition 1.4. Corollary 1.4 ensures that $A(\alpha)$ is a finite extension of F. Proposition 1.3 now implies that α is algebraic over F. □

Corollary 1.6 *The relation $\mathcal{R}$ is transitive, hence a partial order.*

Exercise 1.4 *Suppose that E is an algebraic extension of F and that R is a ring containing F and included in E, i.e., $F \subset R \subset E$. Show that R is a field.*

1.3 Algebraic numbers

An element $\alpha \in \mathbf{C}$ which is algebraic over $\mathbf{Q}$ is said to be an *algebraic number*. This is equivalent to saying that there is a polynomial $f \in \mathbf{Z}[X]$ such that $f(\alpha) = 0$. If $\alpha \in \mathbf{C}$ is not algebraic then we call α a *transcendental number*. We aim to show that $A(\mathbf{C}/\mathbf{Q})$ is countable.

Proposition 1.8 *Let $(E_n)_{n\in\mathbf{N}}$ be a countable collection of countable subsets of a set E. Then the union $S = \cup_{n\in\mathbf{N}} E_n$ is countable.*

PROOF We set $F_0 = E_0$ and $F_n = E_n \setminus (E_0 \cup E_1 \cup \cdots \cup E_{n-1})$, for $n > 0$. Then $S = \cup_{n\in\mathbf{N}} F_n$ and, if $m \neq n$, then $F_m \cap F_n = \emptyset$. Let $f_n : E_n \longrightarrow \mathbf{N}$ be an injection and let us set, for $x \in F_n$, $f(x) = (n, f_n(x))$. It is not difficult to see that f is an injection from S into $\mathbf{N}^2$. As $\mathbf{N}^2$ is countable, S is countable. □

Corollary 1.7 *The collection of polynomials $\mathbf{Z}[X]$ is countable.*

PROOF We note P_d the subset of $\mathbf{Z}[X]$ composed of polynomials whose degree is $d \geq 0$. We obtain a bijection of P_d into $\mathbf{Z}^{d+1}$ by associating to each polynomial f its sequence of coefficients $(a_0, a_1, \ldots, a_d)$. As $\mathbf{Z}^{d+1}$ is countable, P_d is also countable. From the previous proposition $\cup_{d\in\mathbf{N}} P_d$ is countable. If we now add the polynomial 0, we obtain the result. □

We may now prove the result mentioned in the first paragraph.

Theorem 1.5 $A(\mathbf{C}/\mathbf{Q})$ *is countable.*

PROOF From the previous corollary we know that $\mathbf{Z}[X]$ is countable. The subset of $\mathbf{Z}[X]$ composed of nonconstant polynomials is also countable: we may number these polynomials $f_0, f_1, \ldots$. For each $k \in \mathbf{N}$, let R_k be the (finite) set of roots of f_k. Then, from Proposition 1.8, $A(\mathbf{C} \setminus \mathbf{Q}) = \cup R_k$ is countable. □

Corollary 1.8 *The collection of transcendental numbers is not countable.*

As $A(\mathbf{C}/\mathbf{Q})$ is a field, it is easy to construct algebraic numbers. For example, $\sqrt{2}$ and $\sqrt{3}$ are algebraic numbers, hence their sum, $\sqrt{2} + \sqrt{3}$, is also an algebraic number. Although the transcendental numbers form a much larger set, it is not easy to find explicit examples. We know that e and π are transcental, however the proofs are not easy, in particular for π. It is an open question whether the following numbers are transcendental or not: $\pi + e$, $\pi - e$, πe, $\frac{e}{\pi}$, π^π, e^e and π^e.

Exercise 1.5 *Show that, if α and β are both transcendental, then either $\alpha + \beta$ or $\alpha\beta$ is transcendental.*

Chapter 2

Splitting fields

Let E be an extension of the field F and $f \in F[X]$. We say that f splits in E, if we can write

$$f(X) = \lambda(X - \alpha_1) \cdots (X - \alpha_n),$$

with $\lambda \in F$ and $\alpha_1, \ldots, \alpha_n \in E$. Such a field always exists: it is sufficient to apply Theorem 1.2 an appropriate number of times. We say that an extension E of F is a *splitting field* of $f \in F[X]$ if f splits in E and does not do so in any proper subfield of E.

Proposition 2.1 *Let E be an extension of F such that $f \in F[X]$ splits in E:*

$$f(X) = \lambda(X - \alpha_1) \cdots (X - \alpha_n).$$

Then E is a splitting field of f if and only if $E = F(\alpha_1, \ldots, \alpha_n)$.

PROOF Suppose first that E is a splitting field of f. Then E contains F and the elements $\alpha_1, \ldots \alpha_n$, therefore $F(\alpha_1, \ldots, \alpha_n) \subset E$. As f does not split in any proper subfield of E, we must have equality.

Now suppose that $E = F(\alpha_1, \ldots, \alpha_n)$ and let G be a subfield of E such that f splits in G. Then G contains F and the elements $\alpha_1, \ldots, \alpha_n$, hence $F(\alpha_1, \ldots, \alpha_n) \in G$. It follows that $E \subset G$ and so $E = G$. Thus E is a splitting field of f. □

Corollary 2.1 *If $f \in F[X]$ splits in an extension E of F, then E contains a unique splitting field of f, namely $F(\alpha_1, \ldots, \alpha_n)$.*

We can obtain an explicit presentation of a splitting field.

Proposition 2.2 *The splitting field S of $f \in F[X]$ in an extension E of F can be written*

$$S = F(\alpha_1, \ldots, \alpha_n) = F[\alpha_1, \ldots, \alpha_n],$$

i.e., S is composed of the polynomials in the roots α_i, with coefficients in F.

PROOF The splitting field S of f clearly has the form $F(\alpha_1, \ldots, \alpha_n)$. As for the second equality, we only need to notice that the roots $\alpha_1, \ldots, \alpha_n$ are algebraic over F and then apply Corollary 1.5.□

If E is a splitting field of $f \in F[X]$, then we can say something about order of the extension.

Theorem 2.1 *If $f \in F[X]$ and $\deg f = n$, then there is a splitting field E of f such that $[E : F] \leq n!$.*

PROOF If $\deg f = 0$, then f is constant and we can take $E = F$. Now let us suppose that $\deg f = n \geq 1$. From Proposition 1.2 we know that there is an extension E' of F which contains a root α of f. The minimal polynomial $m = m(\alpha, F)$ divides f, so $\deg m \leq \deg f$. Now, from Proposition 1.4, $[F(\alpha) : F] = \deg m$, so there exists an extension E_1 of F which contains a root α_1 of f and is such that with $[E_1 : F] \leq n$. In E_1 we can write $f(Y) = (Y - \alpha_1)^{r_1} g(Y)$, where $r_1 \geq 1$ and $g(\alpha_1 \neq 0$. If g is not constant, then we can find an extension E_2 of E_1 which contains a root α_2 of g (and hence of f) and is such that $[E_2 : E_1] \leq n - 1$. E_2 is an extension of F which contains α_1 and α_2 and $[E_2 : F] = [E_2 : E_1][E_1 : F] \leq (n-1)n$. Continuing in the same way we obtain an extension E of F in which f splits and such that $[E : F] \leq n!$. To finish it is sufficient to notice that E contains a splitting field of f. □

We have seen that every polynomial has a splitting field. We now aim to show that all such fields are isomorphic. We will begin with two preliminary results.

Lemma 2.1 *Let $f \in F[X]$ be irreducible and E an extension of F which contains a root α of f. Then there is an isomorphism*

$$\Phi : F[X]/(f) \longrightarrow F(\alpha)$$

which fixes F, i.e., for g constant, $\Phi(g + (f)) = g$, and such that $\Phi(X + (f)) = \alpha$.

PROOF The mapping $\phi : F[X] \longrightarrow E$ defined by $\phi(g) = g(\alpha)$ is a ring homomorphism. As f is irreducible and $f \in \operatorname{Ker} \phi$, we have $\operatorname{Ker} \phi = (f)$. It follows that the mapping

$$\Phi : F[X]/(f) \longrightarrow \operatorname{Im} \phi, g + (f) \longmapsto \phi(g)$$

is a ring isomorphism which fixes F. In addition,

$$\operatorname{Im} \Phi = \operatorname{Im} \phi = \{g(\alpha) : g \in F[X]\} \subset F(\alpha). \tag{2.1}$$

As f is irreducible, (f) is maximal and so $F[X]/(f)$ is a field. Thus $\operatorname{Im} \Phi$ a field. However, F and α belong to $\operatorname{Im} \Phi$, which implies that $F(\alpha) \subset \operatorname{Im} \Phi$. From the equation (2.1) we obtain equality. □

Lemma 2.2 *Let R and S be rings, I is an ideal of R and J an ideal of S. If $\phi : R \longrightarrow S$ is an isomorphism such that $\phi(I) = J$, then the mapping*

$$\bar{\phi} : R/I \longmapsto S/J, x + I \longmapsto \phi(x) + J$$

is well-defined and is an isomorphism.

PROOF Left to the reader. □

If F and F' are fields and $\sigma : F \longrightarrow F'$ is an isomorphism, then by setting

$$\sigma^*(\sum a_i X^i) = \sum \sigma(a_i) X^i$$

we obtain an isomorphism from the ring $F[X]$ onto the ring $F'[X]$. We will say that σ^* corresponds to σ. We will often write f^* for $\sigma^*(f)$.

Proposition 2.3 *Let $\sigma : F \longrightarrow F'$ be an isomorphism and $f \in F[X]$ irreducible. If E (resp. E') is an extension of F (resp. F') and α (resp. α') a root of f (resp. f^*) in E (resp. E'), then there is an isomorphism $\hat{\sigma} : F(\alpha) \longrightarrow F'(\alpha')$ extending σ, with $\hat{\sigma}(\alpha) = \alpha'$. This isomorphism is unique.*

PROOF First we notice that $\sigma^*(f) = (f^*)$; from the preceding lemma the mapping

$$\bar{\sigma^*} : F[X]/(f) \longrightarrow F'[X]/(f^*), g + (f) \longmapsto \sigma^*(g) + (f^*)$$

is an isomorphism. We now set $\hat{\sigma}$ as the composition

$$F(\alpha) \xrightarrow{\Phi^{-1}} F[X]/(f) \xrightarrow{\bar{\sigma^*}} F'[X]/(f^*) \xrightarrow{\Phi'} F'(\alpha').$$

$\hat{\sigma}$ is an isomorphism extending σ and $\hat{\sigma}(\alpha) = \alpha'$. The uniqueness is clear. $\square$

We are now in a position to prove the result referred to above, namely that splitting fields are isomorphic. We will in fact prove a more general result and derive that on splitting fields as a corollary.

Theorem 2.2 *Let F and F' be fields, $\sigma : F \longrightarrow F'$ an isomorphism, $f \in F[X]$ and $f^* \in F'[X]$ the polynomial corresponding to f. If E is a splitting field of f and E' a splitting field of f^*, then there is an isomorphism $\tilde{\sigma} : E \longrightarrow E'$ extending σ.*

PROOF We will prove this result by recurrence on $n = [E : F]$. First, if $n = 1$, then $E = F$ and $f \in F[X]$ and f is a product of linear factors (polynomials of degree 1) and it follows that f^* is also a product of such factors, so $E' = F'$ and we can define $\tilde{\sigma} = \sigma$.

Now let us suppose that $n > 1$ and that the result is true up to $n - 1$. Let g be an irreducible factor of f with $\deg g \geq 2$ and α a root of g in E ($\alpha \in E$ because α is a root of f). Let g^* be the polynomial in $F'[X]$ corresponding to g and α' a root of g^* ($\alpha' \in E'$ because α' is a root of f^*). From Proposition 2.3 there is a unique isomorphism $\hat{\sigma} : F(\alpha) \longrightarrow F'(\alpha')$ which extends σ and is such that $\hat{\sigma}(\alpha) = \alpha'$. Now, E is a splitting field of f over $F(\alpha)$ and E' a splitting field of f^* over $F'(\alpha')$. As

$$[E : F] = [E : F(\alpha)][F(\alpha) : F]$$

and $[F(\alpha) : F] \geq 2$, we have $[E : F(\alpha)] < n$. By the induction hypothesis there is an isomorphism $\tilde{\sigma} : E \longrightarrow E'$, which extends $\hat{\sigma}$, and hence σ. $\square$

Corollary 2.2 *If $f \in F[X]$ and E and E' are splitting fields of f over F, then E and E' are isomorphic.*

PROOF It is sufficient to take $F' = F$ and $\sigma = \mathrm{id}_F$ in the previous theorem. $\square$

Example Let $f(X) = -2+X^3 \in \mathbf{Q}[X]$. The roots of f in $\mathbf{C}$ are $\alpha_1 = \sqrt[3]{2} \in \mathbf{R}$, $\alpha_2 = \alpha_1(-\frac{1}{2}+\frac{\sqrt{2}}{2})$ and $\alpha_1(-\frac{1}{2} - \frac{\sqrt{2}}{2})$. As none of the roots belong to $\mathbf{Q}$, f is irreducible. As f is also monic f is the minimal polynomial of α_1 and so $[\mathbf{Q}(\alpha_1) : \mathbf{Q}] = 3$. The field $\mathbf{Q}(\alpha_1)$ cannot be the splitting field in $\mathbf{C}$ of f, because $\mathbf{Q}(\alpha_1) \subset \mathbf{R}$ and $\alpha_2 \notin \mathbf{R}$. The field $K = \mathbf{Q}(\alpha_1, \sqrt{3}i) \subset \mathbf{Q}(\alpha_1, \alpha_2, \alpha_3)$; as α_1, α_2, α_3 belong to $\mathbf{Q}$ lie in K, we have $K = \mathbf{Q}(\alpha_1, \alpha_2, \alpha_3)$, i.e., K is the splitting field of f in $\mathbf{C}$.

We only need to find the degree of the extension. From Theorem 2.1 we know that it cannot be greater than $3! = 6$. It also must be a multiple of 3, because

$$[K : \mathbf{Q}] = [K : \mathbf{Q}(\alpha_1)][\mathbf{Q}(\alpha_1) : \mathbf{Q}] = [K : \mathbf{Q}(\alpha_1)]3.$$

If $[K : \mathbf{Q}] = 3$, then $[K : \mathbf{Q}(\alpha_1)] = 1$ and $K = \mathbf{Q}(\alpha_1)$, which is false; hence $[K : \mathbf{Q}] = 6$.

Exercise 2.1 *Find the splitting field K of $f(X) = 4 - 2X + X^2 \in \mathbf{Q}[X]$ in $\mathbf{C}$ and determine the degree of the extension of K over $\mathbf{Q}$.*

Exercise 2.2 *Let C be a family of polynomials in $F[X]$ and K an extension of F such that every f in C splits over K; if, for every proper subfield K' of K, at least one member of C does not split over K', then we say that K is a splitting field of C. Show that, C is finite and K is a splitting field of C, then there is a polynomial $f \in F[X]$ for which K is a splitting field.*

2.1 Existence of finite fields

We recall that we previously saw that the cardinal of a finite field must be p^k, where p is a prime number and k a positive integer. In this section we show that, for any such p^k, there is a finite field F whose cardinal is precisely p^k, and that, in addition, there is essentially only one such finite field. We will use our knowledge of splitting fields in the proofs. We begin with a preliminary result, but for this we need a lemma.

Lemma 2.3 *Let $f, g \in \mathbf{F}[X]$ be nonconstant. Then f and g are relatively prime if and only if they do not have a root in any extension field of $\mathbf{F}$.*

PROOF Assume that f and g are relatively prime in $\mathbf{F}[X]$. Then there exist $u, v \in \mathbf{F}[X]$ such that
$$f(X)u(X) + g(X)v(X) = 1.$$
If α is a common root of f and g in some field extension of $\mathbf{F}$, then substituting α for X we obtain 0 on the left-hand side and 1 on the right-hand side of the equation, a contradiction. Hence f and g have no common root in an extension field of $\mathbf{F}$.

Now suppose that f and g are not relatively prime. Then f and g have a common factor h, which is not a constant. There is a field extension of $\mathbf{F}$ in which h has a root α. Clearly, α is a common root of f and g. □

Proposition 2.4 *If $f \in F[X]$, then f has a multiple root in a splitting field if and only if $\gcd(f, f') \neq 1$.*

PROOF Suppose that f has a multiple root α in a splitting field. Then $f(X) = (X - \alpha)^s g(X)$, where $s \geq 2$ and $g(\alpha) \neq 0$. Hence,
$$f'(X) = s(X - \alpha)^{s-1}g(X) + (X - \alpha)^s g'(X)$$
and so $f'(\alpha) = 0$. From the previous lemma f and f' are not relatively prime, i.e., $\gcd(f, f') \neq 1$.

Now suppose that $\gcd(f, f') \neq 1$. From the previous lemma, f and f' have a common root α in an extension field of $\mathbf{F}$. We may write
$$f(X) = (X - \alpha)^s g(X),$$
with $s \geq 1$ and $g(\alpha) \neq 0$. Then again
$$f'(X) = s(X - \alpha)^{s-1}g(X) + (X - \alpha)^s g'(X).$$
If $s = 1$, then $f'(\alpha) = g(\alpha) \neq 0$, a contradiction, hence $s \geq 2$ and α is a multiple root. □

Theorem 2.3 *If p is a prime number and k a positive integer, then there is a field F whose cardinal is p^k.*

PROOF To simplify the notation we set $q = p^k$. For $k = 1$, we may take $\mathbf{F}_p$. We now suppose that $k > 1$. We set $f(X) = -X + X^q \in \mathbf{F}_p[X]$. As $f'(X) = -1 + qX^{q-1} = -1$, because q is a multiple of p, $\gcd(f, f') = 1$ and so the roots of f in a splitting field are distinct, i.e., there are q roots (Proposition 2.4). Let E be an extension of $\mathbf{F}_p$ which contains the roots of f and F the set of roots. We claim that F is a field. First, if $a \in F$, then

$$0 = f(a) = -a + a^q \Longleftrightarrow x = x^q.$$

We take $x, y \in F$. Then

$$(xy)^q = x^q y^q = xy \Longrightarrow f(xy) = 0 \quad \text{and} \quad (x+y)^q = x^q + y^q = x + y \Longrightarrow f(x+y) = 0.$$

If $p \neq 2$, then

$$(-x)^q = (-1)^q x^q = -x$$

and, if $p = 2$, then

$$(-x)^q = (-1)^q x^q = x^q = x = -x,$$

because the characteristic of E is 2. In both cases we have $f(-x) = -x$. It follows that F is a subring of of E. In addition, if $x \neq 0$, then, using the fact that F is an integral domain, we have

$$-x + x^q = 0 \Longrightarrow -1 + x^q = 0 \Longrightarrow xx^{q-2} = 1,$$

hence x has an inverse for the multiplication. Thus F is a field. We have constructed a field with $q = p^k$ elements. □

We now turn to the uniqueness of finite fields. We should notice that the field F constructed in the proof of preceding theorem is a splitting field for the polynomial f. Any proper subfield of F will lack certain elements of F. As these are all roots of f, f cannot split over such a subfield.

Theorem 2.4 *If F and F' are two finite fields with the same cardinality, then F is isomorphic to F'.*

PROOF If F is a finite field with cardinality $q = p^k$, then F has the prime field $\mathbf{F}_p$. There $q-1$ elements in F^* so, if $x \in F^*$, then $x^{q-1} = 1$ and it follows that $-x + x^q = 0$, for all $x \in F$. Thus the roots of the polynomial $f(X) = -X + X^q \in \mathbf{F}_p[X]$ are the elements of F and it follows that F is a splitting field of f. As all splitting fields of a given polynomial are isomorphic, if F' is another field with cardinality q, then F' is isomorphic to F. □

Notation We often write $\mathbf{F}_q$ for a finite field with q elements.

2.2 Algebraic closures

We have seen that if $f \in F[X]$ then there is an extension E of F over which f splits. It is natural to ask if there exists an extension C of F such that every $f \in F[X]$ splits over this extension. (It is well-known that $\mathbf{C}$ is such an extension of $\mathbf{R}$; however, we will give a proof of this later on in the text.) In this section we aim to study this question. We will begin with an elementary result.

Proposition 2.5 *For a field C the following conditions are equivalent*

- **a.** *Every nonconstant polynomial $f \in C[X]$ has a root $\alpha \in C$;*

- **b.** *Every nonconstant polynomial* $f \in C[X]$ *splits over* C*;*

- **c.** *Every irreducible polynomial* $f \in C[X]$ *is of degree* 1*;*

- **d.** C *has no proper algebraic extension.*

PROOF **a.** $\Longrightarrow$ **b.** If f is nonconstant, then the condition **a.** implies that we can write $f(X) = (X-\alpha)g(X)$. If g is not constant, then we can write $g(X) = (X-\beta)h(X)$. Continuing the process if necessary we finally obtain a splitting of f.
b. $\Longrightarrow$ **c.** If f is irreducible, then f is not constant. From the condition **b.** f splits over C:

$$f(X) = \lambda(X-\alpha_1)\cdots(X-\alpha_n).$$

As f is irreducible, f has a unique nonconstant facteur, i.e., $n = 1$.
c. $\Longrightarrow$ **d.** Let E be an algebraic extension of C and $\alpha \in E$. If $f = m(\alpha, C)$, then f is irreducible and so of degree 1: $f(X) = X - \alpha$. Hence $\alpha \in C$. Thus $E = C$.
d. $\Longrightarrow$ **a.** Let $f \in C[X]$ nonconstant. We can find an extension E of C which contains a root α of f. We may suppose that this extension is finite and so algebraic. From the condition **d.**, $E = C$ and so $\alpha \in C$. $\square$

A field satisfying the conditions of the above proposition is said to be *algebraically closed*. An extension C of a field F is an *algebraic closure* of F if C is algebraic over F and algebraically closed.

Remark An algebraically closed field is infinite. To see this, suppose that F is algebraically closed and finite, with elements $a_1, \dots, a_n$. However, the polynomial $f(X) = 1 + \prod_{i=1}^n(-a_i + X)$ has no root in F, contradicting the fact that F is algebraically closed.

Exercise 2.3 *If* E *is an algebraic extension of* F *and* C *an algebraic closure of* E*, show that* C *is an algebraic closure of* F*.*

Remark If C is an algebraic closure of F and E is an extension of F which is strictly included in C, then E is not algebraically closed. To see this, let $\alpha \in C \setminus E$. As α is algebraic over F, α is algebraic over E. Now, $\alpha \notin E$, hence $\deg m(\alpha, E) > 1$; from the condition **c.** of the above proposition, E is not algebraically closed.

Proposition 2.6 *Let* C *be an algebraic extension of* F*. Then* C *is an algebraic closure of* F *if every nonconstant polynomial* $g \in F[X]$ *splits over* C*. (We do not need to consider polynomials* $f \in C[X] \setminus F[X]$*).*

PROOF Let $f \in F[X]$ and α be a root of f in an extension E of C. The field $C(\alpha)$ is an algebraic extension of F and C is algebraic over F by hypothesis, therefore $C(\alpha)$ is algebraic F. Thus α is the root of a polynomial $g \in F[X]$. As g splits over C, all the roots of g belong to C, in particular $\alpha \in C$. Thus f has a root in C. $\square$

If E and E' are extensions of F and $\sigma : E \longrightarrow E'$ is a homomorphism fixing F (i.e., $\sigma(x) = x$, for all $x \in F$), then we call σ an $F-$ *homomorphism.* The following proposition is well-known if E is a finite extension of F. However, we may relax the conditions:

Proposition 2.7 *Let* E *be an algebraic extension of* F *and* $\sigma : E \longrightarrow E$ *an* F*-homomorphism. If* σ *is injective, then it is also surjective.*

PROOF Let $\alpha \in E$. We have to show that there exists $\beta \in E$ such that $\alpha = \sigma(\beta)$. Let $m = m(\alpha, F)$ and L be the subfield of E generated by F and the roots of m which are in E. These roots are algebraic over F, therefore L is a finite extension of F (see Corollary 1.5). If α' is a root of m in E, then $\sigma(\alpha')$ is also a root of m in E, because σ is an F-homomorphism and so $\sigma(L) \subset L$. However, σ is a linear mapping from the F-vector space L into itself, because F is fixed by σ. As L is finite-dimensional over F and σ injective, $\sigma_{|L} : L \longrightarrow L$ is also surjective. Moreover, $\alpha \in L$, thus there exists $\beta \in L \subset E$ such that $\alpha = \sigma(\beta)$. □

We now prove the most difficult step in showing that a field always has an algebraic closure.

Theorem 2.5 *Every field F has an extension E which is algebraically closed.*

PROOF We note S the collection of nonconstant polynomials of $F[X]$. To each $f \in S$ we associate a variable X_f. Now we let T be the family of these variables and $F[T]$ the ring of polynomials in these variables. (The elements of $F[T]$ are finite sums of monomials of the form $aX_{f_1} \cdots X_{f_s}$, with $a \in F$.) Finally we define I to be the ideal generated by the elements of the form $f(X_f)$, with $f \in S$. (If $f(X) = \sum_{i=0}^n a_i X^i$, then $f(X_f) = \sum_{i=0}^n a_i X_f^i$.). In fact, I is a proper ideal of $F[T]$ as we will now see. If this is not the case, then we can find elements $g_i \in F[T]$ and $f_i \in I$ such that

$$\sum_{i=1}^{s} g_i f_i = 1.$$

Let us write X_i for the variable associated with f_i. There is a finite number of variables $X_1, \ldots, X_m$ with $m \geq s$, which are variables of the g_i. Hence we have

$$\sum_{i=1}^{s} g_i(X_1, \ldots, X_m) f_i(X_i) = 1.$$

(Even if a certain variable X_k does appear explicitly in a certain g_i we can still include it.) Suppose now that E is an extension of F which contains all the roots of the f_i. Then E contains a root α_i of each f_i. If we set $X_i = \alpha_i$ for $1 \leq i \leq s$ and $X_i = 0$ for $s < i \leq m$, then we obtain $0 = 1$, a contradiction. It follows that I is a proper ideal of $F[T]$.

As I is a proper ideal, I is included in a maximal ideal M. The factor ring $E_1 = F[T]/M$ is a field, because M is maximal. The canonical homomorphism

$$\phi : F \longrightarrow E_1, a \longmapsto a + M$$

is injective: If $\phi(a) = 0$ and $a \neq 0$, then $a + M = M$ and

$$(a^{-1} + M)(a + M) \subset M \Longrightarrow 1 \in M,$$

a contradiction. Hence we can write $F \subset E_1$. If $f \in F[X]$ is nonconstant, then $X_f \in E_1$ and

$$f(X_f + M) = f(X_f) + M = 0,$$

because $f(X_f) \in I \subset M$. Therefore f has a root in E_1.

We can now replace F by E_1 and repeat the whole argument to obtain an extension E_2 of E_1 such that every nonconstant polynomial $g \in E_1[X]$ has a root in E_2. Continuing in the same way we obtain a chain of extensions

$$F \subset E_1 \subset E_2 \subset \cdots$$

such that a nonconstant polynomial $h \in E_n[X]$ has a root in E_{n+1}. We now let E be the union of the fields in the chain and we define an addition $\oplus$ and a multiplication $\odot$ on E as follows: If $x \in E_m$ and $y \in E_n$, with $m \leq n$, then $x \oplus y = x +_n y$ and $x \odot y = x \cdot_n y$. These operations are well-defined ($x \oplus y$ and $x \odot y$ do not depend on the choice of $n \geq m$) and a simple check shows that $(E, \oplus, \odot)$ is a field.

Now let f be a nonconstant polynomial in $E[X]$. All the coefficients of f belong to a certain E_n and so f has a root in $E_{n+1} \subset E$. Thus we have an extension of F which is algebraically closed. □

We may now prove the principal result of this section.

Theorem 2.6 *Every field F has an algebraic closure.*

PROOF From the previous theorem, F has an extension E which is algebraically closed. Let $G = A(E/F)$, i.e., the collection of elements of E which are algebraic over F. Proposition 1.6 ensures us that G is a subfield of E. Let us take $f \in G[X]$ nonconstant. As $f \in E[X]$, f has a root $\alpha \in E$. As $f \in G[X]$, α is algebraic over G. Now, G is an algebraic extension of F and α is algebraic over G, therefore α is algebraic over F, by Proposition 1.7. It follows that $\alpha \in G$. We have shown that G is algebraically closed. □

Remark The previous proof shows that the field of algebraic numbers $A(\mathbf{C}/\mathbf{Q})$ is an algebraic closure of $\mathbf{Q}$. Moreover, the remark after Proposition 1.6 and Theorem 1.5 ensures that $A(\mathbf{C}/\mathbf{Q})$ is a countable infinite extension of $\mathbf{Q}$.

Exercise 2.4 *Show that $\mathbf{C}$ is an algebraic closure of $\mathbf{R}$.*

We have shown that a field always has an algebraic closure. Our next task is to show that any two such closures are isomorphic.

Lemma 2.4 *Let σ be a monomorphism from a field F into an algebraically closed field C. If E is an extension of F, $\alpha \in E$ algebraic over F, then σ can be extended to a monomorphism from $F(\alpha)$ into C.*

PROOF Let $F' = \sigma(F)$ and $f = m(\alpha, F)$. If f^* is the polynomial corresponding to f in $F'[X]$, then f^* has a root $\alpha' \in C$. Applying Proposition 2.3 we see that there is an isomorphism $\hat{\sigma}$ from $F(\alpha)$ onto $F'(\alpha')$. As $F'(\alpha') \subset C$ we have a monomorphism from $F(\alpha)$ into C extending σ. □

Theorem 2.7 *If $\sigma : F \longrightarrow C$ is a monomorphism, with C algebraically closed, and E an algebraic extension of F, then σ may be extended to a monomorphism $\hat{\sigma} : E \longrightarrow C$.*

PROOF Let G be the collection of all pairs (K, μ), where K/F, E/K and μ is a monomorphic extension of σ to K. (From the previous lemma, such pairs exist.) We now order these pairs: $(K_1, \mu_1) \leq (K_2, \mu_2)$ if and only if $K_1 \subset K_2$ and μ_2 restricted to K_1 is equal to μ_1. If the pairs (K_i, μ_i) form a chain Q, then Q has a maximum (K, μ), with $K = \cup K_i$ and $\mu(x) = \mu_i(x)$, if $x \in K_i$. From Zorn's lemma, G has a maximal element (K_0, μ_0). We claim that $K_0 = E$. If $K_0 \neq E$ and $\alpha \in E \setminus K_0$, then from the previous lemma, we may extend μ_0 to a monomorphism from $K_0(\alpha)$ into C. However, this contredicts the maximality of the pair (K_0, μ_0). Hence $K_0 = E$; This finishes the proof. □

If we add some conditions we obtain the important following corollary:

Corollary 2.3 *If, in the above theorem, E is algebraically closed and C algebraic over $\sigma(F)$, then $\hat{\sigma}$ is an isomorphism.*

PROOF We only need to show that $\hat{\sigma}(E) = C$. As C is algebraic over $\sigma(F)$, C is algebraic over $\hat{\sigma}(E)$, because $\sigma(F)$ is a subset of $\hat{\sigma}(E)$. Now, $\hat{\sigma}(E)$ is algebraically closed, because E is algebraically closed, hence C is an algebraic extension of the algebraically closed field $\hat{\sigma}(E)$. From Proposition 2.5 d., C cannot be a proper extension and so $\hat{\sigma}(E) = C$. □

We can now prove that the following theorem holds:

Theorem 2.8 *If C_1 and C_2 are algebraic closures of the field F, then C_1 and C_2 are F-isomorphic.*

PROOF F is a subfield of C_1 and C_2. If $\sigma : F \longrightarrow C_2$ is the inclusion mapping, then, from the previous corollary, we may extend σ to an isomorphism $\hat{\sigma} : C_1 \longrightarrow C_2$. This clearly fixes F. □

Exercise 2.5 *Let F be any field. Show that there is an infinite number of irreducible elements in the polynomial ring $F[X]$. Deduce that if F is algebraically closed, then F is infinite.*

Chapter 3

Separability

In this chapter we aim to look at two related topics, namely separable polynomials and separable extensions. We will begin with the first subject.

3.1 Separable polynomials

Let $f \in F[X]$ be nonconstant with the factorization into irreducible elements

$$f(X) = \lambda g_1(X) \cdots g_n(X).$$

If each g_i has no multiple root in a splitting field, then we say that f is *separable.* We will say that a polynomial is *strongly separable*, if it has no multiple roots. Clearly, a strongly separable polynomial is separable, but a separable polynomial is not necessarily strongly separable. For example, $f(X) = (X^2 + 1)^2 \in \mathbf{Q}[X]$ is separable, but not strongly separable. However, for an irreducible polynomial these notions are equivalent: If $f \in F[X]$ is irreducible, then f is separable if and only if f is strongly separable.

Proposition 2.4 is useful in determining whether a polynomial is separable or not. Consider a polynomial $f \in F[X]$. If $\gcd(f, f') = 1$, then f has no multiple root and so this is the case for any factor; it follows that f is strongly separable and hence separable. On the other hand, if $\gcd(f, f') \neq 1$, then f is not strongly separable; however, f may be separable or not. We must consider the irreducible factors of f.

Corollary 3.1 *If the characteristic of the field F is 0, then every polynomial $f \in F[X]$ is separable.*

PROOF Let g be an irreducible factor of f. As the characteristic of F is 0, $g' \neq 0$. If $h = \gcd(g, g')$, then $\deg h < \deg g$, because $\deg g' < \deg g$. As g is irreducible, $h = 1$. From the preceding proposition, g has no multiple root. □

Now we consider finite fields. If F is such a field, then its characteristic is a prime number p. Let $f \in F[X]$. If, for every irreducible factor g of f, $g' \neq 0$, then, using the argument of the corollary we have just proved, f is separable. We claim that this is always the case. Suppose that this is not the case and let g be an irreducible factor of f with $g' = 0$. Then $g \in F[X^p]$. The mapping

$$\phi : F \longrightarrow F : x \longmapsto x^p$$

is a homomorphism: $\phi(1) = 1$ and

$$\begin{array}{rclclclclcl}\phi(xy) & = & (xy)^p & = & x^p y^p & = & \phi(x)\phi(y) & & & & \\ \phi(x+y) & = & (x+y)^p & = & \displaystyle\sum_{i=0}^{p} \binom{p}{i} x^i y^{p-i} & = & x^p + y^p & = & \phi(x) + \phi(y). & &\end{array}$$

(We have used the fact that p divides $\binom{p}{i}$ if $1 \leq i \leq p-1$.) As F is a field and $\operatorname{Ker}\phi$ is an ideal $\operatorname{Ker}\phi = \{0\}$ or $\operatorname{Ker}\phi = F$. As $\phi(1) = 1$, the second alternative is not possible, so $\operatorname{Ker}\phi = \{0\}$, which implies that ϕ is injective. Given that F is finite, ϕ must also be surjective. Now let us return to g. We may write $g(X) = \sum_{i=0}^{k} a_i X^{pi}$. As ϕ is bijective, for each a_i, there exists b_i such that $a_i = b_i^p$. We have

$$g(X) = \sum_{i=0}^{k} b_i^p X^{ip} = \left(\sum_{i=0}^{k} b_i X^i \right)^p ,$$

a contradiction to the irreducibility of g. Hence $g' \neq 0$ and we have proven

Proposition 3.1 *If F is a finite field, then every polynomial $f \in F[X]$ is separable.*

Remark Corollary 3.1 and Proposition 3.1 imply that if char $F = 0$ or F is finite, then an irreducible polynomial $f \in F[X]$ is strongly separable.

Although polynomials which are not separable are relatively rare, such polynomials exist. Here we will give an example. We recall Eisenstein's criterion:

Let R be a unique factorization domain, with quotient field F, and $f(X) = \sum_{i=0}^{n} a_i X^i \in R[X]$, with $\deg f \geq 1$. If q is prime in R and q divides a_i, for $0 \leq i < n$, q does not divide a_n and q^2 does not divide a_0, then f is irreducible in $R[X]$.

Consider $\mathbf{F}_p(t)$, the field of rational fractions over the field $\mathbf{F}_p$, for any given prime p. The characteristic of $\mathbf{F}_p(t)$ is p. We note $f(X) = X^p - t \in \mathbf{F}_p[t][X]$. If $q(t)$ is prime in $\mathbf{F}_p[t]$, then $\deg q^2 \geq 2$ and so q^2 does not divide t; it follows from Eisenstein's criterion that f is irreducible. We claim that f has a multiple root in a splitting field. Let α be a root of f in a splitting field and suppose that

$$f(X) = (X - \alpha)^m g(X),$$

where $\deg g \geq 1$ and $g(\alpha) \neq 0$. Then

$$0 = f'(X) = m(X-\alpha)^{m-1} g(X) + (X-\alpha)^m g'(X).$$

This implies that $mg(X) = -(X-\alpha)g'(X)$ and so $mg(\alpha) = 0$. However, this is impossible, because $m < p$ and $g(\alpha) \neq 0$. Therefore, $f(X) = (X-\alpha)^p$ and f is not separable.

In Theorem 2.2 we showed that an isomorphism σ from the field F onto the field F' may be extended to an isomorphism $\tilde{\sigma} : E \longrightarrow E'$, where E is a splitting field of $f \in F[X]$ and E' a splitting field of f^*, the polynomial in $F'[X]$ corresponding to f. If f is separable, then we can say a little more.

Theorem 3.1 *If f is separable, then σ can be extended to E in exactly $[E : F]$ distinct ways.*

PROOF We prove this result by induction on $n = [E : F]$. First, if $n = 1$, then there is a unique extension of σ, namely $\tilde{\sigma} = \sigma$. Suppose now that $n > 1$ and that the result is true up to $n - 1$. The polynomial f has an irreducible factor g with $\deg g = d > 1$. We may write $f = gh$. Let α de a root of g. If $\tilde{\sigma}$ is an extension of σ, then $\alpha' = \tilde{\sigma}(\alpha)$ is a root of g^*, the polynomial in $F'[X]$ corresponding to g. As f is separable, so is f^*, which implies that g^* has d distinct roots α'. From Proposition 2.2 there are precisely d isomorphisms $\hat{\sigma} : F(\alpha) \longrightarrow F'(\alpha')$ extending σ, one for each root α'. Also, E is a splitting field of f over $F(\alpha)$ and E' a splitting field of f^* over $F'(\alpha')$ (for each α'). We have

$$[E : F] = [E : F(\alpha)][F(\alpha) : F].$$

Because g is irreducible, $[F(\alpha) : F] = d$, which imlies that $[E : F(\alpha)] = \frac{n}{d} < n$. Applying the induction hypothesis, we see that each $\hat{\sigma}$ has exactly $\frac{n}{d}$ from E onto E', hence we have precisely n extensions $\tilde{\sigma}$ of σ. □

We now turn to our second topic.

3.2 Separable extensions

If E is an extension of F and $\alpha \in E$, then α is a *separable element* over F, if α is algebraic over F and the minimal polynomial $m(\alpha, F)$ is separable. If every element $\alpha \in E$ is separable, then we say that E is a *separable extension* of F. From Corollary 3.1 and Proposition 3.1 we know that every algebraic extension of a field of characteristic 0 or of a finite field is separable.

We have seen in Theorem 2.7 that if $\sigma : F \longrightarrow C$ is a monomorphism, with C algebraically closed, and E an algebraic extension of F, then σ may be extended to a monomorphism $\hat{\sigma} : E \longrightarrow C$. If E is a finite separable extension of F then we can say a little more.

Theorem 3.2 *Let E be a finite separable extension of F, with $[E : F] = n$, and σ a monomorphism from F into C, which is algebraically closed. Then there are exactly n monomorphic extensions $\tilde{\sigma} : E \longrightarrow C$ of σ.*

PROOF We will prove this result by induction on n. If $n = 1$ then $E = F$ and there is nothing to prove. Suppose now that $n > 1$ and that the result is correct up to $n - 1$. Let $\alpha \in E \setminus F$, $m = m(\alpha, F)$ and m^* be the polynomial in $K[X]$ corresponding to m, where $K = \sigma(F)$. As m is separable, so is m^*. Given that C is algebraically closed, m^* has a root $\alpha' \in C$ and there is a unique isomorphism $\hat{\sigma} : F(\alpha) \longrightarrow K(\alpha')$ extending σ and such that $\hat{\sigma}(\alpha) = \alpha'$ (Proposition 2.3). If $\deg m = d$, then

$$[F(\alpha) : F] = d \Longrightarrow [E : F(\alpha)] = \frac{n}{d} < n.$$

Also $\deg m^* = d$, so m^* has d distinct roots in C, because it is separable. Thus we have d choices for α', and thus for $\hat{\sigma}$, and, by the induction hypothesis, each mapping $\hat{\sigma} : F(\alpha) \longrightarrow K(\alpha')$ can be extended to a monomorphism from E into C in $\frac{n}{d}$ ways. We thus obtain $\frac{n}{d}d = n$ monomorphisms $\tilde{\sigma}$ from E into C extending σ.

It is not difficult to see that there can be no more than n such extensions. If τ is such an extension, then $\alpha' = \tau(\alpha)$ is a root of m^* and τ restricted to $F(\alpha)$ is an isomorphism onto $F(\alpha')$. The mapping τ is then a monomorphic extension of this restriction and so is one of the mappings we have already considered. □

Corollary 3.2 *If E is a finite separable extension of F, with $[E : F] = n$, and C an algebraically closed extension of F, then there are exactly n F-monomorphisms of E into C.*

PROOF It is sufficient to take $\sigma = \mathrm{id}_F$ in the preceeding theorem. $\square$

Finite separable extensions have a useful property which Theorem 3.2 enables us to prove. We will also need an elementary result on finite fields, which is interesting in itself, namely that the multiplicative group of nonzero elements of a finite field is cyclic. We will prove a more general result. We recall that Euler's totient function ϕ is defined on $\mathbf{N}^*$ as follows: $\phi(n)$ is the number of elements in the set $\{d : 1 \leq d \leq n, (d,n) = 1\}$. We have the following identity $\sum_{d|n} \phi(d) = n$.

Theorem 3.3 *If F is a field and G a finite subgroup of the multiplicative group F^*, then G is cyclic.*

PROOF We set $|G| = n$. If $x \in G$, then $o(x)|n$, where $o(x)$ is the order of the element x. For each divisor d of n, let us write $\psi(d)$ for the number of elements in G whose order is d. If $\psi(d) \neq 0$, then there is an element $x \in G$ whose order is d. If $y \in H$, the group generated by x, then $y^d = 1$, hence y is a root of the polynomial $f(X) = -1 + X^d \in F[X]$. As f has at most d roots and H has d elements, all the roots of f are in H, in particular, any element of order d is in H. Also, the elements of order d in H are the generators of this group and there are $\phi(d)$ such generators, hence we have $\psi(d) = \phi(d)$. If $\psi(d) = 0$, for a certain divisor d of n, then we have

$$n = \sum_{d|n} \psi(d) < \sum_{d|n} \phi(d) = n,$$

a contradiction. It follows that $\psi(d) = \phi(d)$ for every divisor d of n. In particular, $\psi(n) = \phi(n) \geq 1$ and so G is cyclic. $\square$

Corollary 3.3 *If F is a finite field, then its group of nonzero elements is cyclic.*

We may now prove the interesting result we referred to above.

Theorem 3.4 *(primitive element theorem) If E is a finite separable extension of F, then there exists an element $\alpha \in E$, such that $E = F(\alpha)$.*

PROOF If F is finite, then so is E, being a finite extension. If α is a generator of the cyclic group E^*, then $E = F(\alpha)$.

Now let us consider the case where F is not finite. We will use an argument by induction on $[E : F] = n$. If $n = 1$, then $E = F$ and we can take any element $\alpha \in F$. Now let us suppose that $n > 1$ and that the result is true up to $n - 1$. We take $\alpha \in E \setminus F$. We claim that E is a separable extension of $F(\alpha)$. To see this, notice that, if $\gamma \in E$, then γ is algebraic over F, hence algebraic over $F(\alpha)$; in addition, $m(\gamma, F(\alpha)) \mid m(\gamma, F)$, thus, if $m(\gamma, F(\alpha))$ has a multiple root, then so does $m(\gamma, F)$, a contradiction. This proves the claim.

By hypothesis there is a $\beta \in E$ such that $E = F(\alpha, \beta)$. We will now show that there is an element $c \in F$ such that $E = F(\alpha + c\beta)$. From Corollary 3.2 we know that there are exactly n F-monomorphisms of E into an algebraic closure C of F. For any $c \in F$, each one of these mappings restricted to $F(\alpha + c\beta)$ is clearly an F-monomorphism into C. If $F(\alpha + c\beta) \neq E$, then $[F(\alpha + c\beta : F] < n$ and so there are distinct F-monomorphisms σ and τ of E into C which coincident on $F(\alpha + c\beta)$. We have

$$\sigma(\alpha) + c\sigma(\beta) = \tau(\alpha) + c\tau(\beta).$$

If $\sigma(\beta) = \tau(\beta)$, then also $\sigma(\alpha) = \tau(\alpha)$, which implies that $\sigma = \tau$, because $E = F(\alpha, \beta)$. This is a contradiction and so $\sigma(\beta) \neq \tau(\beta)$ and we can write

$$c = \frac{\sigma(\alpha) - \tau(\alpha)}{\tau(\beta) - \sigma(\beta)}.$$

However, a little reflexion shows that there is only a finite number of values c which can be expressed in this form; therefore we can find an element $c \in F$ such that $E = F(\alpha + c\beta)$, which finishes the proof. □

If E is an extension of F and $\alpha \in E$ is such that $E = F(\alpha)$, then we say that α is a *primitive element*, hence the name of the theorem which we have just proved. The primitive element theorem has an interesting application to quadratic number fields, namely

Theorem 3.5 *If E is a quadratic number field, then there is a square-free integer d such that $E = \mathbf{Q}(\sqrt{d})$.*

PROOF Let E be a quadratic number field, i.e., an extension of $\mathbf{Q}$ in $\mathbf{C}$ of degree 2. As this extension is finite and separable, there is a primitive element $\alpha \in E \setminus \mathbf{Q}$, with minimal polynomial

$$f(X) = a + bX + X^2$$

and $a, b \in \mathbf{Q}$. As α is a root of f, we have

$$\alpha = \frac{-b \pm \sqrt{b^2 - 4a}}{2} \Longrightarrow (2\alpha + b)^2 = b^2 - 4a \in \mathbf{Q}.$$

It is clear that $\beta = 2\alpha + b$ does not belong to $\mathbf{Q}$ and so $[\mathbf{Q}(\beta) : \mathbf{Q}] > 1$. As $[E : \mathbf{Q}] = 2$, we must have $E = \mathbf{Q}(\beta)$.

The number β may not be a square-free integer. If $b^2 - 4a = \frac{p}{q}$, then

$$q^2(b^2 - 4a) = p \Longrightarrow (q(2\alpha + b))^2 \in \mathbf{Z}.$$

Setting $\gamma = q(2\alpha + b)$, we have $E = \mathbf{Q}(\gamma)$ and $\gamma^2 \in \mathbf{Z}$. To finish it is sufficient to observe, as previously, that if $d = u^2 v$, where v is square-free, then $\mathbf{Q}(\sqrt{d}) = \mathbf{Q}(\sqrt{v})$. □

Here is another application of the primitive element theorem.

Theorem 3.6 *Let E be a finite separable extension of a field F of degree n. Then the field of fractions $E(X)$ is a finite extension of degree n of the field of fractions $F(X)$.*

PROOF From the primitive element theorem (Theorem 3.4), there exists $\alpha \in E$ such that

$$E = F(\alpha) = F_{n-1}[\alpha],$$

where $F_{n-1}[\alpha]$ is the set of polynomials of degree less than n in α with coefficients in F. We set $A = \{1, \alpha, \alpha^2, \ldots, \alpha^{n-1}\}$. This set is a basis of E over F. We will show that A is also a basis of $E(X)$ over $F(X)$. First we notice that $\mathcal{F}$, the collection of expressions of the form

$$\frac{c_0(X)}{d_0(X)} + \frac{c_1(X)}{d_1(X)}\alpha + \cdots + \frac{c_{n-1}(X)}{d_{n-1}(X)}\alpha^{n-1},$$

where $\frac{c_i(X)}{d_i(X)} \in F(X)$, is a subfield of $E(X)$. We now show that $E(X) \subset \mathcal{F}$. If $f \in E[X]$, then

$$f(X) = p_0(\alpha) + p_1(\alpha)X + \cdots + p_s(\alpha)X^s,$$

where $p_i(\alpha) \in F_{n-1}[\alpha]$, for $i = 0, 1 \ldots, s$. Regrouping terms having the same power of α, we obtain the expression

$$f(X) = u_0(X) + u_1(X)\alpha + \cdots + u_{n-1}(X)\alpha^{n-1},$$

where $u_j \in F[X]$, for all j. Hence any polynomial in $E[X]$ lies in $\mathcal{F}$. Now, if $f \in E[X]$ and $f \neq 0$, then there exists

$$g(X) = \frac{c_0(X)}{d_0(X)} + \frac{c_1(X)}{d_1(X)}\alpha + \cdots + \frac{c_{n-1}(X)}{d_{n-1}(X)}\alpha^{n-1} \in \mathcal{F},$$

such that $fg = 1$, because $\mathcal{F}$ is a field. As the inverse of f in $E(X)$ is unique, g is its inverse in $E(X)$. It now follows that $E(X) = \mathcal{F}$, because every element of $E(X)$ is the product of an element of $E[X]$ and the inverse of a nonzero element of $E[X]$. Hence A is a generating set of $E(X)$ over $F(X)$.

To finish we show that the elements of A form an independant subset of $E(X)$ over $F(X)$. Suppose that

$$\frac{c_0(X)}{d_0(X)} + \frac{c_1(X)}{d_1(X)}\alpha + \cdots + \frac{c_{n-1}(X)}{d_{n-1}(X)}\alpha^{n-1} = 0,$$

where $\frac{c_i(X)}{d_i(X)} \in F(X)$, for all i. Multiplying by the product $d_0(X)d_1(X)\cdots d_{n-1}(X)$ we obtain

$$\sum_{i=0}^{n-1} c_1(X) \left(\prod_{j\neq i} d_j(X) \right) \alpha^i = 0.$$

As the elements of A form an independant set over F, they form an independant set over $F[X]$. Because the products $\prod_{j\neq i} d_j(X)$ are nonzero, we have

$$c_0(X) = c_1(X) = \cdots = c_{n-1}(X) = 0,$$

and it follows that A is an independant set over $F(X)$. □

Exercise 3.1 *In the proof of Theorem 3.6 we stated that the independance of the set A over F implied its independance over $F[X]$. Why is this so?*

We have seen that an algebraic extension E of a field F may not be finite. However, in the case where E/F is separable and satisfies a certain condition, then this is the case.

Proposition 3.2 *Let F be a field and E a separable algebraic extension of F. Then E is a finite extension of F if there exists $n \in \mathbf{N}^*$ such that*

$$\sup_{\alpha \in E} [F(\alpha) : F] \leq n.$$

Moreover, $[E : F] \leq n$.

PROOF Let E be a separable algebraic extension of the field F such that

$$\sup_{\alpha \in E} [F(\alpha) : F] \leq n.$$

Let $r > n$ and $\alpha_1, \ldots, \alpha_r$ elements in E. Then $G = F(\alpha_1, \ldots, \alpha_r) \subset E$ is a finite extension of F. As the α_i are algebraic and separable, G is a separable extension of F (Theorem 3.8). From the primitive element theorem, there exists $\alpha \in G$ such that $G = F(\alpha)$. As $\alpha \in E$,

$$[G : F] = [F(\alpha) : F] \leq n.$$

However, $\alpha_1, \ldots, \alpha_r \in G$, so these elements form a dependant set. It follows that $[E : F] \leq n$. □

It may turn out that every polynomial over a given field is separable. In this case we say that the field is *perfect*. As we have seen, fields of characteristic 0 and finite fields are perfect. As an example of a non-perfect field, we may take the field $\mathbf{F}_p(t)$, discussed in the previous section. We will now give two criteria for a field to be perfect.

Proposition 3.3 *A field F is perfect if and only if every algebraic extension E of F is separable.*

PROOF Suppose first that the field F is perfect and that E is an algebraic extension of F. If $\alpha \in E$, then $m(\alpha, F) \in \mathbf{F}[X]$ and so this polynomial is separable. It follows that E is separable.

We now turn to the converse. We suppose that every algebraic extension E of F is separable. Let $f = \lambda g_1 \cdots g_n \in F[X]$, with $\lambda \in F$ and $g_i \in F[X]$ irreducible for all i. Let E be a finite (hence algebraic) extension of F containing the roots $\alpha_1, \ldots, \alpha_s$ of f. The roots of any g_i are roots of f. For a given root α_k of g_i we have $m(\alpha_k, F) | g_i$. As g_i is irreducible, we have $g_i = \lambda m(\alpha_k, F)$, for some $\lambda \in F$. However, the roots of $m(\alpha_k, F)$ are simple, hence those of g_i (the same) are also simple. Therefore f is separable. It follows that F is perfect. □

We now turn to our second criterion.

Proposition 3.4 *Let F be a field of characteristic $p > 0$. Then F is perfect if and only if, for every $a \in F$, there exists $b \in F$ such that $a = b^p$ (or, alternatively $F = F^p$).*

PROOF First let us suppose that for every $a \in F$ we can find $b \in F$ such that $a = b^p$. Let $f \in F[X]$ be irreducible. If $f(X) = a_0 + a_1 X^p + a_2 X^{2p} + \cdots + a_n X^{np}$, then

$$(b_0 + b_1 X + \cdots + X^n)^p = b_0^p + b_1^p X^p + \cdots + b_n^p X^{np} = a_0 + a_1 X^p + \cdots + a_n X^{np},$$

hence f is reducible, a contradiction. It follows that at least one nonzero monomial in f has a power which is not a multiple of p. This means that the derivative f' is nonzero and so f does not have a multiple root. It now follows that F is perfect.

Now the converse. Suppose that F is perfect and let $a \in F$. We set $f(X) = -a + X^p$ and let α be a root of f. Then $a = \alpha^p$ and $f(X) = (-\alpha + X)^p$. There is an $r \in \mathbf{N}^*$ such that $m(\alpha, F) = (-\alpha + X)^r$, because $m(\alpha, F) | f(X)$. As f is separable, $r = 1$ and so $\alpha \in F$. Thus we have found a $b \in F$, namely α, with $a = b^p$. □

3.3 Transitivity of separability

Before looking at the principle theme of this section we will prove a result which is often useful.

Proposition 3.5 *Let F, K and E be fields with K/F and E/K. If E is separable over F, then K is separable over F and E is separable over K.*

PROOF Suppose that the conditions on the fields F, K and E are satisfied. First, as K is a subfield of E, K is separable over F. We now show that E is separable over K. If $\alpha \in E$, then $m(\alpha, K)|m(\alpha, F)$. As $m(\alpha, F)$ has no multiple roots, $m(\alpha, K)$ also has no multiple roots, because $m(\alpha, F)$ has no multiple roots. Therefore E is separable over K. □

We have seen that we may define a partial order $\mathcal{R}$ on the collection of fields by $F\mathcal{R}E$ if E is an algebraic extension of F. In a similar way, we may define a partial order $\mathcal{R}'$ by $F\mathcal{R}'E$ if E is a finite separable extension of F. As before the relation $\mathcal{R}'$ is clearly reflexive and antisymetric, so we only need to prove the transitivity. Here however the proof is more difficult than in the former case. Clearly the difficulty arises only with infinite fields of characteristic $p > 0$. We will begin with some preliminary results.

Lemma 3.1 *Let f be a field of characteristic $p > 0$, E an algebraic extension of F and $\alpha \in E$. We set $m(X) = m(\alpha, F(\alpha^p))$. Then m splits in E and α is the unique root of m. If α is separable over $F(\alpha^p)$, then $\alpha \in F(\alpha^p)$.*

PROOF We set $f(X) = -\alpha^p + X^p \in F(\alpha^p)$. Then $f(\alpha) = 0$ and so $m|f$. Now, $f(X) = (-\alpha + X)^p$ and so $m(X) = (-\alpha + X)^r$, for some $r \geq 1$, thus m splits in E and has α as unique root.

If α is separable over $F(\alpha^p)$, then m is irreducible and so $m' \neq 0$. Therefore $m(X) = -\alpha + X$ and $\alpha \in F(\alpha^p)$. □

Lemma 3.2 *Let E be a finite extension of F, where F is of characteristic $p > 0$. We note $K = F(E^p)$, the subfield of E generated by F and the pth powers of elements of E. Then K is composed of all the linear combinations of elements of E^p with coefficients in F.*

PROOF Let $(\alpha_1, \ldots, \alpha_n)$ be a basis of E over F. It is clear that $F(\alpha_1^p, \ldots, \alpha_n^p) \subset K$ and, if $e \in E$, then

$$e = \lambda_1\alpha_1 + \cdots + \lambda_n\alpha_n \Longrightarrow e^p = \lambda_1^p\alpha_1^p + \cdots + \lambda_n^p\alpha_n^p \Longrightarrow K \subset F(\alpha_1^p, \ldots, \alpha_n^p).$$

Thus $K = F(\alpha_1^p, \ldots, \alpha_n^p)$.

As E is algebraic over F the elements of $F(\alpha_1^p)$ may be expressed as as polynomials in α_1^p with coefficients in F (see the proof of Proposition 1.4). Now, α_2^p is algebraic over F, hence over $F(\alpha_1^p)$. This means that every element of $F(\alpha_1^p, \alpha_2^p)$ may be expressed as a polynomial in α_2^p with coefficients in $F(\alpha_1^p)$. Simplifying such expressions, we see that every element of $F(\alpha_1^p, \alpha_2^p)$ may be expressed as a polynomial in α_1^p and α_2^p with coefficients in F. Continuing in the same way we find that every element of $F(\alpha_1^p, \ldots, \alpha_n^p)$ may be expressed as a polynomial in $\alpha_1^p, \ldots, \alpha_n^p$ with coefficients in F. This implies that the elements of $F(\alpha_1^p, \ldots, \alpha_n^p)$ are linear combinations of elements of E^p, with coefficients in F. Of course, linear combinations of elements of E^p belong to $F(\alpha_1^p, \ldots, \alpha_n^p)$ and the result follows. □

We now consider the case where $F(E^p)$ is not a proper subset of E, i.e., $E = F(E^p)$.

Lemma 3.3 *We suppose that E be a finite extension of F, where F is of characteristic $p > 0$ and that $E = F(E^p)$. If $(\alpha_1, \ldots, \alpha_n)$ is a basis of E over F, then so is $(\alpha_1^p, \ldots, \alpha_n^p)$.*

PROOF In the previous lemma we saw that all elements of $F(E^p)$ are linear combinations of pth powers of members of E. At the beginning of the proof we also saw that a pth power of a member of E can be expressed as a linear combination of pth powers of a basis, so it follows that $(\alpha_1^p, \ldots, \alpha_n^p)$ is a generating set of $F(E^p) = E$. As $[E : F] = n$, this set must also be a basis of E. □

The following proposition is interesting in its own right.

Proposition 3.6 *Let E be a finite extension of F, where F is of characteristic $p > 0$. Then E is a separable extension of F if and only if $E = F(E^p)$.*

PROOF We suppose first that E is a separable extension of F and take $\alpha \in E$. The minimal polynomial $m(\alpha, F)$ has no multiple roots and so this is the case for the minimal polynomial $m(\alpha, F(\alpha^p))$, because $m(\alpha, F(\alpha^p))|m(\alpha, F)$. Hence α is separable over $F(\alpha^p)$ and, from 3.1, $\alpha \in F(\alpha^p) \subset F(E^p)$. We have $E \subset F(E^p) \subset E$, which implies that $E = F(E^p)$.

We now turn to the converse. Suppose that $E = F(E^p)$. If E is not a separable extension of F, then we can find $\alpha \in E$ such that $m(X) = m(\alpha, F)$ is not separable. We have $m'(X) = 0$ and so $m(X) = m(X^p)$:

$$m(X) = b_0 + b_1 X^p + \cdots + b_{s-1} X^{(s-1)p} + X^{sp}.$$

As $m(\alpha) = 0$, the elements $1, \alpha^p, \ldots, \alpha^{sp}$ are dependant over F. However, $m(X)$ is a minimal polynomial, so the elements $1, \alpha^p, \ldots, \alpha^{sp-1}$ are independant over F. Also, $sp - 1 \geq 2s - 1 \geq s$, hence $1, \alpha, \ldots, \alpha^s$ are independant over F. If necessary we may add vectors to obtain the basis $(1, \alpha, \ldots, \alpha^s, u_1, \ldots, u_t)$ of E over F. From the previous lemma, we know that the pth powers of the elements of this basis form a basis and hence that $1, \alpha^p, \ldots, \alpha^{sp}$ form an independant set, a contradiction. Therefore m is separable and so E is a separable extension of F. □

We are now in a position to establish the transitivity of finite separable extensions.

Theorem 3.7 *Let F, K and E be fields, with K/F, E/K and $[E : F] < \infty$. If E is separable over K and K separable over F, then E is separable over F.*

PROOF From Corollary 3.1 and Proposition 3.1 it is sufficient to consider the case where F is infinite and has a characteristic $p > 0$. From the previous proposition $E = K(E^p)$ and $K = F(K^p)$. Hence

$$E = K(E^p) = F(K^p)(E^p) = F(K^p, E^p) = F(E^p),$$

because $K \subset E$. From the previous proposition again, E is separable over F. □

The result which we have just proved enables us to prove another, which seems quite natural.

Theorem 3.8 *Let E be an extension of F and $\alpha_1, \ldots, \alpha_n$ elements of E which are algebraic and separable over F. If $E = F(\alpha_1, \ldots, \alpha_n)$, then E is separable over F.*

PROOF We only have to consider the case where F is infinite and of characteristic $p > 0$. We note $E_i = F(\alpha_1, \ldots, \alpha_i)$. Thus $E_{i+1} = E_i(\alpha_i)$. We claim that $E_{i+1} = E_i(E^p_{i+1})$. To begin with

$$E_i, E_{i+1} \subset E_{i+1} \Longrightarrow E_i(E^p_{i+1}) \subset E_{i+1}.$$

To prove the equality we only need to show that $\alpha_{i+1} \in E_i(E^p_{i+1})$. Now, α_{i+1} is separable over F, hence over $E_i(\alpha^p_{i+1})$, because $m(\alpha_{i+1}, E_i(\alpha^p_{i+1}))|m(\alpha_{i+1}, F)$. From Lemma 3.1 $\alpha_{i+1} \in E_i(\alpha^p_{i+1})$ and so $E_{i+1} = E_i(E^p_{i+1})$.

Now we can complete the proof. From Proposition 3.6, for each i, E_{i+1} is separable over E_i. Applying successively Theorem 3.7 we obtain that E is separable over E_{n-2}, then that E is separable over E_{n-3} and so on. Finally we obtain that E is separable over F. □

Corollary 3.4 *If E is the splitting field of a separable polynomial $f \in F[X]$, then E is a separable extension of F.*

Chapter 4

Properties of finite fields

In the Chapter **??** we introduced finite fields and in Corollary 3.3 we showed that the multiplicative group of such fields is cyclic. We now examen more closely such fields.

Proposition 4.1 *If $\mathbf{F}_q$ is a finite field, with q elements, then the roots of the polynomial $A(X) = -X + X^q \in \mathbf{F}_q[X]$ are the elements of $\mathbf{F}_q$.*

PROOF From Corollary 3.3 we know that $\alpha^{q-1} = 1$, for all $\alpha \in \mathbf{F}_q$, which implies that $f(\alpha) = 0$. This is also the case for $\alpha = 0$, so the elements of $\mathbf{F}_q$ are all roots of A. Since A can have at most q roots, the elements of $\mathbf{F}_q$ form a complete set of roots of A. □

Determining subfields is not difficult.

Theorem 4.1 *Let $\mathbf{F}_q$ be a finite field, with $q = p^n$ elements, where p is a prime number and n a positive integer. Then a subfield of $\mathbf{F}_q$ has p^m elements, for some m dividing n. On the other hand, if m divides n, then there is a subfield of $\mathbf{F}_q$ with p^m elements, and this subfield is unique.*

PROOF Clearly a subfield K of $\mathbf{F}_q$ must have p^m elements, for some $m \leq n$. Let $[F_q : K] = s$ and $\mathcal{B} = \{b_1, \dots, b_s\}$ be a basis of $\mathbf{F}_q$ over K. The elements $x \in \mathbf{F}_q$ can be written $x = k_1 b_1 + \cdots + k_s b_s$, with $k_i \in K$. Since each k_i can take on p^m values, $\mathbf{F}_q$ must have exactly $(p^m)^s$ elements. Thus $ms = n$ and so m divides n.

Conversely, if m divides n, then $p^m - 1$ divides $p^n - 1$, so $f(X) = -1 + X^{p^m - 1}$ divides $g(X) = -1 + X^{p^n - 1}$ in $\mathbf{F}_q[X]$. Hence every root of $B(X) = -X + X^{p^m}$ is a root of $A(X) = -X + X^{p^n}$ and so belongs to $\mathbf{F}_q$. Considering B as a polynomial over the field $\mathbf{F}_{p^m}$, we see that $\mathbf{F}_q$ must contain a splitting field of B, which has order p^m, because B has p^m distinct roots.

If there were two distinct subfields of order p^m in $\mathbf{F}_q$, then the polynomial B, which has degree p^m, would have more than p^m roots in $\mathbf{F}_q$, which is impossible. Therefore, there is a unique subfield of $\mathbf{F}_q$ of order p^m, where m divides n, which considts precisely of the roots of B in $\mathbf{F}_q$. □

We now consider irreducible polynomials over finite fields. In the first result we use the primitive element theorem.

Proposition 4.2 *For any finite field $\mathbf{F}_q$ and positive integer n, there exists an irreducible polynomial $f \in \mathbf{F}_q[X]$ of degree n.*

PROOF There is a finite extension E of $\mathbf{F}_q$ with q^n elements and so $[E : \mathbf{F}_q] = n$. From the primitive element theorem, there exists $\alpha \in E$ such that $E = \mathbf{F}_q(\alpha)$. The minimal polynomial $m(\alpha, \mathbf{F}_q)$ has degree $[\mathbf{F}_q(\alpha) : F] = n$, because $E = F(\alpha)$. □

Remark Since there is only q possibilities for each coefficient, there can only be a finite number of polynomials, *a fortiori* of irreducible polynomials, of degree n over any $\mathbf{F}_q$.

To continue we need two preliminary results.

Lemma 4.1 *Let $q = p^n$ and $f \in \mathbf{F}_q[X]$ irreducible. If α is a root of f in an extension of $\mathbf{F}_q$ and $h \in \mathbf{F}_q[X]$, then $h(\alpha) = 0$ if and only if f divides h.*

PROOF It is sufficient to notice that the minimal polynomial of α is $a^{-1}f$, where a is the leading coefficient of f. □

Lemma 4.2 *Let $f \in \mathbf{F}_q[X]$ be irreducible of degree m. Then f divides $A(X) = -X + X^{q^n}$ if and only if m divides n.*

PROOF First suppose that f divides A. Let α be a root of f in a splitting of f over $\mathbf{F}_q$. Then $-\alpha + \alpha^{q^n} = 0$, so $\alpha \in \mathbf{F}_{q^n}$. Thus $\mathbf{F}_q(\alpha)$ is a subfield of $\mathbf{F}_{q^n}$. Since $[\mathbf{F}_q(\alpha) : \mathbf{F}_q] = m$, we have

$$n = [\mathbf{F}_{q^n} : \mathbf{F}_q(\alpha)][\mathbf{F}_q(\alpha) : \mathbf{F}_q] = [\mathbf{F}_{q^n} : \mathbf{F}_q(\alpha)]m \Longrightarrow m|n.$$

Conversely, suppose that m divides n. Suppose that $q = p^k$; then mk divides nk and so, by Theorem 4.2, $\mathbf{F}_{p^{nk}}$ contains $\mathbf{F}_{p^{mk}}$ as a subfield, i.e., $\mathbf{F}_{q^n}$ contains $\mathbf{F}_{q^m}$ as a subfield. Let α be a root of f in a splitting field of f over $\mathbf{F}_q$. Then $[\mathbf{F}_q(\alpha) : \mathbf{F}_q] = m$ and so we have

$$m = [\mathbf{F}_{q^m} : \mathbf{F}_q] = [\mathbf{F}_{q^m} : \mathbf{F}_q(\alpha)][\mathbf{F}_q(\alpha) : \mathbf{F}_q] = [\mathbf{F}_{q^m} : \mathbf{F}_q(\alpha)]m \Longrightarrow [\mathbf{F}_{q^m} : \mathbf{F}_q(\alpha)] = 1.$$

It follows that $\mathbf{F}_{q^m} = \mathbf{F}_q(\alpha)$ and so $\alpha \in \mathbf{F}_{q^m} \subset \mathbf{F}_{q^n}$. This implies that α is a root of $A(X) = -X + X^{p^n} \in \mathbf{F}_q[X]$. Therefore f divides A, by Lemma 4.1. □

Corollary 4.1 *Let E be an algebraic extension of a finite field $\mathbf{F}_q$. Then, for any element $\alpha \in E^*$, there exists a positive integer n such that $\alpha^n = 1$.*

PROOF Let $f = \min(\alpha, \mathbf{F}_q)$. If the degree of f is m, then, using Lemma 4.2 (with $m = n$), we obtain that f divides the polynomial $B(X) = -X + X^{q^m}$. Hence $-\alpha + \alpha^{q^m} = 0$. Multiplying by α^{-1}, we obtain $\alpha^{q^m - 1} = 1$. □

In the next result we show that the roots of an irreducible polynomial may be expressed as powers of a given root. This will enable us to find an explicit form of a splting field.

Theorem 4.2 *If $f \in \mathbf{F}_q[X]$ is of degree m, then f has a root α in $\mathbf{F}_{q^m}$. Moreover, all the roots of f are simple and are powers of α.*

PROOF Let α be a root of f in a splitting field of f over $\mathbf{F}_q$. A splitting field of f over $\mathbf{F}_q$ has the form $\mathbf{F}_{q^s}$, with $s \geq 1$, and $\mathbf{F}_q(\alpha) \subset \mathbf{F}_{q^s}$. If $\mathbf{F}_q(\alpha)$ strictly contains $\mathbf{F}_{q^m}$, then

$$m = [\mathbf{F}_q(\alpha) : \mathbf{F}_{q^m}][\mathbf{F}_{q^m} : \mathbf{F}_q] = [\mathbf{F}_q(\alpha) : \mathbf{F}_{q^m}]m > m,$$

a contradiction. Hence $\mathbf{F}_q(\alpha) \subset \mathbf{F}_{q^m}$, which implies that $\alpha \in \mathbf{F}_{q^m}$.

If β is a root of f in $\mathbf{F}_{q^s}$, then β^q is also a root: If $f(X) = \sum_{i=0}^m a_i X^i$, with $a_i \in \mathbf{F}_q$, then

$$\begin{aligned} f(\beta^q) &= a_0 + a_1\beta^q + \cdots + a_m\beta^{qm} \\ &= a_0^q + a_1^q\beta^q + \cdots + a_m^q\beta^{qm} \\ &= (a_0 + a_1\beta + \cdots + a_m\beta^m)^q \;=\; f(\beta)^q, \end{aligned}$$

so β^q is a root of f, as claimed. It follows that the elements $\alpha, \alpha^q, \ldots, \alpha^{q^{m-1}}$ are roots of f. These roots are distincts: Suppose, on the contrary, that $\alpha^{q^j} = \alpha^{q^k}$, with $0 \leq j < k \leq m-1$. Then, multiplying by α^{m-k}, we obtain

$$\alpha^{q^{m-k+j}} = \alpha^{q^m} = \alpha.$$

From Lemma 4.1, f divides the polynomial $A(X) = -X + X^{q^{m-k+j}}$. However, from Lemma 4.2, we have m divides $m-k+j$, which is impossible, because $0 < k-j \leq k-1$ implies that $0 < m-k+j < m$. Hence the m roots of f in $\mathbf{F}_{q^m}$ are $\alpha, \alpha^q, \ldots, \alpha^{q^{m-1}}$. □

Corollary 4.2 *If f is an irreducible polynomial in $\mathbf{F}_q[X]$ of degree m, then $\mathbf{F}_{q^m}$ is a splitting field of f over $\mathbf{F}_q$.*

PROOF In Theorem 4.2 we established that $\mathbf{F}_{q^m} = \mathbf{F}_q(\alpha)$, where α is a root of f in a splitting field of f over $\mathbf{F}_q$. However, $\mathbf{F}_q(\alpha) = \mathbf{F}_q(\alpha, \alpha^q, \ldots, \alpha^{q^{m-1}})$, which is a splitting field of f over $\mathbf{F}_q$. Therefore $\mathbf{F}_{q^m}$ is a splitting field of f over $\mathbf{F}_q$. □

Using Lemma 4.2 we may deduce a factorization of the polynomial $A[X] = -X + X^{q^n}$.

Theorem 4.3 *For a finite field $\mathbf{F}_q$ and $n \in \mathbf{N}^*$, the product of all the monic irreducible polynomials over F_q whose degree divides n is equal to $A[X] = -X + X^{q^n}$.*

PROOF From Lemma 4.2, the monic irreducible polynomials in $\mathbf{F}_q[X]$ which occur in the factorization of $A[X]$ are precisely those whose degree divides n. Since $A'(X) = -1 + q^n X^{q^n - 1} = -1$, A has no multiple roots in a splitting field over $\mathbf{F}_q$. Thus each monic irreducible polynomial occurring in the factorization of A occurs exactly once. □

Example The monic irreducible polynomials in $\mathbf{F}_2[X]$ are $f_1(X) = X$, $f_2(X) = 1 + X$ and $f_3(X) = 1 + X + X^2$. A simple calculation shows that the product of the f_i is $A(X) = -X + X^4$, which is not surprising, because $4 = 2^2$ and the divisors of 2 are 1 and 2.

Exercise 4.1 *Let $N_q(d)$ be the number of monic irreducible polynomials of degree d in $\mathbf{F}_q[X]$. Show that*

$$q^n = \sum_{d|n} d N_q(d).$$

Chapter 5

Normal extensions

In this short chapter we will consider another type of extension. Let E be an algebraic extension of F such that any irreducible polynomial $f \in F[X]$ having a root $\alpha \in E$ splits over E. In this case we say that E is a *normal extension* of F.

Proposition 5.1 *The algebraic extension E is normal over F if and only if, for each $\alpha \in E$, the minimal polynomial $m(\alpha, F)$ splits over E*

PROOF Let E be a normal extension of F and $\alpha \in E$. The polynomial $m = m(\alpha, F)$ is irreducible and has a root, namely α, in E. Therefore m splits over E.

Now let us suppose that E is an algebraic extension of F and that, for each $\alpha \in E$, the minimal polynomial $m(\alpha, F)$ splits over E. Let f be an irreducible polynomial in $F[X]$ and β a root of f in E. As $m = m(\beta, F)$ and f are irreducible and $m|f$, i.e., $f = cm$, where $c \in F$. As m splits over E, so does f. Thus E is a normal extension of F. □

Example The number field $\mathbf{Q}(\sqrt[3]{2})$ is not a normal extension of $\mathbf{Q}$. The minimal polynomial $m(\sqrt[3]{2}, \mathbf{Q}) = 2 - X^3$ and the complex roots of this polynomial do not belong to $\mathbf{Q}(\sqrt[3]{2})$.

We have other equivalent conditions particularly when E is a finite extension of F. We need a definition. If $\mathcal{F} = \{f_i\}_{i \in I}$ is a collection of polynomials in $F[X]$, E an extension of F such that E is generated by F and the roots of the f_i, then we say that E is a *splitting field* of $\mathcal{F}$.

Proposition 5.2 *The following conditions are equivalent for an algebraic extension E of F:*

- **a.** *E is a normal extension of F;*
- **b.** *E is the splitting field of a collection of polynomials in $F[X]$;*
- **c.** *If C is an algebraic closure of F, with E/F and C/E, and $\sigma : E \longrightarrow C$ is an F-monomorphism, then $\sigma(E) = E$.*

PROOF **a.** $\Longrightarrow$ **b.** Let $\mathcal{F} = \{m(\alpha, F) : \alpha \in E\}$ and A the family of roots of the polynomials in $\mathcal{F}$. If $\alpha \in E$, then $\alpha \in A$ and so $E \subset F(A)$, the subfield of E generated by F and A. To see that $F(A) \subset E$ it is sufficient to notice that $F \subset E$, because E is an extension of F and that $A \subset E$, because the extension E is normal. (If $\alpha \in E$, then all the roots of $m(\alpha, F)$ are in E).

b. $\Longrightarrow$ **c.** By hypothesis there is a collection of polynomials $\mathcal{F} \subset F[X]$ such that $E = F(A)$, where A is the family of roots of members of $\mathcal{F}$. Let C be an algebraic closure of F containing

E and $\sigma : E \longrightarrow C$ a monomorphism. We claim that $\sigma(A) = A$. Indeed, if $a \in A$, then a is a root of a polynomial $f \in \mathcal{F}$; this implies that $\sigma(a)$ is also a root of f. Thus $\sigma(A) \subset A$ and σ induces an injection from the set of roots of f into itself. As f has a finite number of roots, this injection is also a surjection and it follows that $\sigma(A) = A$. Then

$$\sigma(E) = \sigma(F(A)) = F(\sigma(A)) = F(A) = E.$$

c. $\Longrightarrow$ **a.** Suppose that the condition **c.** is satisfied and that the extension E is not normal. Then there exists an irreducible polynomial $f \in F[X]$ which has roots α and β, with $\alpha \in E$ and $\beta \in C \setminus E$. Let σ be the F-homomorphism of $F(\alpha)$ into C such that $\sigma(\alpha) = \beta$. σ is an F-monomorphism because $m(\alpha, F) = m(\beta, F)$. As E is an algebraic extension of $F(\alpha)$, from Theorem 2.7, σ may be extended to a monomorphism τ of E into C. However,

$$\tau(\alpha) = \sigma(\alpha) = \beta \notin E,$$

and so we have a contradiction to the condition **c.** It follows that **c.** $\Longrightarrow$ **a.** □

We have seen that there is a transitivity property for algebraic extensions and for finite separable extensions. However, such a property does not exist for normal extensions. It may be so that K is a normal extension of F and E a normal extension of K, without E being a normal extension of F. Here is an example. We set $F = \mathbf{Q}$, $K = F(\alpha)$, where α is the positive square root of 2 and $E = F(\beta)$, where β is the positive 4th root of 2. K is a splitting field of the polynomial $f(X) = -2 + X^2 \in F[X]$ and so K is a normal extension of F. Also, E is a splitting field of the polynomial $g(X) = -\alpha + X^2 \in K[X]$, so E is a normal extension of K. Let $h(X) = -2 + X^2 \in F[X]$. Then h has a root in E (in fact, two roots); however, the roots $\pm i\beta$ are not in E. Therefore, E is not a normal extension of F.

Although we do not have transitivity, we can say something when we have three fields related by inclusion.

Proposition 5.3 *Suppose that K/F and E/K, with E normal over F. Then E is normal over K.*

PROOF As E is normal over F, by Proposition 5.2 **a.** $\Longrightarrow$ **b.**, there is a collection of polynomials $\mathcal{F} \subset F[X]$ such that $E = F(A)$, where A is the family of roots of the polynomials in $\mathcal{F}$. Now, $F \subset K$ implies that $\mathcal{F} \subset K[X]$, hence, by Proposition 5.2 **b.** $\Longrightarrow$ **a.**, E is normal over K. □

For finite extensions we have a particularly simple characterization of normality:

Theorem 5.1 *The finite extension E of F is normal if and only if E is the splitting field of a polynomial $f \in F[X]$.*

PROOF Suppose that E is normal over F. Let $\alpha_1, \ldots, \alpha_n$ be a basis of E over F and $m_i = m(\alpha_i, F)$, for $i = 1, \ldots, n$. As $\alpha_i \in E$ and E is normal, m_i splits over E. It follows that $f = m_1 \cdots m_n$ splits over E. If K/F and E/K and f splits over K, then $\alpha_1, \ldots, \alpha_n \in K$. As the α_i form a basis of E, we must have $K = E$. Therefore E is a splitting field of f.

For the converse it is sufficient to apply Proposition 5.2 (**b.** $\Longrightarrow$ **a.**). □

Corollary 5.1 *A finite extension of a finite field is normal.*

PROOF Let F be a finite field and E a finite extension of F, with $[E : F] = n$. As F is finite we know that there is a prime number p and a positive integer k such that $|F| = p^k$. It follows that $|E| = p^{kn}$. Every element $a \in E$ is a root of the polynomial $f(X) = -X + X^{p^{kn}} \in F[X]$. As $\deg f = p^{kn}$, f splits in E. If K is a proper subfield of E, then f cannot split in K, because at least one element of E, i.e., a root of f, is missing. Therefore E is a splitting field of f and so, from Theorem 5.1, E is a normal extension of F. □

We finish this section with another criterion for an extension to be normal.

Proposition 5.4 *Let F be a field and $\alpha_1, \ldots, \alpha_n$ algebraic over F such that the roots of the minimal polynomials $m(\alpha_i, F)$ lie in $F(\alpha_1, \ldots, \alpha_n)$. Then the field $F(\alpha_1, \ldots, \alpha_n)$ is a normal extension of F.*

PROOF Let f be the highest common factor of the minimal polynomials $m(\alpha_i, F)$. Then $f \in F[X]$ and f divides the product of the minimal polynomials. Thus every root of f is a root of one of the minimal polynomials and so, by hypothesis, lies in $F(\alpha_1, \ldots, \alpha_n)$. It follows that $F(\alpha_1, \ldots, \alpha_n)$ contains a splitting field of f. However, for each i, α_i is a root of one of the factors of $m(\alpha_i, F)$ and so is a root of f. This means that each α_i must belong to a splitting field of f and so $F(\alpha_1, \ldots, \alpha_n)$ lies in such a field. We have shown that $F(\alpha_1, \ldots, \alpha_n)$ is a splitting field of f and so , by Theorem 5.1, is a normal extension of F. □

5.1 Normal closures

Let E be an algebraic extension of F and N an algebraic extension of E such that N is normal over F. If N is minimal with this property, i.e., there is no proper subfield of N with the same property, then we say that N is a *normal closure* of E over F.

Let E be finite extension of F. Then, from Proposition 1.3, E is algebraic over F and there exist $\alpha_1, \ldots, \alpha_n \in E$ such that $E = F(\alpha_1, \ldots, \alpha_n)$. We note $m_i(X) = m(\alpha_i, F)$ and $m(X) = m_1(X) \cdots m_n(X)$ and let N be a splitting field of m. N is a finite extension of F containing E. As N is a finite extension of E, N is algebraic over E. From Theorem 5.1, N is a normal extension of F. We claim that N is a normal closure of E over F. To see this, let K be a subfield of N containing E, which is also normal over F. From Proposition 5.1, each m_i splits over K, hence so does m. It follows that $K = N$ and so N is a normal closure of E over F. Therefore, at least in the case of finite extensions, normal closures exist. In fact, this is also true for transcendental extensions.

Lemma 5.1 *Let F be a field and E an algebraic extension of F. If $\{E_i\}_{i \in I}$ is a collection of subfields of E normal over F, then the intersection K of the E_i is normal over F.*

PROOF The intersection K is clearly a field. If $\alpha \in K$, then $\alpha \in E_i$, for each $i \in I$. This implies that the minimal polynomial $m(\alpha, F)$ splits over E_i, for each $i \in I$, and hence over K. It follows that K is normal over F. □

Theorem 5.2 *If E is an algebraic extension of F, then there is a normal closure of E over F.*

PROOF Let C be an algebraic closure of E. Then C is an algebraic extension of E, hence of F. C is also a normal over F. Thus the collection of normal extensions of F containing E is non-empty. Using the lemma, we see that the intersection N of all such extensions of F is normal and contains E and so is a normal closure of E over F. □

We will now see that normal closures are unique up to isomorphism.

Theorem 5.3 *If N and N' are normal closures of E over F, then N and N' are F-isomorphic.*

PROOF Let C be an algebraic closure of F and $\sigma : E \longrightarrow C$ a F-monomorphism. (From Theorem 2.7 such a monomorphism exists.) From Theorem 2.7 again, we can extend σ to a monomorphism τ (resp. τ') from N (resp. N') into C. Then $\tau(N)$ and $\tau'(N')$ are both normal closures of $\sigma(E)$ over $\sigma(F)$. From Lemma 5.1, $\tau(N) \cap \tau'(N')$ is normal over $\sigma(F)$ and contains $\sigma(E)$. By minimality, $\tau(N) = \tau(N) \cap \tau'(N') = \tau'(N')$. If we set $\phi = \tau' \circ \tau$, then ϕ is an isomorphism from N onto N'. □

Exercise 5.1 *Let E be finite separable extension of F and N a normal closure of E over F. Show that N is a finite separable extension of F.*

An extension E of F is a *Galois extension* if it is both separable and normal. In the case of fields of characteristic 0 or of finite fields such extensions are very common: the extension E only needs to be a splitting field of a polynomial in $F[X]$. From what we have seen, a finite extension of a finite field is a Galois extension.

Chapter 6

The Galois group

If E is an extension of F, then the collection of automorphisms of E fixing F, together with the composition of mappings $\circ$, form a group called the *Galois group* of the extension E of F. We note this group $Gal(E/F)$. We begin with some basic properties of this group.

Proposition 6.1 *If E is a finite extension of F, then the Galois group $Gal(E/F)$ is finite.*

PROOF Let $(\alpha_i)_{i=1}^n$ be a basis of E over F and let us note $m_i = m(\alpha_i, F)$. If $\sigma \in Gal(E/F)$, then, for any α_i, $\sigma(\alpha_i)$ is a root of m_i, hence there is a finite number of choices for $\sigma(\alpha_i)$. As σ is determined by the values of the $\sigma(\alpha_i)$ and those of F, which are left unchanged by σ, there is a finite number of automorphisms. $\square$

Let us look at some examples of Galois groups.

Example 1. $G = Gal(\mathbf{Q}(\sqrt{2}), \mathbf{Q})$. An element $\sigma \in G$ is determined by its value on $\sqrt{2}$. Since $\sqrt{2}$ is a root of the polynomial $f(X) = -2 + X^2$, so is $\sigma(\sqrt{2})$, which implies that $\sigma(\sqrt{2}) = \pm\sqrt{2}$. This leads to two distinct automorphisms, namely the identity and the automorphism τ defined by $\tau(a + b\sqrt{2}) = a - \sqrt{2}$, hence $G = \{\mathrm{id}_{\mathbf{Q}(\sqrt{2})}, \tau\} \simeq \mathbf{Z}_2$.

Example 2. $G = Gal(\mathbf{Q}(\sqrt[3]{2}), \mathbf{Q})$. An element $\sigma \in G$ is determined by its value on $\sqrt[3]{2}$. Since $\sqrt[3]{2}$ is a root of the polynomial $f(X) = -2 + X^3$, so is $\sigma(\sqrt[3]{2})$. However, $\sigma(\sqrt[3]{2}) \in \mathbf{Q}(\sqrt[3]{2}) \subset \mathbf{R}$, so $\sigma(\sqrt[3]{2}) = \sqrt[3]{2}$, which implies that σ is the identity. Thus $G = \{\mathrm{id}_{\mathbf{Q}(\sqrt[3]{2})}\}$.

It is interesting to notice that apparently similar extensions may have quite different Galois groups. It is quite easy to see that the Galois group of $\mathbf{C}$ over $\mathbf{R}$ has just two elements, namely the identity and complex conjugation and so is isomorphic to $\mathbf{Z}_2$. But what can we say of the Galois group of $\mathbf{R}$ over $\mathbf{Q}$.

Example 3. $G = Gal(\mathbf{R}/\mathbf{Q})$. Let $\sigma \in G$ and suppose that $a < b$. Then $b - a = y^2$, for some $y \neq 0$, and

$$\sigma(b) - \sigma(a) = \sigma(b - a) = \sigma(y^2) = \sigma(y)^2 > 0 \Longrightarrow \sigma(a) < \sigma(b).$$

If $\sigma \neq \mathrm{id}_{\mathbf{R}}$, then there exists x such that $\sigma(x) \neq x$. If $\sigma(x) > x$, then there exists a rational number r such that $x < r < \sigma(x)$. and $\sigma(x) < \sigma(r) < \sigma^2(x)$. However, $\sigma(r) = r$, because $r \in \mathbf{Q}$, so we have a contradiction, hence $\sigma(x) \not> x$. A similar argument shows that $\sigma(x) \not< x$ and it follows thar σ is the identity on R. Therefore $G = \{\mathrm{id}_{\mathbf{R}}\}$.

If the extension E of F is Galois, then we can be more precise.

Theorem 6.1 *If E is a finite Galois extension of F, then we have $|Gal(E/F)| = [E : F]$.*

PROOF As E is a finite normal extension of F, E is the splitting field of a polynomial $f \in F[X]$, which is a product of minimal polynomials (see Theorem 5.1 and its proof). However, the extension E is also separable, hence the minimal polynomials in the product are separable and it follows that E is a splitting field of a separable polynomial. Now applying Theorem 3.1 with $E' = E$, $F' = F$ and σ the identity, we obtain the result. □

Remark From Theorem 6.1, the extension $\mathbf{Q}(\sqrt[3]{2})$ is not Galois.

6.1 Fundamental theorem of Galois theory

In this section we consider the relation between extensions of a field F included in a given extension E and subgroups of the Galois group $Gal(E/F)$. We begin with two definitions. For H, a subgroup of $Gal(E/F)$, we write

$$\mathcal{F}(H) = \{x \in E : \sigma(x) = x,\ \forall \sigma \in H\}.$$

We often write E^H for $\mathcal{F}(H)$. It is easy to check that E^H is a field and that $F \subset \mathcal{F}(H) \subset E$. E^H is called the *fixed field* of H in E. For an intermediate field K, i.e., K/F and E/K, we set

$$\mathcal{G}(K) = Gal(E/K) = \{\sigma \in Gal(E/F) : \sigma(x) = x,\ \forall x \in K\}.$$

It is not difficult to show that $\mathcal{G}(K)$ is a subgroup of $Gal(E/F)$.

We will note $\mathbf{S}(Gal(E/F))$, or just $\mathbf{S}(G)$, the set of subgroups of $Gal(E/F)$ and $\mathbf{T}(E/F)$, or just $\mathbf{T}$, the set of intermediate fields between F and E. With inclusion both of these sets are partially ordered.

We recall that, if $(A, \leq_a)$ and $(B, \leq_b)$ are partially ordered sets and ϕ is a mapping from A into B such that, for $x, y \in A$,

$$x \leq_a y \Longrightarrow \phi(x) \leq_b \phi(y),$$

then ϕ is said to *order-preserving*. On the other-hand, if

$$x \leq_a y \Longrightarrow \phi(y) \leq_b \phi(x),$$

then ϕ is said to *order-reversing*. It is not difficult to see that the mappings $\mathcal{F}$ and $\mathcal{G}$ are order-reversing.

Theorem 6.2 *Suppose that E is a finite extension of F. Then E is Galois extension if and only if $\mathcal{F}(G) = F$, where $G = Gal(E/F)$.*

PROOF Let us first suppose that E is a Galois extension of F. We set $F_0 = \mathcal{F}(G)$. As $F \subset F_0$, every F_0-automorphism is an F-automorphism. If there is an F-automorphism σ which is not an F_0-automorphism, then we can find an element $y \in F_0 \setminus F$ such that $\sigma(y) \neq y$. However, by definition of F_0, this is not possible, and so every F-automorphism is an F_0-automorphism. As E is separable over F and F_0 is an intermediate field, E is separable over F_0 (Proposition 3.5). Therefore, using Theorem 6.1, we have

$$[E : F] = |Gal(E/F)| = |Gal(E/F_0)| = [E : F_0]$$

and it follows that $F_0 = F$.

We now turn to the converse. We suppose that $\mathcal{F}(G) = F$. From Proposition 6.1 we know that the Galois group $G = Gal(E/F)$ is finite. Let $G = \{\sigma_1, \ldots, \sigma_n\}$, with σ_1 the identité. We need to show that the extension E is both normal and separable. We will first show that it is normal. We consider an irreducible polynomial $f \in F[X]$ with a root α in E. Applying the automorphisms σ_i to α, we obtain r distinct images:

$$\alpha = \alpha_1 = \sigma_1(\alpha), \alpha_2 = \sigma_2(\alpha), \ldots, \alpha_r = \sigma_r(\alpha),$$

where we have supposed that the first r automorphisms give the distinct images. Let us write

$$e_1 = \sum_{i=1}^{r} \alpha_i, \; e_2 = \sum_{i<j} \alpha_i\alpha_j, \; e_3 = \sum_{i<j<k} \alpha_i\alpha_j\alpha_k, \ldots, \; e_r = \prod_{i=1}^{r} \alpha_i.$$

(These expressions are just the evaluations at $(\alpha_1, \ldots, \alpha_r)$ of the elementary polynomials in $E(X_1, \ldots, X_r)$.)

Any $\sigma \in G$ permutes the α_i and so, for each i, we have $\sigma(e_i) = e_i$. Therefore the e_i belong to $\mathcal{F}(G) = F$. We now consider the polynomial

$$g(X) = (-\alpha_1 + X) \cdots (-\alpha_r + X) = (-1)^r e_r + \cdots + e_2 X^{r-2} - e_1 X^{r-1} + X^r \in F[X].$$

We claim that $g = m(\alpha, F)$. Let $h(X) = \sum_{i=0}^{m} b_i X^i$, with $h(\alpha) = 0$. Then, for every i,

$$0 = \sigma_i(h(\alpha)) = h(\sigma_i(\alpha)) = h(\alpha_i).$$

As the roots of g are roots of h, g divides h and so $g = m(\alpha, F)$ as claimed.

We now return to the polynomial f. As f is irreducible and has α as a root, there is a constant $c \in F$ such that $f = cg$. As the $\alpha_i \in E$, g splits over E, and so does f. We have shown that E is a normal extension.

We now show that the extension E is also separable. We take $\alpha \in E$. The polynomial g which we defined above is the minimal polynomial $m(\alpha, F)$ and this has distinct roots. Hence α is a separable element and it follows that the extension E is separable over F. □

In the last result we saw that, in the case of a finite Galois extension, $\mathcal{F}(G) = F$. It is natural to ask whether there is a subgroup H of G such that $\mathcal{F}(H) = F$. In the next theorem, we will see that the answer is negative.

Theorem 6.3 *If E is a finite Galois extension of F and H a proper subgroup of the Galois group $G = Gal(E/F)$, then F is properly contained in $\mathcal{F}(H)$.*

PROOF We will give a proof by contradiction. Suppose that H is a proper subgroup of G and that $\mathcal{F}(H) = F$. As E is a finite separable extension of F we may apply the primitive element theorem (Theorem 3.3): there exists $\alpha \in E$ such that $E = F(\alpha)$. We define a polynomial $f \in E[X]$ by

$$f(X) = \prod_{\sigma \in H} (-\sigma(\alpha) + X).$$

For $\tau \in H$, we define the polynomial τf by applying τ to the coefficients of f. It is easy to see that

$$\tau f(X) = \prod_{\sigma \in H} (-\tau\sigma(\alpha) + X) = f(X).$$

Therefore the coefficients of F are fixed by τ, which implies that $f \in F[X]$, because $\mathcal{F}(H) = F$.
Now we notice that α is a root of f. (It is sufficient to take $\sigma = \mathrm{id}$). Thus

$$\deg f = |H| < |G| = [E : F] = [F(\alpha) : F] = \deg m(\alpha, F) \leq \deg f,$$

a contradiction. This establishes the result. $\square$

We now turn to the fundamental theorem of Galois theory. The theorem has three parts, which we will handle separately.

Theorem 6.4 *Let E be a finite Galois extension of a field F, with Galois group G. As above we write* $\mathbf{S}$ *the set of subgroups of G and* $\mathbf{T}$ *for the set of intermediate fields between F and E. Then the mappings $\mathcal{F} : \mathbf{S} \longrightarrow \mathbf{T}$ and $\mathcal{G} : \mathbf{T} \longrightarrow \mathbf{S}$ are bijections, each one being the inverse of the other.*

PROOF First, let us consider the mapping $\mathcal{GF}$. We take a subgroup H of G. Then

$$\sigma \in H \Longrightarrow \sigma(x) = x \; \forall x \in \mathcal{F}(H) \Longrightarrow \sigma \in Gal(E/\mathcal{F}(H)) = \mathcal{GF}(H).$$

Therefore $H \subset \mathcal{GF}(H)$. Suppose that we do not have equality. Using Propositions 3.5 and 5.3 we see that E is a finite Galois extension of $\mathcal{F}(H)$. As H is a proper subgroup of $\mathcal{GF}(H) = Gal(E/\mathcal{F}(H))$, from Theorem 6.3, with $\mathcal{F}(H)$ as F, then $\mathcal{F}(H)$ is properly contained in itself, a contradiction. It follows that we have $H = \mathcal{GF}(H)$.
We now consider the mapping $\mathcal{FG}$. Let K be a field intermediate between F and E. Using Propositions 3.5 and 5.3 we see that E is a finite Galois extension of K. Then, from Theorem 6.2, $\mathcal{F}(Gal(E/K)) = K$, i.e., $\mathcal{FG}(K) = K$. This finishes the proof. $\square$

Up to now we have seen that, in the case of finite Galois extensions, the mappings $\mathcal{F}$ and $\mathcal{G}$ are order-reversing bijections. We will now see that these mappings have other properties, namely they associate certain types of subgroups with particuler sorts of intermediate fields.

We need a definition. If K is a subfield of a field E and σ an automorphism of E, then $\sigma(K)$ is a subfield of E. Such a subfield is called a *conjugate subfield* of K.

Theorem 6.5 *Let E be a finite Galois extension of F and G the associated Galois group. If H is a subgroup of G, $\sigma \in G$ and $K = \mathcal{F}(H)$, then $\mathcal{F}(\sigma H \sigma^{-1}) = \sigma(K)$, i.e., $\mathcal{F}$ associates a conjugate subgroup to a corresponding conjugate subfield.*

PROOF We have

$$\begin{aligned}
\mathcal{F}(\sigma H \sigma^{-1}) &= \{x \in E : \sigma\tau\sigma^{-1}(x) = x \; \forall \tau \in H\} \\
&= \{x \in E : \tau(\sigma^{-1}(x)) = \sigma^{-1}(x) \; \forall \tau \in H\} \\
&= \{x \in E : \sigma^{-1}(x) \in \mathcal{F}(H)\} \;\; = \;\; \sigma(K).
\end{aligned}$$

This ends the proof. $\square$

We now consider normal subgroups of the Galois group. We notice first that, if K is an intermediate field, then E is always a normal extension of K (Proposition 5.3); however, K may not be a normal extension of F.

Theorem 6.6 *Suppose that E is a finite Galois extension of F and G the associated Galois group. Then K is a normal extension of F if and only if $H = Gal(E/K)$ is a normal subgroup of G. In this case the Galois group $Gal(K/F)$ is isomorphic to the quotient group G/H.*

In addition, for any subgroup H (not necessarily normal),

$$[K : F] = [G : H] \qquad \text{and} \qquad [E : K] = |H|.$$

PROOF Let K be an intermediate field which is a normal extension of F and C an algebraic closure of F, with C/E. (From Exercise 2.3 such an algebraic closure exists.) Suppose that σ is an F-monomorphism from K into E, thus into C. As K is separable over E, we may extend σ to an F-monomorphism $\tilde{\sigma} : E \longrightarrow C$ (Theorem 3.2). As E is a normal extension of F, from Proposition 5.2, $\tilde{\sigma}$ is an F-automorphism of E. Hence, every F-monomorphism σ of K into E is a restriction of an F-automorphism $\tilde{\sigma}$ of E. In addition, clearly every F-automorphism of E restricted to K is an F-monomorphism of K into E. Thus the F-monomorphisms from K into E are the restrictions to K of F-automorphisms of E, i.e., of elements of $\tau \in G$. As K is a normal extension of F, using Proposition 5.2 again, we see that τ is an F-automorphism of K. If $K = \mathcal{F}(H)$, then with Theorem 6.5 we have

$$\mathcal{F}(H) = K = \tau(K) = \mathcal{F}(\tau H \tau^{-1}) \Longrightarrow H = \tau H \tau^{-1},$$

and so H is a normal subgroup of G.

Now we suppose that H is a normal subgroup of G. For any $\sigma \in G$, we have $H = \sigma H \sigma^{-1}$. Then, for $K = \mathcal{F}(H)$,

$$\sigma(K) = \mathcal{F}(\sigma H \sigma^{-1}) = \mathcal{F}(H) = K.$$

Let $f \in F[X]$ be irreducible with a root $\alpha \in K$. Because $K \subset E$ and E is a normal extension of F, all the roots of f lie in E, so E contains a splitting field S of f, which is an extension of K. If α' is another root of f, then using Proposition 2.2 with $\sigma = \mathrm{id}$, we may find an F-isomorphism $\sigma : F(\alpha) \longrightarrow F(\alpha')$, which is such that $\sigma(\alpha) = \alpha'$. Now, applying Theorem 2.2, we can extend σ to an F-automorphism σ' of E'. We would like to extend σ' to an F-automorphism of E. We take an algebraic closure C of E', which is an extension of E. Then we may consider σ' as a monomorphism of E' into C, which we can extend to $\hat{\sigma} : E \longrightarrow C$. However, E is a normal extension of E', because E is such an extension of F and so, from Proposition 5.2, $\hat{\sigma}(E) = E$. Thus, $\hat{\sigma}$ is an F-automorphism of E, such that $\hat{\sigma}(\alpha) = \alpha'$. As $\hat{\sigma}(K) = K$ and $\alpha \in K$, $\alpha' \in K$. It follows that K is a normal extension of F.

We have proved the hardest part of the theorem. Now we turn to the remaining parts. First, we show that $Gal(K/F) \simeq G/H$, if $H \lhd G$. Consider the mapping

$$\phi : Gal(E/F) \longrightarrow Gal(K/F), \sigma \longmapsto \sigma_{|K}.$$

In the first part of the proof we saw that the elements of the Galois group $Gal(K/F)$ are the restrictions to K of the elements of the Galois group $Gal(E/F)$. Hence, the mapping ϕ is an epimorphism. Also,

$$\operatorname{Ker} \phi = \{\sigma \in Gal(E/F) : \sigma_{|K} = \mathrm{id}_{|K}\} = Gal(E/K) = H.$$

It follows that

$$Gal(E/F)/H \simeq Gal(K/F).$$

To conclude, we notice that

$$|G| = [E : F] = [E : K][K : F] = |H|[K : F] \Longrightarrow [K : F] = \frac{|G|}{|H|} = [G : H]$$

and

$$[E:K] = \frac{[E:F]}{[K:F]} = \frac{|G|}{|G|/|H|} = |H|.$$

This ends the proof □

Remark We may sum up the results of Theorem 6.6 in the following way. If H is a subgroup of the Galois group $G = Gal(E/F)$ and K the corresponding intermediate field between F and E ($K = \mathcal{F}(H)$), then

$$[E:K] = |H| = |Gal(E/K)|$$

and

$$[K:F] = [G:H].$$

If, in addition, H is a normal subgroup of G, then K is a normal extension of F and we may extend the second line to obtain

$$[K:F] = [G:H] = |G/H| = |Gal(K/F)|.$$

The Theorems 6.4, 6.5 and 6.6 which we have just proved are usually handled together under the name of the fundamental theorem of Galois theory. As two of the parts are rather long, it seems to us preferable to divide the theorem into parts.

We have seen that a finite extension E of a field F gives rise to a finite group of automorphisms of E, namely the Galois group $Gal(E/F)$. Suppose now that we have a finite group of automorphisms G of a field E. It is natural to ask whether there exists a subfield F of E such that G is the Galois group $Gal(E/F)$. This is in fact the case as we will now see.

Let E be a field and G a finite subgroup of the group of automorphisms of E. We suppose that $|G| = n$ and set

$$F = E^G = \{x \in E : g(x) = x, \ \forall g \in G\}.$$

F is clearly a subfield of E; it is called the *fixed field of G in E*.

Theorem 6.7 *(Artin) The field E is a finite Galois extension of F and*

$$Gal(E/F) = G.$$

PROOF We define an action Φ of the group G on E :

$$\Phi : G \times E \longrightarrow E, (g, x) \longmapsto g(x).$$

Let us take $\alpha \in E$ and note O_α the orbit of α:

$$O_\alpha = \{g(\alpha) : g \in G\} = \{\alpha_1, \ldots, \alpha_s\},$$

with $\alpha_1 = \alpha$ and $s \leq n$. We set

$$f(X) = \prod_{k=1}^{s}(-\alpha_k + X).$$

An element of G permutes the α_i; given that the coefficients of the polynomial f are symmetric polynomials in the α_i, these coefficients are fixed by G and so $f \in F[X]$. Hence every element $\alpha \in E$ is the root of a $f \in F[X]$, with $\deg f \leq n$. As the roots of f are distinct, E is a separable extension of F. From Proposition 3.2, E is a finite extension of F and $[E:F] \leq n$.

We need to show that E is a normal extension of F. From the primitive element theorem, there exists $\alpha \in E$ such that $E = F(\alpha)$. As the roots of the minimal polynomial $m(\alpha, F)$ lie in the orbit of α, which is contained in E, E is a splitting field of $m(\alpha, F)$; it follows from Theorem 5.1 that E is a normal extension of F. We have shown that E is a Galois extension of F.

To conclude, we show that G is the Galois group $Gal(E/F)$. By definition of F, every element of G fixes the elements of F, so $G \subset Gal(E/F)$. In addition, from Theorem 6.1, we know that $|Gal(E/F)| = [E : F] \leq n$, hence

$$n = |G| \leq |Gal(E/F)| \leq n$$

and it follows that

$$G = Gal(E/F).$$

This ends the proof. □

The theorem which we have just proved has an interesting application. We recall a definition. If F is a field and $F[X_1, \ldots, X_n]$ is the ring of polynomials in n variables with coefficients in F, then we write $F(X_1, \ldots, X_n)$ for the field of fractions of $F[X_1, \ldots, X_n]$. This field is called the *field of rational functions* in n variables over F. The rational fractions of the symmetric polynomials form a subfield of $F(X_1, \ldots, X_n)$, which we will note $F_S(X_1, \ldots, X_n)$. We are interested in finding the degree of the extension $F(X_1, \ldots, X_n)/F_S(X_1, \ldots, X_n)$ and its Galois group.

If $\sigma \in S_n$, then the mapping defined by $X_i \longmapsto X_{\sigma(i)}$ induces an automorphism $\bar{\sigma}$ of the field $F(X_1, \ldots, X_n)$. The mapping $\sigma \longmapsto \bar{\sigma}$ is a group monomorphism, so S_n may be considered to be a subgroup of the group of automorphisms of $F(X_1, \ldots, X_n)$. The fixed field of S_n is clearly $F_S(X_1, \ldots, X_n)$. From Artin's theorem (Theorem 6.7) we deduce that $F(X_1, \ldots, X_n)$ is a finite Galois extension of $F_S(X_1, \ldots, X_n)$, with Galois group S_n. It folows that the dimension of $F(X_1, \ldots, X_n)$ over $F_S(X_1, \ldots, X_n)$ is $n!$.

Conjugates in Galois extensions

If E is a finite field extension of a field F and $\alpha \in E$, then we say that any root of the minimal polynomial $m(\alpha, F)$ is an (F-)conjugate of α. It is clear that, for all $\sigma \in Gal(E/F)$, $\sigma(\alpha)$ is an F-conjugate of α. However, in general, not all conjugates of α are of this form. For example, the $\mathbf{Q}$-conjugates of $\sqrt[3]{2}$ are $\sqrt[3]{2}$, $j\sqrt[3]{2}$ and $j^2\sqrt[3]{2}$, where j is a primitive 3rd root of unity. If $\sigma \in Gal(\mathbf{Q}(\sqrt[3]{2}), \mathbf{Q})$, then Im $(\sigma) \subset \mathbf{R}$, so there is no $\sigma \in Gal(\mathbf{Q}(\sqrt[3]{2}), \mathbf{Q})$ such that $\sigma(\sqrt[3]{2}) = j\sqrt[3]{2}$. The following result ensures that, if E/F is a finite normal extension, then all F-conjugates of an element $\alpha \in E$ are images of α by an element in the Galois group.

Proposition 6.2 *If E is a finite normal extension of F and $\alpha \in E$ then the set*

$$A = \{\sigma(\alpha) : \sigma \in Gal(E/F)\}$$

is the set of conjugates of α.

PROOF If β is a conjugate of α, then, from Proposition 2.3, there is an F-isomorphism $\phi : F(\alpha) \longrightarrow F(\beta)$ such that $\phi(\alpha) = \beta$, since $m(\alpha, F) \in F[X]$ is irreducible. Both $F(\alpha)$ and $F(\beta)$ are subfields of E. (As E is a normal extension of F, we may suppose that all the conjugates of α lie in E.) From Theorem 5.1 there exists a polynomial $g \in F[X]$ whose splitting field is E. Now, $g \in F(\alpha)[X]$ and, in the notation of Theorem 2.2, with $\phi = \sigma$, we have $g^* = g$. It follows that there exists $\sigma' \in Gal(E/F)$ such that $\sigma'(\alpha) = \beta$. □

We have shown, at least in the case where E is a normal extension of F, that the set of conjugates of the element $\alpha \in F$ is composed of elements of the form $\sigma(\alpha)$, where $\sigma \in Gal(E/F)$. However, it may be so that there are members $\sigma, \tau \in Gal(E/F)$ such that $\sigma(\alpha) = \tau(\alpha)$. We are interested in knowing the number of automorphisms $\sigma \in Gal(E/F)$ which give us the same conjugate.

Proposition 6.3 *Let E be a finite Galois extension of F, $\alpha \in E$ and β a conjugate of $\alpha \in L$. Then the number of $\sigma \in Gal(E/F)$ such that $\sigma(\alpha) = \beta$ is equal to the dimension $[E : F(\alpha)]$.*

PROOF Let β be a conjugate of α. There exists $\sigma' \in Gal(E/F)$ such that $\sigma'(\alpha) = \beta$. We have

$$\begin{aligned} \{\sigma \in Gal(E/F) : \sigma(\alpha) = \beta\} &= \{\sigma \in Gal(E/F) : \sigma(\alpha) = \sigma'(\alpha)\} \\ &= \{\sigma \in Gal(E/F) : \sigma'^{-1}\sigma(\alpha) = \alpha\}. \end{aligned}$$

Thus we have a bijection between the automorphisms $\sigma \in Gal(E/F)$ such that $\sigma(\alpha) = \beta$ and the automorphisms $\sigma \in Gal(E/F)$ such that $\sigma(\alpha) = \alpha$. However, $\sigma \in Gal(E/F)$ fixes α if and only if $\sigma \in Gal(E/F(\alpha))$. From Theorem 6.6 we have

$$|Gal(E/F(\alpha))| = [E : E^{Gal(E/F(\alpha))}],$$

where $E^{Gal(E/F(\alpha))}$ is the fixed field of $Gal(E/F(\alpha))$. Moreover, by Propositions 3.5 and 5.3 E is a Galois extension of $F(\alpha)$. Using Theorem 6.2 we obtain

$$E^{Gal(E/F(\alpha))} = F(\alpha)$$

and so

$$[E : E^{Gal(E/F(\alpha))}] = [E : F(\alpha)].$$

This ends the proof. □

Remark If E is a Galois extension of F and the conjugates of an element $\alpha \in E$ are distinct, then it is natural to ask whether these elements form a basis of E over F. (If E is a Galois extension of F, then $|Gal(E/F)| = [E : F]$.) This is not in general the case. However, the normal basis theorem ensures that for some $\alpha \in E$ this is the case. (For a proof, see for example [23]).

6.2 Composita

In this section we will be primarily interested in intersections of subgroups of the Galois group. We begin with a definition. If K and L are subfields of a field E, then the intersection of all subfields of E containing these fields, which we note KL, is called the *compositum* of K and L. Clearly KL is the smallest subfield of E containing K and L. Of course we may easily generalize this definition to more than two subfields, even to an infinite number of subfields.

The subset R of E defined by

$$R = \big\{ \sum_{i \in I} k_i l_i : k_i \in K, l_i \in L, |I| < \infty \big\}$$

is the smallest subring of E containing both K and L. The ring of fractions of R is the compositum KL in E.

Theorem 6.8 *Let K and L be extensions of F in E, where K is a finite Galois extension of F. Then*

- **a.** *KL is a finite Galois extension of L;*
- **b.** *If $\sigma \in Gal(KL/L)$, then the restriction of σ to K belongs to $Gal(K/F)$ and the mapping*

  $$\phi : Gal(KL/L) \longrightarrow Gal(K/F), \sigma \longmapsto \sigma_{|K}$$

  is a monomorphism;
- **c.** *K is a Galois extension of $K \cap L$ and the image of ϕ is $Gal(K/K \cap L)$; ϕ is an isomorphism if and only if $K \cap L = F$.*

PROOF **a.** From the primitive element theorem there is an element $\alpha \in K$ such that $K = F(\alpha)$, hence

$$KL = LF(\alpha) = L(\alpha).$$

As α is algebraic over F, therefore over L, $L(\alpha)$ is a finite extension of L. As K is a separable extension of F, α is separable over F, hence over L, and it follows that $L(\alpha)$ is separable over L. We have shown that KL is separable over L.

We now need to show that KL is a normal extension of L. Let $f = m(\alpha, F)$ and $g = m(\alpha, L)$. Then $g|f$. As f has a root $\alpha \in K$ and K is a normal extension of F, all the roots of f are in K. It follows that all the roots of g are in $K \subset KL = L(\alpha)$ and so $L(\alpha)$ is a splitting field of g. Thus KL is a normal extension of L.

b. Let $\sigma \in Gal(KL/L)$. We need to show that $\sigma(K) = K$ and $\sigma_{|K}$ fixes F. For any $\alpha \in K$, $\sigma(\alpha)$ is a root of the minimal polynomial $m(\alpha, F)$. As K is a normal extension of F, $\sigma(\alpha) \in K$. Thus $\sigma(K) \subset K$. In the same way, $\sigma^{-1}(K) \subset K$ and so $\sigma(K) = K$. In addition, the fact that $F \subset L$ implies that σ fixes F and so $\sigma_{|K}$ fixes F. Therefore $\sigma_{|K} \in Gal(K/F)$. If $\tau \in Gal(KL/L)$ and $\alpha \in K$, then

$$(\sigma \circ \tau)_{|K}(\alpha) = (\sigma \circ \tau)(\alpha) = \sigma(\tau(\alpha)) = \sigma_{|K} \circ \tau_{|K}(\alpha),$$

therefore ϕ is a homomorphism.

We now need to show that ϕ is injective. If $\sigma_{|K}$ fixes each element of K, then σ fixes each element of K and each element of L and so fixes each element of KL. This establishes the injectivity of ϕ. Hence ϕ is a monomorphism.

c. First we show that K is a Galois extension of $K \cap L$. As $F \subset K \cap L \subset K$ and K is a Galois extension of F, from Propositions 3.5 and 5.3, K is a Galois extension of $K \cap L$.

We set $A = \operatorname{Im}\phi$. A is a subgroup of the Galois group $Gal(K/F)$, thus, by Theorem 6.4, $A = Gal(K/K^A)$. Moreover,

$$K^A = \{x \in K : \sigma(x) = x \ \forall \sigma \in Gal(KL/L)\},$$

since the elements of A are restrictions of elements of $Gal(KL/L)$ to K. Theorem 6.2 ensures that any element of KL fixed by all elements of $Gal(KL/L)$ lies in L. Hence

$$K^A = K \cap L$$

and $A = Gal(K/K \cap L)$, i.e. $\operatorname{Im}\phi = Gal(K/K \cap L)$, as claimed.

Now, ϕ is an isomorphism if and only if $Gal(K/K \cap L) = Gal(K/F)$. However, Theorem 6.2 ensures that $K^{Gal(K/K \cap L)} = K \cap L$ and $K^{Gal(K/F)} = F$. Finally, ϕ is an isomorphism if and only if $K \cap L = F$. This finishes the proof. □

The theorem we have just proved has an interesting corollary linking the degrees of the extensions over F.

Corollary 6.1 *Under the conditions of Theorem 6.8 , we have*

$$[KL : F] = \frac{[K : F][L : F]}{[K \cap L : F]}.$$

PROOF We have

$$[KL : F] = [KL : L][L : F] \Longrightarrow \frac{[KL : F]}{[L : F]} = [KL : L]$$

and

$$[K : F] = [K : K \cap L][K \cap L : F] \Longrightarrow \frac{[K : F]}{[K \cap L : F]} = [K : K \cap L].$$

From the previous theorem, KL is a Galois extension of L and there is no difficulty in seeing that this is also the case for K over $K \cap L$. Hence,

$$[KL : L] = |Gal(KL/L)| = |Gal(K/K \cap L)| = [K : K \cap L].$$

The second equality holds, because in the proof of Theorem 6.8 we showed that the Galois groups $Gal(KL/L)$ and $Gal(K/K \cap L)$ are isomorphic. The result now follows. □

Exercise 6.1 *Show that* $[KL : L]$ *divides* $[K : F]$.

We may now consider the image under $\mathcal{F}$ of the intersection of two subgroups of the Galois group and of the group generated by two subgroups.

Theorem 6.9 *Let E be a finite Galois extension of F and H_1, H_2 subgroups of the Galois group $G = Gal(E/F)$. We note $K_1 = \mathcal{F}(H_1)$ and $K_2 = \mathcal{F}(H_2)$. Then $\mathcal{F}(H_1 \cap H_2) = K_1K_2$ and, if H is the subgroup generated by $H_1 \cup H_2$, then $\mathcal{F}(H) = K_1 \cap K_2$.*

PROOF If σ fixes each element of K_1K_2, then σ fixes each element of K_1 and each element of K_2, hence $\sigma \in H_1 \cap H_2$. On the other hand, suppose that $\sigma \in H_1 \cap H_2$. Then σ restricted to K_1 or to K_2 is the identity mapping. Therefore a polynomial in elements of K_1 and K_2 is fixed by σ and, more generally, K_1K_2 is fixed by σ. Thus

$$H_1 \cap H_2 = \mathcal{G}(K_1K_2) \Longrightarrow \mathcal{F}(H_1 \cap H_2) = K_1K_2.$$

If $\sigma \in H_1 \cup H_2$, then σ fixes K_1 or σ fixes K_2. As $K_1 \cap K_2 \subset K_1$, and $K_1 \cap K_2 \subset K_2$, σ fixes $K_1 \cap K_2$. Hence $H \subset \mathcal{G}(K_1 \cap K_2)$. If $H \neq \mathcal{G}(K_1 \cap K_2)$, then $K_1 \cap K_2$ is properly contained in $\mathcal{F}(H)$, hence there exists $x \in \mathcal{F}(H) \setminus K_1 \cap K_2$. If $x \notin K_1$, then we can find $\sigma \in H_1 \subset H$ such that $\sigma(x) \neq x$, hence $x \notin \mathcal{F}(H)$, a contradiction. We have the same situation if $x \notin K_2$ and so $H = \mathcal{G}(K_1 \cap K_2)$, which implies that $\mathcal{F}(H) = K_1 \cap K_2$. □

Remark There is no difficulty in extending the above result to n subgroups and n subfields for any $n > 2$.

We now return briefly to Corollary 6.1. It is easy to deduce that

$$[KL : F] \leq [K : F][L : F].$$

However, we do not need the condition on K.

Proposition 6.4 *Let E be a finite extension of F. In addition, let K and L be extensions of F in E. Then*

$$[KL : F] \leq [K : F][L : F],$$

with equality if $[K : F]$ and $[L : F]$ are coprime.

PROOF Let $(\alpha_i)_{i=1}^m$ and $(\beta_j)_{j=1}^n$ be respective bases of K over F and L over F. Then

$$K = F(\alpha_1, \dots, \alpha_m), L = F(\beta_1, \dots, \beta_n) \Longrightarrow KL = F(\alpha_1, \dots, \alpha_m, \beta_1, \dots, \beta_n).$$

As $KL = L(\alpha_1, \dots, \alpha_m)$, we have

$$[KL : L] \leq m \Longrightarrow [KL : F] = [KL : L][L : F] \leq mn.$$

Now suppose that $(m, n) = 1$. As $m|[KL : F]$ and $n|[KL : F]$, $mn|[KL : F]$ and hence the equality. □

We say that K and L are *linearly disjoint over F* if $[K : F]$ and $[L : F]$ are coprime. If this is not the case, then we may have a strict inequality in the equation of the proposition. For example, if $K \neq F$ and $K = L$, then

$$[KL : F] = [K : F] < [K : F][L : F].$$

If K, L are linearly disjoint over F and $(\alpha_1, \dots, \alpha_m)$, $(\beta_1, \dots, \beta_n)$ respective bases of K and L, then a basis of KL may be found by taking the products $\alpha_i\beta_j$. Indeed, from Corollary 1.5,

$$KL = F(\alpha_1, \dots \alpha_m, \beta_1, \dots, \beta_n) = F[\alpha_1, \dots \alpha_m, \beta_1, \dots, \beta_n],$$

so the elements of KL are polynomials in the α_i and β_j. However, an expression of the form $\alpha_1^{s_1} \cdots \alpha_m^{s_m}$ belongs to K, so we may it write it as a linear combination (with coefficients in F) of the α_i. In the same way, we may write an expression of the form $\beta_1^{t_1} \cdots \beta_n^{t_n}$ as a linear combination of the β_j. As a consequence, the elements $\alpha_i\beta_j$ form a generating set of KL (as a vector space over F). Given that there are mn such elements and that the dimension of KL over F is mn, the $\alpha_i\beta_j$ form a basis of KL.

In Theorem 6.8 we considered the compositum of two extensions of a field, one of which was Galois. We now suppose that K and L are both Galois extensions of the field F contained in a field E. We claim that the compositum KL is a Galois extension of F. As KL is a separable extension of L and L a separable extension of F, from Theorem 3.7, KL is a separable extension of F. Proving that KL is a normal extension of F is a little more difficult. First we notice that K and L are splitting fields of respectively polynomials f and g of $F[X]$. We have

$$K = F(\alpha_1, \dots, \alpha_m) \qquad \text{and} \qquad L = F(\beta_1, \dots, \beta_n),$$

where $\alpha_1, \dots, \alpha_m$ (resp. $\beta_1, \dots, \beta_n$) are the roots of f (resp g) in E. If $\gamma_1, \dots, \gamma_s$ are the distinct elements in the set $\{\alpha_1, \dots, \alpha_m, \beta_1, \dots, \beta_n\}$, then $KL = F(\gamma_1, \dots, \gamma_s)$. The polynomial fg splits in KL. Let $U \subset KL$ be a splitting field of fg. As $\gamma_1 \dots \gamma_s \in U$, $F(\gamma_1, \dots, \gamma_s) \subset U$, i.e., $KL \subset U$. It follows that KL is a splitting field of fg and so a normal extension of F. We have shown that KL is a Galois extension of F, as claimed.

If $\sigma \in Gal(KL/F)$, then $\sigma_{|K} \in Gal(K/F)$ and $\sigma_{|L} \in Gal(L/F)$, because K/F and L/F are both normal.

Theorem 6.10 *Let us suppose that K/F and L/F are both normal. The mapping*

$$\psi : Gal(KL/F) \longrightarrow Gal(K/F) \times Gal(L/F), \sigma \longmapsto (\sigma_{|K}, \sigma_{|L}),$$

is a monomorphism and ψ is an isomorphism if and only if $K \cap L = F$.

PROOF The mapping ψ is clearly a homomorphism and, if $\sigma \in Gal(KL/F)$ fixes each element of K and each element of L, then σ fixex each element of KL. Cosequntly, ψ is a monomorphism.

The mapping ψ is an isomorphism if and only if $[KL : F] = [K : F][L : F]$, which applies only under the condition $[KL : L] = [K : F]$. This is the case if and only if the mapping

$$\phi : Gal(KL/L) \longrightarrow Gal(K/F), \sigma \longmapsto \sigma_{|K}$$

is an isomorphism. From Theorem 6.8, a necessary and sufficient condition for this is $K \cap L = F$.□

Remark We have seen that if K and L are both Galois extensions of F, then KL is Galois extension of F and we may consider that the Galois group of KL over F is a subgroup of the direct product of the Galois groups of K and L over F. In particular, if the Galois groups $Gal(K/F)$ and $Gal(L/F)$ are both abelian, then so is the Galois group $Gal(KL/F)$.

6.3 The fundamental theorem of algebra

It is a well-known that any nonconstant complex polynomial has a complex root. This is the *fundamental theorem of algebra*. In this section we will give a proof based on the field theory we have developpped.

Proposition 6.5 *The field of complex numbers* $\mathbf{C}$ *has no extension of degree* 2*.*

PROOF Suppose tht $\mathbf{C}$ has an extension E of degree 2. If $\alpha \in E \setminus \mathbf{C}$, then $\deg m(\alpha, F) = 2$. However, every polynomial $f \in \mathbf{C}[X]$ of degree 2 has a complex root, hence $m(\alpha, F)$ is reducible, a contradiction. Hence the result. □

Now we consider extensions of the field of real numbers $\mathbf{R}$.

Proposition 6.6 $\mathbf{R}$ *has no extension of odd degree strictly greater than* 1*.*

PROOF Suppose that $\mathbf{R}$ has an extension E with odd degree strictly greater than 1. Let $\alpha \in E \setminus \mathbf{R}$. If $\deg m(\alpha, \mathbf{R})$ is odd, then the polynomial $m(\alpha, \mathbf{R})$ has a real root and so is reducible, a contradiction. It follows from Proposition 1.4 that $[\mathbf{R}(\alpha) : \mathbf{R}]$ is even. As

$$[E : \mathbf{R}] = [E : \mathbf{R}(\alpha)][\mathbf{R}(\alpha) : \mathbf{R}],$$

$[E : \mathbf{R}]$ is even. □

We are now in a position to prove the fundamental theorem of algebra.

Theorem 6.11 *If* $f \in \mathbf{C}[X]$ *is nonconstant, then* f *has a root in* $\mathbf{C}$*.*

PROOF We will first prove the result for a nonconstant polynomial $f \in \mathbf{R}[X]$. We note $g(X) = (1 + X^2)f(X) \in \mathbf{R}[X]$ and let E be a splitting field of g. The complex numbers $\pm i$ and $\mathbf{R}$ belong to E so $\mathbf{C}$ is contained in E. As the characteristic of $\mathbf{R}$ is 0, g is separable and so E is separable (see Theorem 3.8). Therefore E is a Galois extension of $\mathbf{R}$. We now set $G = Gal(E/\mathbf{R})$, i.e., G is the Galois group of g. If $|G| = 2^s m$, with m odd, then G has a (Sylow-)subgroup H of order 2^s. We set $K = \mathcal{F}(H)$. Then, from Theorem 6.6,

$$[K : \mathbf{R}] = [G : H] = m.$$

As m is odd and $\mathbf{R}$ has no extension of odd degree strictly greater than 1, $m = 1$. Thus G is a 2-group.

We now set $H' = Gal(E/\mathbf{C})$ (the Galois group of g considered as a member of $\mathbf{C}[X]$). As H' is a subgroup of G, H' is a 2-group. If $|H'| = 2^t$, with $t \geq 1$, then H' has a subgroup H'' of index 2. If $K'' = \mathcal{F}(H'')$, then

$$[K'' : \mathbf{C}] = [H' : H''] = 2,$$

which contredicts Proposition 6.5. It follows that $H' = \{\mathrm{id}\}$ and $E = \mathbf{C}$ and so all the roots of g, and hence of f, lie in $\mathbf{C}$.

We now consider polynomials $f \in \mathbf{C}[X] \setminus \mathbf{R}[X]$. If we set $g = \bar{f}f$, where $\bar{f}$ is the polynomial whose coefficients are the complex conjugates of those of f, then $g \in \mathbf{R}[X]$. If α is a root of g, then α is a root of $\bar{f}$ or of f. This implies that α or $\bar{\alpha}$ is a root of f. Hence f has a root in $\mathbf{C}$. This ends the proof. □

6.4 Normal closures

In this short section we give a useful characterization of the normal closure N of E over F in the case where E is a finite extension of F. In Section 5.1 we saw that, if $E = F(\alpha_1, \ldots, \alpha_n)$ and $m_i(X) = m(\alpha_i, F)$, then a splitting field of $m(X) = m_1(X) \cdots m_n(X)$ is a normal closure N of E over F. We recall that if L_1 and L_2 are subfields of a field E, then $L_1 L_2$ is the smallest subfield of E containg both L_1 and L_2. More generally, if $L_1, \ldots, L_s$ are subfields of E, then $L_1 L_2 \ldots L_s$ is the smallest subfield of E containing the L_i.

Theorem 6.12 *Let E be a finite extension of F and N the normal closure of E over F in an algebraic closure C of E. Then*

$$N = \prod_{\sigma \in Gal(N/F)} \sigma(E).$$

PROOF We use the description of N as the splitting field of $m = m_1 \cdots m_n$ seen above. If $\sigma \in Gal(N/F)$, then $\sigma(F) = F$ and $\sigma(\alpha_i) \in N$, for all i, because the $\sigma(\alpha_i)$ are roots of m. Hence $\sigma(E) \subset N$, for all $\sigma \in Gal(N/F)$ and so

$$\prod_{\sigma \in Gal(N/F)} \sigma(E) \subset N.$$

If $\alpha \in N$ is a root of m, then α is a root of m_i, for some i. From Proposition 2.3, we know that there is an F- isomorphism $\tau : F(\alpha_i) \longrightarrow F(\alpha)$, with $\tau(\alpha_i) = \alpha$. Using Theorem 2.7, we may extend τ to a monomorphism σ from N into C. As N is a normal extension, we know from Proposition 5.2 that σ is an automorphism of N, i.e., $\sigma \in Gal(N/F)$. Given that $\alpha_i \in E$ and $\sigma(\alpha_i) = \alpha$, we have $\alpha \in \sigma(E)$. It follows that

$$\alpha \in \prod_{\sigma \in Gal(N/F)} \sigma(E) \Longrightarrow N \subset \prod_{\sigma \in Gal(N/F)} \sigma(E).$$

This ends the proof. □

Chapter 7

The Galois group of a polynomial

In this chapter we continue our study of the Galois group. If f is a polynomial with coefficients in the field F and E a splitting field of f, then we call $Gal(E/F)$ a *Galois group of the polynomial* f. As splitting fields of a polynomial are isomorphic, any two Galois groups of a polynomial are isomorphic, so we often, with an abuse of language, speak of the Galois group of a polynomial.

Proposition 7.1 *If E is a splitting field of a separable polynomial $f \in F[X]$, then E is a Galois extension of F.*

PROOF From Theorem 2.1 we know that the extension E is finite. Being a splitting field of a polynomial, we also know that it is normal, so we only need to show that E is separable. Now, $E = F(\alpha_1, \dots, \alpha_n)$, where the α_i are the roots of f. Each minimal polynomial $m_i = m(\alpha_i, F)$ divides an irreducible factor of f. As the irreducible factors of f do not have multiple roots, no m_i has a multiple root. Thus each α_i is separable. From Theorem 3.8, $F(\alpha_1, \dots, \alpha_n)$ is separable. □

Corollary 7.1 *If $G = Gal(E/F)$ is the Galois group of a separable polynomial, then $|G| = [E : F]$.*

PROOF It is sufficient to apply Theorem 6.1. □

Different polynomials over the same field may have the same Galois group. This may be useful in determining the Galois group of a given polynomial. For example, if $f \in F[X]$ has the splitting field E and $a \in F$, then E is also the splitting field of $g(X) = f(-a + X)$: if $\alpha_1, \dots, \alpha_n$ are the roots of f in$E$, then $a + \alpha_1, \dots, a + \alpha_n$ are the roots of g in E. The following result is useful, because certain methods of determining the Galois group only apply to monic polynomials with integer coefficients.

Proposition 7.2 *If $f \in \mathbf{Q}[X]$, then there is a strongly separable monic polynomial $g \in \mathbf{Z}[X]$ with the same Galois group over $\mathbf{Q}$ as f.*

PROOF Let E be the splitting field of $f \in \mathbf{Q}[X]$ in $\mathbf{C}$. If we set $f_1 = \frac{f}{\mathrm{hcf}(f,f')}$, then f_1 has the same roots as f and these roots are simple. Therefore f_1 is strongly separable and has the same splitting field as f.

Now let u be the lcm of the denomoinators of the coefficients of f_1. If we set $f_2 = uf_1$, then $f_2 \in \mathbf{Z}[X]$ and has the same roots as f_1.

Finally, if $f_2(X) = \sum_{i=0}^n a_i X^i$, then we set

$$g(Y) = \sum_{k=0}^{n-1} a_k (a_n)^{n-k-1} Y^k + Y^n \ \in \mathbf{Z}[X].$$

As

$$g(a_n X) = a_n^{-1} f_2(X),$$

g has the same roots as f up to multiplication by the contant a_n and so has the same splitting field as f_2. Thus we have found a monic strongly separable polynomial in $\mathbf{Z}[X]$ with splitting field E. □

By Cayley's theorem, any finite group of cardinal k can be identified with a subgroup of S_k, the group of permutations of the set $\mathbf{N}_k = \{1, \dots, k\}$. In general, a Galois group G of a polynomial can be identified with a subgroup of a group of permutations S_n, where n is much smaller that the cardinal of the group.

Proposition 7.3 *If $f \in F[X]$ has n distinct roots in a splitting field, then the Galois group of f is isomorphic to a subgroup of S_n.*

PROOF We set $A = \{\alpha_1, \dots, \alpha_n\}$ the set of roots of f in a splitting field E. If $\sigma \in Gal(E/F)$, then σ permutes the roots of f, so we may define a mapping

$$\phi : Gal(E/F) \longrightarrow S_A, \sigma \longmapsto \sigma_{|A},$$

where S_A denotes the group of permutations on A. The mapping ϕ is clearly a group homomorphism. The F-automorphism σ is determined by its effect on the roots of f, so ϕ is injective. Thus $Gal(E/F)$ is isomorphic to a subgroup of S_A. As S_A is isomorphic to S_n, $Gal(E/F)$ is isomorphic to a subgroup G of S_n. □

We have assumed a certain order on the roots of the polynomial. It is natural to ask what happens when we change the order. Suppose that we choose a different ordering of the roots:

$$A = \{\alpha'_1, \dots, \alpha'_n\}.$$

We obtain an isomorphism ϕ' of the Galois group $Gal(E/F)$ onto another subgroup G' of S_n. If $\sigma \in Gal(E/F)$, $\phi(\sigma) = s$ and $\phi'(\sigma) = s'$, then

$$\sigma(\alpha_i) = \alpha_{s(i)} \qquad \text{and} \qquad \sigma(\alpha'_i) = \alpha'_{s'(i)},$$

for $i = 1, \dots, n$. There is a unique permutation $r \in S_n$ such that $\alpha'_i = \alpha_{r(i)}$, for all i, hence we can write

$$\alpha_{sr(i)} = \sigma(\alpha_{r(i)}) = \sigma(\alpha'_i) = \alpha'_{s'(i)} = \alpha_{rs'(i)}.$$

Therefore, for all i,

$$sr(i) = rs'(i) \Longrightarrow r^{-1}sr = s' \Longrightarrow G' = r^{-1}Gr,$$

i.e., G' is a conjugate of G.

The general polynomial

The general polynomial of degree n over a field F is

$$f(Y) = Y^n - X_1 Y^{n-1} + X_2 Y^{n-2} - \cdots + (-1)^{n-1} X_{n-1} + (-1)^n X^n \in F(X_1, \dots, X_n)[Y],$$

where $F(X_1, \dots, X_n)$ is the rational function field over the field F in n variables. It is not difficult to determine the Galois group of f.

Theorem 7.1 *The Galois group of the general polynomial f is the symmetric group S_n.*

PROOF Let $L = F(X_1, \ldots, X_n)$. Then $f \in L[Y]$. Now let $Z_1, \ldots, Z_n$ be the roots of f in some extension of L. Then $X_i = s_i(Z_1, \ldots, Z_n)$, where s_i is the ith elementary symmetric polynomial. Hence $L = F(s_1(Z_1, \ldots, Z_n), \ldots, s_n(Z_1, \ldots, Z_n))$ and a splitting field of f is given by

$$L(Z_1, \ldots, Z_n) = F(s_1(Z_1, \ldots, Z_n), \ldots, s_n(Z_1, \ldots, Z_n), Z_1, \ldots, Z_n) = F(Z_1, \ldots Z_n).$$

Therefore

$$Gal_L(f) \simeq Gal(F(Z_1, \ldots, Z_n)/F(s_1, \ldots, s_n)) \simeq Gal(F(Z_1, \ldots, Z_n)/F_S(Z_1, \ldots, Z_n)) = S_n,$$

according to the discussion after Theorem 6.7. □

7.1 Irreducible polynomials

Before studying the particular properties of Galois groups of irreducible polynomials, we will revise the notion of the *action of a group* on a set. We recall that a group G, with identity e, acts on a set X if there is a mapping $\Phi : G \times X \longrightarrow X$, called an action and usually written $\Phi(g, x) = g.x$, such that

- $e.x = x$, for all $x \in X$;
- $(gh).x = g.(h.x)$, for all $g, h \in G$ and $x \in X$.

(We sometimes refer to the action we have just defined as a left action to distinguish it from a right action, where we replace the second condition by the following:

$$(gh).x = h.(g.x),$$

for all $g, h \in G$ and $x \in X$. Of course, if the group G is abelian, then there is no distinction between left and right actions.)

The orbit of an element $x \in X$, written O_x, is the collection of $y \in X$ for which there exists $g \in G$ with $y = g.x$. We define a relation $\mathcal{R}$ on X by $x\mathcal{R}y$ if $y \in O_x$. Then $\mathcal{R}$ is an equivalence relation on X and the distinct orbits are its equivalence classes. We say that the action is *transitive* if there is a unique orbit, i.e., for any $x, y \in X$, there is a $g \in G$, with $g.x = y$. The action is *free* if $g.x = x$ implies that g is the identity of G.

If $x \in X$, then the *stabilizer of* x, which we write G_x, is the set of elements of G which leave x unchanged:

$$G_x = \{g \in G : g.x = x\}.$$

Clearly G_x is a subgroup of G. The following result is known as the orbit-stabilizer theorem.

Theorem 7.2 *If G is finite and $x \in X$, then*

$$|O_x| = [G : G_x] = \frac{|G|}{|G_x|}.$$

PROOF We define a mapping

$$\phi : G \longrightarrow O_x, g \longmapsto g.x.$$

ϕ is clearly surjective. As G_x is a subgroup of G,

$$\phi(g) = \phi(h) \Longleftrightarrow g.x = h.x \Longleftrightarrow g^{-1}h \in G_x.$$

Therefore we have a well-defined bijection $\bar{\phi} : G/G_x \longrightarrow O_x$ defined by

$$\bar{\phi}(gG_x) = \phi(g).$$

It follows that

$$|O_x| = [G : G_x] = \frac{|G|}{|G_x|}.$$

This ends the proof. □

If $f \in F[X]$ is separable, $A = \{\alpha_1, \dots, \alpha_n\}$ the roots of f in a splitting field E and $G = Gal(E/F)$, then the mapping

$$\Phi : G \times A, (\sigma, \alpha_i) \longmapsto \sigma(\alpha_i)$$

defines an action of G on A. (As the Galois group G of a polynomial of degree n is isomorphic to a subgroup H of S_n, we may consider that G acts on $\mathbf{N}_n$.) For irreducible, separable polynomials we can say more.

Theorem 7.3 *Let f be a separable polynomial in $F[X]$ of degree n with Galois group $G = Gal(E/F)$. If f is irreducible, then*

- **a.** *n divides the order of G;*
- **b.** *the action of G on A is transitive.*

PROOF **a.** Let $\alpha \in E$ be a root of f. From Proposition 1.4 we have $[F(\alpha) : F] = n$. Now $[F(\alpha) : F] | [E : F]$. In addition, E is a Galois extension of F and so, from Corollary 7.1, $[E : F] = |G|$. Therefore n divides $|G|$.

b. Let $f \in F[X]$ be irreducible and α, α' two roots of f in E. From Proposition 2.3, with $F' = F$ and $\sigma = \mathrm{id}_F$, we obtain an isomorphism $\hat{\sigma}$ from $F(\alpha)$ onto $F(\alpha')$ extending id_F such that $\hat{\sigma}(\alpha) = \alpha'$. We now apply Theorem 2.2 to obtain $\sigma \in Gal(E/F)$ taking α to α'. This implies that the action of the Galois group on A is transitive. □

Remark We recall that a group of permutations G on a set X is said to be *transitive* if for any pair $(x, y) \in X^2$, there exists $\pi \in G$ such that $\pi(x) = y$. Thus, if f is irreducible, then $G_{|A}$ is a transitive permutation group.

The second part of the theorem which we have just proved has a partial converse.

Proposition 7.4 *Let $f \in F[X]$, with $\deg f \geq 2$, and G be its Galois group. If f has two distinct irreducible factors, then the action of G on A is not transitive.*

PROOF Let α_1, α_2 be roots of f and g_1, g_2 be distinct irreducible factors of f, with $g_1(\alpha_1) = g_2(\alpha_2) = 0$. If $\sigma \in G$ and $\sigma(\alpha_1) = \alpha_2$, then

$$g_1(\alpha_2) = g_1(\sigma(\alpha_1)) = \sigma(g_1(\alpha_1)) = 0.$$

We may suppose that g_1 and g_2 are monic polynomials. Then both g_1 and g_2 are minimal polynomials of α_2, which is impossible. Therefore the action of G on A is not transitive. □

Remark If $f = \lambda g^m$, where $\lambda \in F$, $g \in F[X]$ is irreducible and $m \geq 2$, then the action of G on A is transitive. It is sufficient to notice that a splitting field of g is a splitting field of f and then apply the second part of Theorem 7.3.

7.2 Cyclotomic extensions

We consider the polynomial $f(X) = -1 + X^n \in F[X]$. The roots of this equation in a splitting field are called nth roots of unity. If char $F = 0$ or char $F = p > 0$, with $(p, n) = 1$, then f is separable:

$$f'(X) = nX^{n-1} \Longrightarrow gcd(f, f') = 1.$$

In this case, f has n distinct roots in a splitting field E. The set of these roots, which we will note μ_n, form a subgroup of the multiplicative group of E. As μ_n is finite, by Theorem 3.3, μ_n is cyclic. A generator ζ of this group is said to be a *primitive nth root of unity.* An extension $E = F(\zeta)$, where ζ is a primitive nth root of unity is called a *cyclotomic extension* of F. In fact, E is a splitting field of the polynomial $f(X) = -1 + X^n$, so we have $E = F(\mu_n)$ and it follows that E is a Galois extension of F. Clearly, if ζ' is another primitive nth root of unity, then $E = F(\zeta')$. We write μ_n^* for the subset of μ_n composed of primitive nth roots of unity. The cardinal of μ_n^* is $\phi(n)$, where ϕ is Euler's totient function.

Exercise 7.1 *Show that, if char $F = p > 0$ and $(p, n) \neq 1$, then there is no primitive nth root of unity.*

Up to now we have assumed that char $F = 0$, or char $F = p > 0$ with $(p, n) = 1$. In this section we will continue to do so. We consider the Galois group of the cyclotomic extension $F(\mu_n)$.

Proposition 7.5 *If $\sigma \in Gal(F(\mu_n)/F)$, then there is an integer $a = a(\sigma)$, with $(a, n) = 1$, such that $\sigma(x) = x^a$, for all $x \in \mu_n$.*

PROOF Let ζ be a generator of μ_n. Then

$$\sigma(\zeta)^n = \sigma(\zeta^n) = \sigma(1) = 1$$

and, for $j = 1, \ldots, n-1$,

$$\sigma(\zeta)^j = \sigma(\zeta^j) \neq 1,$$

because $\zeta^j \neq 1$ and σ is injective. Hence $\sigma(\zeta)$ is also a generator of μ_n. This implies that $\sigma(\zeta) = \zeta^a$, where $(a, n) = 1$. Now take any $x \in \mu_n$. There exists an integer k such that $x = \zeta^k$, so

$$\sigma(x) = \sigma(\zeta^k) = \sigma(\zeta)^k = (\zeta^a)^k = (\zeta^k)^a = x^a,$$

which is what we set out to prove. □

We may define a mapping ϕ from $Gal(F(\mu_n)/F)$ into $\mathbf{Z}_n^\times$, the group of units of $\mathbf{Z}_n$, by setting $\phi(\sigma) = [a(\sigma)]$, where $[u]$ denotes the congruence class modulo n of u.

Theorem 7.4 *The mapping ϕ is a monomorphism.*

PROOF Let σ and τ be elements of $Gal(F(\mu_n)/F)$ and ζ a primitive nth root of unity. Then

$$(\sigma\tau)(\zeta) = \sigma(\tau(\zeta)) = \sigma(\zeta^{a(\tau)}) = \sigma(\zeta)^{a(\tau)} = (\zeta^{a(\sigma)})^{a(\tau)} = \zeta^{a(\sigma)a(\tau)}.$$

In addition, $(\sigma\tau)(\zeta) = \zeta^{a(\sigma\tau)}$ and it follows that $a(\sigma\tau) \equiv a(\sigma)a(\tau)(\mod n)$. Therefore

$$[a(\sigma\tau)] = [a(\sigma)][a(\tau)] \Longrightarrow \phi(\sigma\tau) = \phi(\sigma)\phi(\tau).$$

We have shown that ϕ is a homomorphism. It remains to establish the injectivity. If σ is in the kernel of ϕ, then $a(\sigma) = 1$ and so $\sigma(\zeta) = \zeta$. As σ fixes all the elements of F, σ is the identity on $F(\mu_n)$, i.e., ϕ is injective. □

Corollary 7.2 *If E is a cyclotomic extension of F, then the Galois group $G = Gal(E/F)$ is abelian.*

PROOF As G is isomorphic to a subgroup of $\mathbf{Z}_n^\times$, which is abelian, G is abelian. □

Remark The Galois group of a cyclotomic extension may be cyclic. This is so if $n = 2^k$, with $k = 1, 2$, or $n = p^k$, where p is an odd prime and $k \in \mathbf{N}^*$, because in these cases the group $\mathbf{Z}_n^\times$ is cyclic (see [21], for example).

Exercise 7.2 *Let $n = 5$ or $n > 6$. Show that the injection of $Gal(\mathbf{R}(\mu_n)/\mathbf{R})$ in $\mathbf{Z}_n^\times$ is not surjective.*

It is interesting to consider composita of cyclotomic extensions. To do so we will need a little elementary group theory.

Theorem 7.5 *Let G be a group, with identity e, and x, y elements of G which commute. If $o(x) = m$, $o(y) = n$ and $(m, n) = 1$, i.e., m and n are coprime, then $o(xy) = mn$.*

PROOF We first notice that $\langle x\rangle \cap \langle y\rangle = \{e\}$. By Lagrange's theorem, $|\langle x\rangle \cap \langle y\rangle|$ divides both m and n. As $(m, n) = 1$, we have $\langle x\rangle \cap \langle y\rangle = \{e\}$. Now,

$$(xy)^{mn} = (x^m)^n(y^n)^m = ee = e.$$

On the other hand, if $(xy)^k = e$, then $x^k = y^{-k}$ and so $x^k \in \langle x\rangle \cap \langle y\rangle$. Hence, $x^k = e$, which implies that $m|k$. In the same way, we have $n|k$. It follows that $mn|k$, because $(m, n) = 1$ and so $o(xy) = mn$. □

It would be natural to assume that if x and y commute then $o(xy) = [m, n]$. However, this is not true. We only need to consider the case where $y = x^{-1}$ and $x \neq e$; then $o(xy) = o(e) = 1$ and $[m, n] = [m, m] > 1$. On the other hand, we have a result which is quite close to the statement we have just considered. It follows from the theorem.

Corollary 7.3 *Let G be a group, with identity e, and x, y elements of G which commute. If $o(x) = m$, $o(y) = n$, then there are powers a of x and b of y such that $o(x^a y^b) = [m, n]$.*

PROOF If $p_1, \ldots, p_s$ are the primes in the decomposition of m and n and $m = \prod_{i=1}^s p_i^{\alpha_i}$ and $n = \prod_{i=1}^s p_i^{\beta_i}$, then $[m, n] = \prod_{i=1}^s p_i^{m_i}$, where $m_i = \max(\alpha_i, \beta_i)$. We divide the indices i into two distinct classes, I being composed of those i for which $\alpha_i = m_i$ and J of those indices for which $\beta_i = m_i > \alpha_i$. We set

$$m' = \prod_{i\in I} p^{m_i} \quad \text{and} \quad n' = \prod_{i\in J} p^{m_i}.$$

Clearly $[m', n'] = [m, n]$. We also notice that $m'|m$, $n'|n$ and

$$o(x^{\frac{m}{m'}}) = m', \quad o(y^{\frac{n}{n'}}) = n' \quad \text{and} \quad (m', n') = 1,$$

hence, by Theorem 7.5,

$$o(x^{\frac{m}{m'}} y^{\frac{n}{n'}}) = m'n' = [m, n],$$

which completes the proof. □

We now consider the compositum of two cyclotomic fields.

Proposition 7.6 *The compositum of the fields $F(\mu_m)$ and $F(\mu_n)$ is $F(\mu_{[m,n]})$.*

PROOF Because $[m, n]$ is a multiple of m and n, both the fields $F(\mu_m)$ and $F(\mu_n)$ are included in $F(\mu_{[m,n]})$, hence the compositum of these two fields is also included in $F(\mu_{[m,n]})$. Now let ζ_m (resp. ζ_n) be an mth (resp. nth) primitive root of unity. From Corollary 7.3, there are powers a of ζ_m and b of ζ_n such that $o(\zeta_m^a \zeta_n^n) = [m, n]$, which implies that a primitive $[m, n]$th root of unity lies in the compositum $F(\mu_m)F(\mu_n)$. Therefore $F(\mu_{[m,n]}) \subset F(\mu_m)F(\mu_n)$. We thus have the equality we were looking for. □

Remark We might be tempted to think that $F(\mu_m) \cap F(\mu_n) = F(\mu_{(m,n)})$. As m and n are both multiples of (m, n), we certainly have $F(\mu_{(m,n)}) \subset F(\mu_m) \cap F(\mu_n)$, however the other inclusion may not be true. Here is an example. We set $F = \mathbf{Q}(\sqrt{3})$ and we consider $F(\mu_3)$ and $F(\mu_4)$. As $(3, 4) = 1$, $F(\mu_{(3,4)}) = F(1) = F$. On the other hand,

$$F(\mu_4) = \mathbf{Q}(\sqrt{3}, i) = F(\mu_3) \Longrightarrow F(\mu_3) \cap F(\mu_4) = \mathbf{Q}(\sqrt{3}, i) \neq F.$$

With more knowledge of the field F we can say more about cyclotomic extensions. We will first consider the case where $F = \mathbf{Q}$. To do so we will introduce *cyclotomic polynomials.*

Exercise 7.3 *Let F be field and ξ_1 (resp. ξ_2) an mth (resp. nth) root of unity. Show that the compositum $F(\xi_1)F(\xi_2)$ is included in the cyclotomic field $F(\mu_{[m,n]})$.*

7.3 Cyclotomic polynomials

In this section we will be concerned with a class of polynomials with coefficients in $\mathbf{Q}$. The nth cyclotomic polynomial $\Phi_n \in \mathbf{C}[X]$ is defined by

$$\Phi_n(X) = \prod_{\zeta \in \mu_n^*} (-\zeta + X).$$

The degree of Φ_n is $\phi(n)$, because $|\mu_n^*| = \phi(n)$.

If $z \in \mu_n$, then $o(z)|n$, hence $z \in \cup_{d|n} \mu_d^*$. On the other hand, if $d|n$ and $z \in \mu_d^*$, then $z \in \mu_n$. Thus $\mu_n = \cup_{d|n} \mu_d^*$. As $\mu_d^* \cap \mu_d'^* = \emptyset$, if $d \neq d'$, the sets μ_d^*, with $d|n$, form a partition of μ_n and

$$-1 + X^n = \prod_{d|n} \left(\prod_{z \in \mu_d^*} (-z + X) \right) = \prod_{d|n} \Phi_d.$$

In fact, all the coefficients of Φ_n are integers.

Proposition 7.7 *The polynomial Φ_n belongs to $\mathbf{Z}[X]$ and is monic; in addition, its first coefficient is 1, if $n \geq 2$.*

PROOF From the definition of Φ_n, it is clearly monic. We now prove by induction that $\Phi_n \in \mathbf{Z}[X]$ and also that the constant term of the polynomial is 1, if $n \geq 2$. As $\Phi_1(X) = -1 + X$ and $\Phi_2(X) = 1 + X$, the claim is true for $n = 1$ and $n = 2$. Suppose now that it is true up to $n - 1$, with $n > 2$, and consider the case n. We have

$$-1 + X^n = \left(\prod_{d|n, d<n} \Phi_d \right) \Phi_n = A\Phi_n.$$

If $A(X) = \sum_{i=0}^{s} a_i X^i$ and $\Phi_n(X) = \sum_{j=0}^{t} b_j X^j$, then $a_i \in \mathbf{Z}$, for all i and $a_0 = -1$. As $a_0 b_0 = -1$, we have $b_0 = 1$. Also,

$$a_0 b_1 + a_1 b_0 = -b_1 + a_1 = 0 \Longrightarrow b_1 = a_1 \in \mathbf{Z}.$$

In addition, as

$$a_0 b_2 + a_1 b_1 + a_2 b_0 = -b_2 + a_1 b_1 + a_2 = 0 \Longrightarrow b_2 = a_1 b_1 + a_2 \in \mathbf{Z}.$$

Continuing in the same way, we see that $b_j \in \mathbf{Z}$, for all j. □

Exercise 7.4 *Show that, if p is a prime number and $r \in \mathbf{N}^*$, then $\Phi_{p^r}(X) = \Phi_p(X^{p^{r-1}})$.*

We have seen that the coefficients of a cyclotomic polynomial are integers. We can say more. In particular, any integer figures as a coefficient of at least one cyclotomic polynomial. A proof of this may be found in [17]. For $n \geq 3$, the degree is even so there is a middle coefficient. If n is a power of 2, then this coefficient is 0; otherwise it is an odd number. This is proved in [7].

We may thus consider the polynomials Φ_n as members of $\mathbf{Z}[X]$. We will now show that they are irreducible over $\mathbf{Q}$. However, we need some preliminary results.

If f is a polynomial in $\mathbf{Z}[X]$ and p a prime number, then we may define $\bar{f} \in \mathbf{F}_p[X]$ by replacing the coefficients of f by their congruence classes modulo p. The polynomial $\bar{f}$ so obtained is called the *reduction modulo* p of f. Clearly, if $f = AB$, then $\bar{f} = \bar{A}\bar{B}$. The next result needs a proof.

Lemma 7.1 *Let F be a field and $A, B \in F[X]$, with A irreducible. If A and B have a common root, then A divides B.*

PROOF Let α be a common root of A and B. If A does not divise B, then A and B are coprime and so there exist $S, T \in F[X]$ such that

$$SA + TB = 1 \Longrightarrow S(\alpha)A(\alpha) + T(\alpha)B(\alpha) = 1,$$

which is a contradiction, because α is a root of A and B. Hence A divides B. □

Lemma 7.2 *If p is a prime number and $A_1, \ldots, A_n \in \mathbf{F}_p[X]$, then $(\sum_{i=1}^{n} A_i)^p = \sum_{i=1}^{n} A_i^p$. Also, if $A(X) \in \mathbf{F}_p[X]$, then $A(X)^p = A(X^p)$.*

PROOF As char $\mathbf{F}_p[X] = p$ and $p|\binom{p}{i}$, for $i = 1, \ldots, p-1$, we have $(A_1 + A_2)^p = A_1^p + A_2^p$. An induction argument allows us to obtain the result for any n.

If $A(X) = \sum_{i=0}^m a_i X^i$, then from the first part of the proof,

$$A(X)^p = \sum_{i=0}^m (a_i X^i)^p = \sum_{i=0}^m a_i^p X^{ip} = \sum_{i=0}^m a_i^p X^{pi} = A(X^p).$$

This ends the proof. □

Before turning to the proof of the irreducibility of cyclotomic polynomials, we recall the following result, which follows from Gauss's lemma:

If $A \in \mathbf{Z}[X]$ and $A = BC$, with $B, C \in \mathbf{Q}[X]$ and monic, then $B, C \in \mathbf{Z}[X]$.

Theorem 7.6 *For all $n \in \mathbf{N}^*$, the polynomial Φ_n is irreducible over $\mathbf{Q}$.*

PROOF Let A be a monic, irreducible polynomial in $\mathbf{Q}[X]$, which divides Φ_n. If $\alpha \in \mathbf{C}$ is a root of A, then α is also a root of Φ_n and so a primitive nth root of unity.

As A divides Φ_n and Φ_n divides $f(X) = -1 + X^n$, there exists $B \in \mathbf{Q}[X]$ such that $AB = f$. As A is monic, so is B. Now using the result cited before the statement of the theorem, we see that $A, B \in \mathbf{Z}[X]$. In addition, A and B are coprime. (If this were not the case, then A and B would have a common root and their product at most $n-1$ distinct roots, a contradiction.)

Let p be a prime number such that $p < n$ and $p \not| n$. We will show that α^p is a root of A. If this is not the case, then α^p is a root of B. (As α is a root of f, any power of α is also a root of f, hence of A or B.) It follows that α is a root of $B(X^p)$. From Lemma 7.1, we have $A(X)|B(X^p)$. Taking reductions modulo p, we obtain $\bar{A}(X)|\bar{B}(X^p)$. If $C \in \mathbf{F}_p[X]$ is irreducible, then, using Lemma 7.2,

$$C(X)|\bar{A}(X) \Longrightarrow C(X)|\bar{B}(X^p) \Longrightarrow C(X)\bar{B}(X)^p \Longrightarrow C(X)|\bar{B}(X).$$

Hence $\bar{A}$ and $\bar{B}$ are not coprime in $\mathbf{Z}_p[X]$. However, A and B are coprime, so we have a contradiction. It follows that α^p is a root of A, and also a primitive nth root of unity.

If $1 < s < n$) is coprime with n and has the prime factorization $s = p_1 \cdots p_k$, then all the p_i are coprime with n. From what we have just seen, α^{p_1} is a root of A, and also a primitive nth root of unity. Replacing α by α^{p_1} we obtain that $\alpha^{p_1 p_2}$ is a root of A and also a primitive nth root of unity. continuing in the same way, we see that α^s is a root of A and also a primitive nth root of unity. It follows that all the primitive nth roots of unity are roots of A and therefore $A = \Phi_n$, i.e., Φ_n is irreducible. □

Corollary 7.4 *The cyclotomic polynomial Φ_n is the minimal polynomial over $\mathbf{Q}$ of each primitive nth root ζ of unity, i.e., $m(\zeta, \mathbf{Q}) = \Phi_n$.*

Exercise 7.5 *Show that the polynomial*

$$P_n(X) = 1 + X + \cdots + X^n \in \mathbf{Q}[X]$$

is irreducible if and only if $n+1$ is a prime number.

7.4 Cyclotomic extensions of the rationals

We now consider the Galois group of certain polynomials in $\mathbf{Q}[X]$, namely the cyclotomic polynomials.

Theorem 7.7 *The Galois group $G = Gal(\mathbf{Q}(\mu_n)/\mathbf{Q})$ is isomorphic to $\mathbf{Z}_n^\times$.*

PROOF From Theorem 7.4 we know that G is isomorphic to a subgroup of $\mathbf{Z}_n^\times$. However, if ζ is a primitive nth root of unity, then

$$|G| = [\mathbf{Q}(\zeta) : \mathbf{Q}] = \deg \Phi_n = \phi(n).$$

The second equality comes from Corollary 7.4. As $|\mathbf{Z}_n^\times| = \phi(n)$ and $\mathbf{Q}(\mu_n) = \mathbf{Q}(\zeta)$, G is isomorphic to $\mathbf{Z}_n^\times$. □

In the remark after Proposition 7.6 we observed that $F(\mu_{(m,n)}) \subset F(\mu_m) \cap F(\mu_n)$ and then gave an example to show that equality is generally not the case. However, using the theorem we have just proved, we may show that, in the case where the field F is $\mathbf{Q}$, then we do indeed have equality.

Corollary 7.5 *The property*

$$\mathbf{Q}(\mu_{(m,n)}) = \mathbf{Q}(\mu_m) \cap \mathbf{Q}(\mu_n)$$

is true for all $m, n \in \mathbf{N}^*$.

PROOF As $\mathbf{Q}(\mu_{(m,n)}) \subset \mathbf{Q}(\mu_m) \cap \mathbf{Q}(\mu_n)$, we only need to prove that

$$[\mathbf{Q}(\mu_{(m,n)}) : \mathbf{Q}] = [\mathbf{Q}(\mu_m) \cap \mathbf{Q}(\mu_n) : \mathbf{Q}].$$

From Proposition 7.6 we know that $\mathbf{Q}(\mu_m)\mathbf{Q}(\mu_n) = \mathbf{Q}(\mu_{[m,n]})$. Now, using Corollary 6.1, we obtain

$$[\mathbf{Q}(\mu_{[m,n]}) : \mathbf{Q}] = \frac{[\mathbf{Q}(\mu_m) : \mathbf{Q}][\mathbf{Q}(\mu_n) : \mathbf{Q}]}{[\mathbf{Q}(\mu_m) \cap \mathbf{Q}(\mu_n) : \mathbf{Q}]}.$$

Now, using the theorem, we have

$$\phi([m,n]) = \frac{\phi(m)\phi(n)}{[\mathbf{Q}(\mu_m) \cap \mathbf{Q}(\mu_n) : \mathbf{Q}]}.$$

However,

$$\phi([m,n])\phi((m,n)) = \phi(m)\phi(n) \Longrightarrow [\mathbf{Q}(\mu_m) \cap \mathbf{Q}(\mu_n) : \mathbf{Q}] = \phi((m,n)) = [\mathbf{Q}(\mu_{(m,n)}) : \mathbf{Q}].$$

This finishes the proof. □

There are other interesting questions concerning cyclotomic extensions of the rational numbers. We will now consider two of these, namely the number of roots of unity in a cyclotomic extension and the coincidence of two such extensions. We will begin with two results concerning Euler's totient function ϕ.

Proposition 7.8 *For any given positive integer N, there are at most finitely many integers n such that $\phi(n) = N$.*

PROOF Let N be a positive integer and p the least prime number greater than $N+1$. Suppose that n is an integer such that $\phi(n) = N$. If $q \geq p$ is a prime divisor of n, then $n = q^k m$, for some $k, m \in \mathbf{N}^*$, with $(q, m) = 1$. We have

$$\phi(n) = \phi(q^k)\phi(m) \geq q - 1 \geq p - 1 > N,$$

a contradiction. Therefore no prime divisor of n is greater than $N+1$. In particular, the distinct prime divisors of n belong to a finite set. Let us note these primes $p_1, \ldots, p_s$. Then

$$n = p_1^{a_1} \cdots p_s^{a_s} \Longrightarrow \phi(n) = \prod_{i=1}^{s} p_i^{a_i - 1}(p_i - 1).$$

For each prime p_i we have

$$\phi(n) \geq p_i^{a_i - 1}(p_i - 1).$$

If a_i sufficiently large, the expression on the right hand side of the equality is greater than N, hence there is a finite number of choices for the exponents. Therefore the set of all n such that $\phi(n) = N$ is finite. □

Remark If N is not 1 or an even number, then there are no integers n such that $\phi(n) = N$. It has been shown that, for any integer $k \geq 2$, there is an integer N such that there are just k solutions to the equation $\phi(n) = N$ [8]. For the case $k = 1$, the question is open.

Corollary 7.6 *We have*

$$\lim_{n \to \infty} \phi(n) = \infty.$$

PROOF If $\lim_{n \to \infty} \phi(n) \neq \infty$, then there is an integer $N > 0$ and an infinite sequence of integers (n_i) such that $\phi(n_i) \leq N$, for all n_i. For the values of the $\phi(n_i)$ let us write $N_1, \ldots, N_s$. There is a finite number of such values and $N_i \leq N$, for all i. However, from Proposition 7.8, there can only be a finite number of elements of the sequence whose image is equal to one of N_i. If we take an element n_i larger than all these elements, then we must have $\phi(n_i) > \max N_j$, a contradiction. This implies that $\lim_{n \to \infty} \phi(n) = \infty$. □

We need another elementary result.

Proposition 7.9 *If a and b are positive integers, then*

$$\phi(ab) = \frac{\phi(a)\phi(b)(a,b)}{\phi((a,b))}.$$

PROOF If $a = 1$ or $b = 1$, then the result is trivial, so suppose that this is not the case. Let $p_1, \ldots, p_s$ be the prime divisors of a which are not divisors of b and $q_1, \ldots, q_t$ the prime divisors of b which are not divisors of a. Finally let $u_1, \ldots, u_r$ be the prime divisors of both a and b. Then

$$\begin{aligned}
\phi(ab) &= ab\prod_{i=1}^{s}(1 - \frac{1}{p_i})\prod_{j=1}^{r}(1 - \frac{1}{u_j})\prod_{k=1}^{t}(1 - \frac{1}{q_k}) \\
&= \frac{a\prod_{i=1}^{s}(1 - \frac{1}{p_i})\prod_{j=1}^{r}(1 - \frac{1}{u_j})b\prod_{k=1}^{t}(1 - \frac{1}{q_k})\prod_{j=1}^{r}(1 - \frac{1}{u_j})}{\prod_{j=1}^{r}(1 - \frac{1}{u_j})} \\
&= \frac{\phi(a)\phi(b)(a,b)}{(a,b)\prod_{j=1}^{r}(1 - \frac{1}{u_j})} \\
&= \frac{\phi(a)\phi(b)(a,b)}{\phi((a,b))}.
\end{aligned}$$

This ends the proof. □

We may now handle the questions referred to before Proposition 7.8. We will say that a root of unity is an nth root of unity for some $n \in \mathbf{N}^*$. By definition, the set $\mathbf{Q}(\mu_m)$ contains the mth roots of unity in $\mathbf{C}$. There are m such roots of unity. The following result shows that if, if m is even, then $\mathbf{Q}(\mu_m)$ contains no other roots of unity and, if m is odd, then $\mathbf{Q}(\mu_m)$ contains the mth roots of unity and m other roots roots of unity.

Theorem 7.8 *If m is a positive integer, then the number of roots of unity in $\mathbf{Q}(\mu_m)$ is $[2, m]$.*

PROOF In this proof ζ denotes a primitive mth root of unity; then $-\zeta \in \mathbf{Q}(\mu_m)$ and, by Theorem 7.5, it has order $2m$, if m is odd. This implies that the set $\mu_{[2,m]} \subset \mathbf{Q}(\mu_m)$. We have shown that $\mathbf{Q}(\mu_m)$ contains $\mu_{[2,m]}$. Let us show that $\mathbf{Q}(\mu_m)$ contains no other roots of unity.

We claim that there is a largest r, which we note $\bar{r}$, for which $\mathbf{Q}(\mu_m)$ contains a primitive rth root of unity. If $\mathbf{Q}(\mu_m)$ contains a primitive rth root of unity, then $\mu_r \subset \mathbf{Q}(\mu_m)$, which implies that $\mathbf{Q}(\mu_r) \subset \mathbf{Q}(\mu_m)$ and

$$[\mathbf{Q}(\mu_m) : \mathbf{Q}] = [\mathbf{Q}(\mu_m) : \mathbf{Q}(mu_r)]\mathbf{Q}(\mu_r)][\mathbf{Q}(\mu_r : \mathbf{Q}] \Longrightarrow \phi(m) \geq \phi(r).$$

Now, using Corollary 7.6, we see that there is a largest r for which $\mathbf{Q}(\mu_m)$ contains a primitive rth root of unity.

Suppose now that x is a nth root of unity belonging to $\mathbf{Q}(\mu_m)$ and y a primitive $\bar{r}$th root of unity. From Corollary 7.3, there is a power a of x such that $o(x^a y) = [m, \bar{r}]$. Since $x^a y \in \mathbf{Q}(\mu_m)$, the definition of $\bar{r}$ implies that $[n, \bar{r}] \leq \bar{r}$. It follows that $[n, \bar{r}] = \bar{r}$ and $n|\bar{r}$. Finally, every root of unity belongs to $\mu_{\bar{r}}$.

Let us now show that $\bar{r} = [2, m]$. As ζ is an mth root of unity, from what we have just seen, m divides $\bar{r}$. Let $\bar{r} = ms$. Using Proposition 7.9, we have

$$\phi(\bar{r}) = \phi(ms) = \frac{\phi(m)\phi(s)(m, s)}{\phi((m, s))} \geq \phi(m)\phi(s).$$

Now, as $m|\bar{r}$, we must have $\mathbf{Q}(\mu_m) \subset \mathbf{Q}(\mu_{\bar{r}})$. Given that $\mathbf{Q}(\mu_m)$ contains a primitive $\bar{r}$th root of unity, we also have $\mathbf{Q}(\mu_{\bar{r}}) \subset \mathbf{Q}(\mu_m)$ and so $\mathbf{Q}(\mu_m) = \mathbf{Q}(\mu_{\bar{r}})$. This implies that

$$\phi(m) = \phi(\bar{r}) \Longrightarrow 1 \geq \phi(s) \Longrightarrow \phi(s) = 1 \Longrightarrow s = 1 \text{ or } s = 2,$$

and so $\bar{r} = m$ or $\bar{r} = 2m$. If m is even, then $\phi(2m) = 2\phi(m) > \phi(m)$, so $\bar{r} = m$; on the other hand, if m is odd, then $-\zeta$ has order $2m$, so $\bar{r} \geq 2m$, and so $\bar{r} = 2m$. We have shown that $\bar{r} = [2, m]$.

To conclude, we have shown that the set of roots of unity belonging to $\mathbf{Q}(\mu_m)$ contains $\mu_{[2,m]}$ and is contained in $\mu_{[2,m]}$. This implies that this set is $\mu_{[2,m]}$. □

Corollary 7.7 *If $m \neq n$, then $\mathbf{Q}(\mu_m) = \mathbf{Q}(\mu_n)$ if and only if n is odd and $m = 2n$, or m is odd and $n = 2m$.*

PROOF If m is even, then $\mathbf{Q}(\mu_m)$ has m roots of unity. If $\mathbf{Q}(\mu_m) = \mathbf{Q}(\mu_n)$, then $\mathbf{Q}(\mu_n)$ also has m roots of unity. If n is even, then $\mathbf{Q}(\mu_n)$ has n roots of unity, so $m = n$, a contradiction. It follows that n is odd and $\mathbf{Q}(\mu_n)$ has $2n$ roots of unity. Thus we have $m = 2n$.

If m is odd, then $\mathbf{Q}(\mu_m)$ has $2m$ roots of unity. If $\mathbf{Q}(\mu_m) = \mathbf{Q}(\mu_n)$, then $\mathbf{Q}(\mu_n)$ also has $2m$ roots of unity. If n is odd, then $\mathbf{Q}(\mu_n)$ has $2n$ roots of unity, so $m = n$, a contradiction. It follows that n is even and has n roots of unity. Thus we have $2m = n$. □

7.5 Cyclotomic extensions of finite fields

We have looked in some detail at cyclotomic extensions of $\mathbf{Q}$. We will now consider cyclotomic extensions of finite fields. Being finite extensions of finite fields such extensions are Galois extensions (Proposition 3.1, Corollary 5.1). We will begin with a preliminary result, which is interesting in its own right. We recall that the cardinal of a finite field has the form p^k, where p is a prime number and k a positive integer.

Theorem 7.9 *Let F be a finite field, with $|F| = p^k$, and E a finite extension of F of degree n. Then the Galois group $G = Gal(E/F)$ is cyclic and generated by the Frobenius automorphism $Fr : x \longmapsto x^{p^k}$.*

PROOF To simplify the notation, let us write q for p^k. First we show that the mapping Fr is indeed an automorphism. Fr is clearly linear. If $x^q = 0$, then $x = 0$, because $x^q = x$, for all $x \in F$, so Fr is injective. An endomorphism of a finite-dimensional vector space is also surjective, so Fr is a bijective endomorphism of E. Finally, $(xy)^q = x^q y^q$, so Fr is an automorphism of E. As $x^q = x$, for all $x \in F$, $\mathrm{Fr} \in G$.

If $x \in E$, then $x^{q^n} = x$, which implies that $o(\mathrm{Fr}) \leq n$. However, if $\bar{x}$ is a generator of E^*, then $\bar{x}^s \neq \bar{x}$, for any $s < q^n$, and so $o(\mathrm{Fr}) = n$. Now, $|G| = [E : F] = n$, therefore G is cyclic with generator Fr. □

Now we turn to cyclotomic extensions of $\mathbf{F}_p$. (As usual we suppose that p and n are coprime.) From the previous theorem the Galois group of a cyclotomic extension $\mathbf{F}_p(\mu_n)$ of $\mathbf{F}_p$ must be cyclic. We are interested in finding a generator of this group in $\mathbf{Z}_n^\times$. As the Frobenius mapping Fr defined on E maps every element x of $\mathbf{F}_p(\mu_n)$ to x^p, we have $\phi(Fr) = [p]$, where ϕ is the mapping defined in Theorem 7.4. Hence we have

Proposition 7.10 *The image of the Galois group $G = Gal(\mathbf{F}_p(\mu_n)/\mathbf{F}_p)$ in $\mathbf{Z}_n^\times$ under the mapping ϕ is generated by the congruence class $[p]$, so the cardinal of G is the order of $[p]$ in $\mathbf{Z}_n^\times$.*

Exercise 7.6 *Find the value of the following degrees :*

$$[\mathbf{F}_3(\mu_7) : \mathbf{F}_3] \qquad [\mathbf{F}_5(\mu_4) : \mathbf{F}_5] \qquad [\mathbf{F}_7(\mu_{10}) : \mathbf{F}_7].$$

7.6 Quadratic and cyclotomic extensions

An easy calculation shows that

$$(e^{\frac{2\pi i}{5}} - e^{\frac{4\pi i}{5}} - e^{\frac{6\pi i}{5}} + e^{\frac{8\pi i}{5}})^2 = 5,$$

which implies that the expression between the brackets is a square root of 5. As this expression is an element of the cyclotomic field $\mathbf{Q}(\mu_5)$ the quadratic extension $\mathbf{Q}(\sqrt{5})$ of the rationals is contained in the cyclotomic field $\mathbf{Q}(\mu_5)$. The goal of this section is to generalize this by showing that any quadratic extension of the rationals is included in some cyclotomic field. In fact, we may say more. A quadratic extension E of $\mathbf{Q}$ is abelian, i.e., the Galois group $Gal(E/\mathbf{Q})$ is abelian, since its cardinal is 2 (see Theorems 3.5, 5.1 and 6.1). The Kronecker-Weber Theorem, which we will prove further on, states that any finite abelian extension of $\mathbf{Q}$ is included in some cyclotomic field.

We begin with Gauss sums. Let ζ be a primitive pth root of unity, where p is an odd prime number. We define the *Gauss sum* by

$$\tau_p = \sum_{k=1}^{p-1} \left(\frac{k}{p}\right) \zeta^k,$$

where $\left(\frac{\cdot}{\cdot}\right)$ denotes the Legendre symbol. Then

Proposition 7.11 *We have*

$$\tau_p^2 = (-1)^{\frac{p-1}{2}} p.$$

PROOF First

$$\tau_p^2 = \sum_{k,l=1}^{p-1} \left(\frac{k}{p}\right) \left(\frac{l}{p}\right) \zeta^{k+l}.$$

If we fix $k \in \{1, \ldots, p-1\}$, then the set $\{k \cdot 1, k \cdot 2, \ldots, k \cdot (p-1)\}$ is a set of representatives of the nonzero congruence classes of $\mathbf{Z}_p$, hence we can write

$$\begin{aligned} \tau_p^2 &= \sum_{k=1}^{p-1} \sum_{m=1}^{p-1} \left(\frac{k}{p}\right) \left(\frac{km}{p}\right) \zeta^{k+km} \\ &= \sum_{k=1}^{p-1} \sum_{m=1}^{p-1} \left(\frac{k^2}{p}\right) \zeta^{k+km} \left(\frac{m}{p}\right) \\ &= \sum_{k=1}^{p-1} \sum_{m=1}^{p-1} \left(\frac{m}{p}\right) \zeta^{k+km}, \end{aligned}$$

because $\left(\frac{k^2}{p}\right) = 1$. Rearranging the terms, we obtain

$$\tau_p^2 = \sum_{m=1}^{p-1} \left(\sum_{k=1}^{p-1} \zeta^{k(1+m)} \right) \left(\frac{m}{p}\right).$$

If $m \neq p-1$, then the sequence $\zeta^{1+m}, \zeta^{2(1+m)}, \ldots, \zeta^{(p-1)(1+m)}$ runs through all the pth roots of unity with the exception of 1, hence their sum has the value -1. On the other hand, if $m = p-1$, then the sum of the members of the sequence has the value $p-1$. Therefore

$$\tau_p^2 = -\sum_{m=1}^{p-2} \left(\frac{m}{p}\right) + (p-1)\left(\frac{p-1}{p}\right) = \sum_{m=1}^{p-2} \left(\frac{m}{p}\right) + p\left(\frac{-1}{p}\right) = p\left(\frac{-1}{p}\right),$$

because the number of nonzero squares in $\mathbf{Z}_p$ is the same as that of the nonsquares. The result follows from the fact that $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$. $\square$

Corollary 7.8 *We have*

$$\sqrt{(-1)^{\frac{p-1}{2}} p} \in \mathbf{Q}(\mu_p).$$

PROOF τ_p is a square root of $\tau_p^2 = (-1)^{\frac{p-1}{2}} p$ and $\tau_p \in \mathbf{Q}(\zeta) = \mathbf{Q}(\mu_p)$. $\square$

We now consider the relation between quadratic and cyclotomic extensions of $\mathbf{Q}$.

Proposition 7.12 *Let p be an odd prime number. Then the field $\mathbf{Q}(\mu_p)$ contains a unique quadratic extension of $\mathbf{Q}$, namely*

$$\mathbf{Q}\left(\sqrt{(-1)^{\frac{p-1}{2}}p}\right).$$

(If $p \equiv 1(mod\, 4)$, then $(-1)^{\frac{p-1}{2}}p = p$ and if $p \equiv 3(mod\, 4)$, then $(-1)^{\frac{p-1}{2}}p = -p$.)

PROOF Theorem 7.7 ensures that $G = Gal(\mathbf{Q}(\mu_p)/\mathbf{Q})$ is cyclic of order $p-1$, hence contains a unique subgroup H of order $\frac{p-1}{2}$. Let K be a field intermediate between $\mathbf{Q}$ and $\mathbf{Q}(\mu_p)$ such that $[K:\mathbf{Q}] = 2$. By Theorem 5.1, $\mathbf{Q}(\mu_p)$ is a Galois extension of $\mathbf{Q}$. Consequently, Proposition 5.3 ensures that $\mathbf{Q}(\mu_p)$ is a Galois extension of K. Thus, Theorem 6.1 entails that $Gal(\mathbf{Q}(\mu_p)/K)$ is a subgroup of G of order $\frac{p-1}{2}$. From the unicity of H, we have $H = Gal(\mathbf{Q}(\mu_p)/K)$. Theorem 6.4 now implies that $K = \mathcal{F}(H)$. We have shown that $\mathbf{Q}(\mu_p)$ contains a unique quadratic extension. To conclude the proof it suffices to notice that $\mathbf{Q}\left(\sqrt{(-1)^{\frac{p-1}{2}}p}\right)$ is a quadratic extension of $\mathbf{Q}$ contained in $\mathbf{Q}(\mu_p)$, by Corollary 7.8. □

For the moment we have only seen that quadratic extensions of a certain form are included in a cyclotomic extension of $\mathbf{Q}$. This is not difficult to extend. First let us suppose that $p \equiv 1(\text{mod } 4)$ and consider $-p$. We may write $\sqrt{-p} = i\sqrt{p}$. Then, using Proposition 7.6, we obtain

$$\mathbf{Q}(\sqrt{-p}) = \mathbf{Q}(i\sqrt{p}) \subset \mathbf{Q}(i)\mathbf{Q}(\sqrt{p}) \subset \mathbf{Q}(\mu_4)\mathbf{Q}(\mu_p) = \mathbf{Q}(\mu_{[4,p]}) = \mathbf{Q}(\mu_{4p}).$$

If $p \equiv 3(\text{mod } 4)$, then

$$\mathbf{Q}(\sqrt{p}) = \mathbf{Q}(i\sqrt{-p}) \subset \mathbf{Q}(i)\mathbf{Q}(\mu_p) = \mathbf{Q}(\mu_{4p}).$$

We have considered odd primes. What can we say about the prime 2? We claim that $\mathbf{Q}(\sqrt{2})$ and $\mathbf{Q}(\sqrt{-2})$ are included in $\mathbf{Q}(\mu_8)$. First we notice that $\zeta = e^{i\pi}$ is a primitive 8th root of unity. Also, $\zeta^7 = \zeta^{-1}$. Hence, $\zeta + \zeta^{-1}$ is an element of $\mathbf{Q}(\mu_8)$. However, this sum has the value $\sqrt{2}$. It follows that $\mathbf{Q}(\sqrt{2}) \subset \mathbf{Q}(\mu_8)$.

Now, $\sqrt{-2} = i\sqrt{2}$ and $i, \sqrt{2} \in \mathbf{Q}(\mu_8)$, therefore $\sqrt{-2} \in \mathbf{Q}(\mu_8)$ and it follows that $\mathbf{Q}(\sqrt{-2}) \subset \mathbf{Q}(\mu_8)$.

Theorem 7.10 *Every quadratic extension of the rationals is included in some cyclotomic extension.*

PROOF We have seen that, if E is a quadratic extension of the rationals, then there is a square-free integer d such that $E = \mathbf{Q}(\sqrt{d})$ (Theorem 3.5). If $d = \pm p_1 \cdots p_k$, where the p_i are distinct primes, then

$$\mathbf{Q}(\sqrt{d}) = \mathbf{Q}\left(\sqrt{\pm p_1}\sqrt{p_2}\cdots\sqrt{p_k}\right) \subset \mathbf{Q}(\sqrt{\pm p_1})\mathbf{Q}(\sqrt{p_2})\cdots\mathbf{Q}(\sqrt{p_k}).$$

However, we have just seen that, if p is a prime number, there is an integer $n \geq 2$ such that $\mathbf{Q}(\sqrt{p}) \subset \mathbf{Q}(\mu_n)$ and the same applies for $-p$. Hence, there are integers $n_i \geq 2$ such that

$$\mathbf{Q}(\sqrt{d}) \subset \mathbf{Q}(\mu_{n_1})\mathbf{Q}(\mu_{n_2})\cdots\mathbf{Q}(\mu_{n_k}) = \mathbf{Q}(\mu_{[n_1,n_2,\ldots,n_k]}).$$

This ends the proof. □

Exercise 7.7 *Find a condition on d which ensures that $\mathbf{Q}(\sqrt{d}) \subset \mathbf{Q}(\mu_d)$.*

Remark We have seen that the square root of an integer lies in some cyclotomic extension of $\mathbf{Q}$. A natural question arises, namely, if p is an odd prime, does a pth root of an integer necessarily lie in some cyclotomic extension of $\mathbf{Q}$. In fact, this is not in general true. Let $\alpha = \sqrt[p]{2}$, where p is an odd prime and ζ a primitive nth root of unity for some n. The Galois group $G = Gal(\mathbf{Q}(\zeta)/\mathbf{Q})$ is abelian. If $\alpha \in \mathbf{Q}(\zeta)$, then $\mathbf{Q}(\alpha)$ is a subfield of $\mathbf{Q}(\zeta)$ and the Galois group $G' = Gal(\mathbf{Q}(\zeta)/\mathbf{Q}(\alpha))$ is normal in G, because G' is a subgroup of the abelian group G. This implies that $\mathbf{Q}(\alpha)$ is a normal extension of $\mathbf{Q}$. However, this is not so, because lies in $\mathbf{Q}(\alpha)$, but the other roots of $f(X) = -2 + X^p$ do not. It follows that $\alpha \notin \mathbf{Q}(\zeta)$.

7.7 Orbites of the Galois group action

In Section 7.1 we introduced the action of a Galois group of a separable polynomial f on its roots. In this section we aim to look more closely at this. In particular, we will show that there is an interesting relation between the orbits of the action and the decomposition into irreducible polynomials of the polynomial f. We consider a separable polynomial $f \in F[X]$, with set of roots $A = \{\alpha_1, \ldots, \alpha_n\}$ in a splitting field E and we note Φ the action of the Galois group $G = Gal(E/F)$ on A. We write $O_1, \ldots, O_r$ for the orbits of Φ and set $n_i = |O_i|$.

Proposition 7.13 *Let S be a subset of A and the polynomial $f_S \in E[X]$ be defined by*

$$f_S(X) = \prod_{\alpha_i \in S} (-\alpha_i + X).$$

If S^G is the subset of S fixed by G, i.e., the subset of elements $x \in A$ for which $\sigma(x) = x$ for all $\sigma \in G$, then $f_S \in F[X]$ if and only if $S^G = S$.

PROOF Suppose that $f_S \in F[X]$ and take $\sigma \in G$. Let

$$\tilde{f}_S(X) = \prod_{\alpha_i \in S} (-\sigma(\alpha_i) + X).$$

The coefficients b_k of this polynomial are expressions, i.e., sums of products, of the $\sigma(\alpha_i)$. As σ is an automorphim, a coefficient b_k is the image under σ of the corresponding sum of products of the α_i, i.e., $b_k = \sigma(a_k)$. As σ fixes the elements of F, $a_k = b_k$, for all k and so $\tilde{f}_S = f_S$. This implies that σ fixes S. As this is so for all $\sigma \in G$, we have $S^G = S$.

Now suppose that $S^G = S$ and let σ be an element of G. As σ fixes S, $\tilde{f}_S = f_S$. However, this is so for all $\sigma \in G$, so the coefficients of f_S belong to the set of elements of E fixed by G, i.e., the field F (see Theorem 6.2). Hence $f_S \in F[X]$. □

Remark Let g be a monic, irreducible factor of the polynomial f. Then there is a subset S of A such that $g = f_S$. As $g \in F[X]$, by the previous proposition, we have $S^G = S$, which implies that S is a union of orbits of the action Φ.

Proposition 7.14 *Suppose that the polynomial f_S defined above is in $F[X]$. Then f_S is irreducible if and only if S is a minimal set fixed by G.*

PROOF Suppose that f_S is irreducible. If S' is strictly included in S and S' is fixed by G, then $f_{S'} \in F[X]$ and $f_{S'}|f$, with $\deg f_{S'} < \deg f_S$. This is a contradiction to the irreducibility of f_S. Hence S must be minimal.

Now suppose that S is a minimal set fixed by G. If f_S is not irreducible, then there exists $g \in F[X]$ which is monic, divides f_S and is such that $\deg g < \deg f_S$. There exists S' strictly included in S such that $g = f_{S'}$ and so S is not minimal, a contradiction. It follows that f_S is irreducible. $\square$

We may now prove the main result of this section.

Theorem 7.11 *If the separable polynomial $f \in F[X]$ has the decomposition into irreducible factors*

$$f = \lambda f_1 \cdots f_r,$$

where $\lambda \in F$ and the f_i are monic, then the action Φ has r orbits $O_1, \ldots, O_r$, with $\deg f_i = |O_i|$.

PROOF The minimal sets fixed by G are the orbits of Φ, therefore the monic irreducible factors of f are in one-to-one correspondence with the orbits and we have

$$f = \lambda f_{O_1} \cdots f_{O_r},$$

where $\lambda \in F$ and the polynomials f_{O_i} are monic, irreducible. The degree of f_{O_i} is $n_i = |O_i|$. $\square$

It is interesting to consider the case where $F = \mathbf{F}_p$. From Theorem 7.4 we know that, if E is a finite Galois extension of $\mathbf{F}_p$, then the Galois group $G = Gal(E/\mathbf{F}_p)$ is cyclic and generated by the Frobenius automorphism $\mathrm{Fr} : x \longmapsto x^p$. If we suppose that E is a splitting field of a separable polynomial $f \in \mathbf{F}_p[X]$, then the orbits of the action Φ defined above are of the form $O_i = \{\mathrm{Fr}^s(\alpha_j)\}_{s \in \mathbf{N}}$, for some α_j. If s' is the smallest index $s \geq 1$ such that $\mathrm{Fr}^s(\alpha_j) = \alpha_j$, then $s' = n_i - 1$ and $O_i = \{\alpha_j, \mathrm{Fr}(\alpha_j), \ldots, \mathrm{Fr}^{n_i-1}(\alpha_j)\}$, i.e., O_i is a cycle of Fr of length $n_i = \deg f_i$.

Chapter 8

Dedekind's reduction theorem

We recall that, if f is a polynomial in $\mathbf{Z}[X]$ and p a prime number, then we may define $\bar{f} \in \mathbf{F}_p[X]$ by replacing the coefficients of f by their congruence classes modulo p. The polynomial $\bar{f}$ so obtained is called the *reduction modulo* p of f. We will sometimes refer to $\bar{f}$ as a reduced polynomial. In this chapter we aim to establish an important relation between the Galois groups of f over $\mathbf{Q}$ and $\bar{f}$ over $\mathbf{F}_p$, which will enable us to find useful information about the former Galois group. We will need some preliminaries.

8.1 A basic result in module theory

We say that a module M over a ring R is *finitely generated* if there are $m_1, \ldots, m_s \in M$ such that every element $m \in M$ can be expressed in at least one way as

$$m = r_1 m_1 + \cdots + r_s m_s,$$

with the $r_i \in R$. The module M is *free* if it has a *basis*, i.e., a set U which has the properties:

- U is a generating set: every element $m \in M$ can be expressed as

  $$m = r_1 u_1 + \cdots + r_s u_s,$$

  with the $u_i \in U$ and the $r_i \in R$;

- U is an independant set:

  $$r_1 u_1 + \ldots + r_s u_s = 0 \Longrightarrow r_i = 0, \quad \text{for all } i.$$

Let M be a module over an integral domain R. If $x \in M$ and there exists $r \in R^*$ such that $rx = 0$, then we say that x is a *torsion element*. The set of torsion elements form a submodule of M, which we write tM. (Clearly tM is closed under scalar multiplication; if $rx = 0$ and $sx = 0$, then $rs(x + y) = 0$, so tM is closed under addition.) We say that M is *torsion-free* if $tM = \{0\}$ and *torsion* if $tM = M$. We now bring these ideas together.

Proposition 8.1 *Let R be principal ideal domain and M a finitely generated R-module. Then M has a finite basis if and only if M is torsion-free.*

We will give a proof of this result in Appendix E.

Exercise 8.1 *Show that a free module over an integral domain is torsion-free.*

8.2 Dedekind's lemma

In this section we present an important result due to Dedekind, which we will need further on in this chapter. Let G be a (multiplicative) semi-group and F a field. A *character* of G into F is a mapping from G into F which preserves multiplication and is not identically zero. We will write $\mathrm{Char}(G,F)$ for the set of characters from G into F. The set of all mappings from G into F, which we note F^G, can be given a vector space structure over F with the vector space operations defined pointwise. The following result is referred to as *Dedekind's lemma*.

Theorem 8.1 *The set of characters $Char(G,F)$ is a linearly independant subset of F^G.*

PROOF Let $n \geq 1$ and $\chi_1,\dots,\chi_n$ be distinct elements of $\mathrm{Char}(G,F)$. Suppose that

$$a_1\chi_1 + \cdots + a_n\chi_n = 0, \tag{8.1}$$

where $a_1,\dots,a_n \in F$. We will show by induction that $a_1 = \cdots = a_n = 0$.

For $n = 1$, let $x \in G$ be such that $\chi_1(x) \neq 0$. Then $a_1\chi_1(x) = 0$ implies that $a_1 = 0$. Now suppose that $n > 1$ and that the result is true up to $n-1$. Since $\chi_1 \neq \chi_n$, there exists $y \in G$ such that $\chi_1(y) \neq \chi_n(y)$. Evaluating equation (8.1) at x and yx, where x is an arbitrary member of G, we obtain

$$a_1\chi_1(x) + \cdots + a_n\chi_n(x) = 0 \tag{8.2}$$

and

$$a_1\chi_1(y)\chi_1(x) + \cdots + a_n\chi_n(y)\chi_n(x) = 0. \tag{8.3}$$

We now multiply equality (8.2) by $\chi_n(y)$ and subtract it from equality (8.3). Bearing in mind that the element x was chosen arbitrarily, we obtain

$$a_1(\chi_1(y) - \chi_n(y))\chi_1 + \cdots + a_{n-1}(\chi_{n-1}(y) - \chi_n(y))\chi_{n-1} = 0.$$

From the induction hypothesis we deduce that all the coefficients of the linear combination on the left hand side of the equality have the value 0. In particular, $a_1(\chi_1(y) - \chi_n(y)) = 0$. As $\chi_1(y) - \chi_n(y) \neq 0$, we must have $a_1 = 0$. However, now equation (8.1) is reduced to $n-1$ terms and so, using the induction hypothesis again, we obtain $a_2 = \cdots = a_n = 0$. □

Remark A character is not required to have only nonzero values; it is sufficient that it has at least one nonzero value. However, if G is a monoïd, then the image of an invertible element is nonzero. In particular, if G is a group, then the image of G under a character is a subgroup of the multiplicative subgroup F^* of F.

Corollary 8.1 *A set of distinct automorphisms $S = \{\sigma_1,\dots,\sigma_n\}$ on a field F is independant.*

PROOF An automorphism σ of a field F, when restricted to the multiplicative group F^* becomes a group automorphism, hence σ is a character of the group F^* into the field F. □

8.3 Splitting fields of polynomials in $\mathbf{Z}[X]$

In this section (and the following sections) we aim to consider certain properties of splitting fields of monic polynomials belonging to $\mathbf{Z}[X]$. Let $f \in \mathbf{Z}[X]$ be monic, $A = \{\alpha_1,\dots,\alpha_n\}$ the set of roots of f in $\mathbf{C}$ and E a splitting field of f contained in $\mathbf{C}$. We may consider f as a polynomial in $\mathbf{Q}[X]$. Then, from Proposition 2.2, we have

$$E = \mathbf{Q}[\alpha_1,\dots,\alpha_n],$$

i.e., E is composed of the polynomials in the α_i with coefficients in $\mathbf{Q}$. We set

$$D = \mathbf{Z}[\alpha_1, \ldots, \alpha_n].$$

Then D is a subring of E and also a $\mathbf{Z}$-module.

Proposition 8.2 *The $\mathbf{Z}$-module D is finitely generated and torsion-free, therefore has a finite basis $U = (u_1, \ldots, u_r)$.*

PROOF If $f(X) = \sum_{i=0}^{n} a_i X^i$ and $\alpha \in A$, then $\alpha^n = -\sum_{i=0}^{n-1} a_i \alpha^i$, therefore D is generated by the elements $\alpha_1^{e_1}\alpha_2^{e_2}\cdots\alpha_n^{e_n}$, with $0 \le e_i \le n-1$. Thus D is finitely generated.

If $am = 0$, with $a \neq 0$, then considering $D \subset E$, we have

$$a^{-1}(am) = (a^{-1}a)m = 0 \Longrightarrow m = 0.$$

Thus D is torsion-free.

As $\mathbf{Z}$ is a P.I.D. and D is finitely generated and torsion-free, we may apply Proposition 8.1 to obtain the existence of a finite basis $U = (u_1, \ldots, u_r)$. □

A natural question now arises: Can we find a natural basis of the $\mathbf{Q}$-vector space E? In fact, this is the case.

Proposition 8.3 *The basis $U = (u_1, \ldots, u_r)$ of D is a basis of the $\mathbf{Q}$-vector space $E = \mathbf{Q}[\alpha_1, \ldots, \alpha_n]$.*

PROOF E is the fraction field of D, so, by Corollary E.1, U is a basis of the $\mathbf{Q}$-vector space E.□

8.4 Splitting fields of reduced polynomials

Our aim in this section is to find a splitting field of a reduced polynomial.

Proposition 8.4 *Let p be a prime number and M a maximal ideal of D which contains the proper ideal Dp. If $f \in \mathbf{Z}[X]$ and is monic, then $K = D/M$ is a splitting field of $\bar{f}$, the reduction modulo p of f.*

PROOF It is clear that the characteristic of K is p, hence K is an extension of $\mathbf{F}_p$. Let us write π for the standard projection of D on K. If $U = (u_r)$ is the basis found in the preceding section and

$$x = a_1u_1 + \cdots + a_ru_r, \qquad \text{with } a_i \in \mathbf{Z},$$

then

$$\pi(x) = \pi(a_1)\pi(u_1) + \cdots + \pi(a_r)\pi(u_r).$$

We may identify the image of π restricted to $\mathbf{Z}$ with $\mathbf{F}_p$, because the kernel of this mapping is $\mathbf{Z} \cap M = \mathbf{Z}p$. Thus we may consider the $\pi(a_i)$ belonging to $\mathbf{F}_p$. Therefore $\{\pi(u_i)\}$ is a generating set of K over $\mathbf{F}_p$ and K is a finite extension of $\mathbf{F}_p$. We next notice that $\bar{f}$ splits over K:

$$\bar{f}(X) = \tilde{\pi}(f(X)) = \tilde{\pi}\Big(\prod_{i=1}^{n}(-\alpha_i + X)\Big) = \prod_{i=1}^{n}(-\pi(\alpha_i) + X),$$

where $\tilde{\pi}$ is the mapping of $\mathbf{Z}[X]$ into $\mathbf{F}_p[X]$ which corresponds to π and the α_i are the roots of f. In addition,

$$K = \pi(D) = \pi(\mathbf{Z}[\alpha_1, \ldots, \alpha_n]) = \mathbf{F}_p[\pi(\alpha_1), \ldots, \pi(\alpha_n)] = \mathbf{F}_p(\pi(\alpha_1), \ldots, \pi(\alpha_n)),$$

because $\mathbf{F}_p[\pi(\alpha_1), \ldots, \pi(\alpha_n)]$ is a field. It follows that K is a splitting field of $\bar{f}$. $\square$

The mapping $\pi : D \longrightarrow K$ is a surjective ring homomorphism and the roots of $\bar{f}$ are the images of the roots of f. In fact, we may generalize this.

Proposition 8.5 *If $\phi : D \longrightarrow K$ is a ring homomorphism, then ϕ restricted to $\mathbf{Z}$ is the same for all $\phi \in Hom(D, K)$. Also, ϕ is surjective and the images of the roots of f are roots of $\bar{f}$.*

PROOF That ϕ restricted to $\mathbf{Z}$ is the same for all $\phi \in Hom(D, K)$ follows from the fact that $\phi(1) = 1 + M$.

Now we observe that

$$\tilde{\phi}(f(X)) = \tilde{\phi}\left(\prod_{i=1}^{n}(-\alpha_i + X)\right) = \prod_{i=1}^{n}(-\phi(\alpha_i) + X),$$

hence the $\phi(\alpha_i)$ are the roots of $\bar{f}$.

Finally let us consider the surjectivity. We have

$$\phi(D) = \phi(\mathbf{Z}[\alpha_1, \ldots, \alpha_n]) = \mathbf{F}_p[\phi(\alpha_1), \ldots, \phi_n(\alpha_n)].$$

Also, $\mathbf{F}_p[\phi(\alpha_1), \ldots, \phi(\alpha_n)]$ is a subset of K and also a splitting field of $\bar{f}$ (Proposition 2.2), therefore $\mathbf{F}_p[\phi(\alpha_1), \ldots, \phi(\alpha_n)]$ is isomorphic to K. It follows that $\phi(D) = K$. $\square$

Remark This generalization, which is interesting in its own right, will be used in a proof a little further on, namely that of Proposition 8.7.

8.5 Resultants and discriminants

In the following we will use the discriminant of a polynomial, which is useful in determining whether an extension is separable. However, in order to study this concept it is useful to introduce another concept, namely the resultant of two polynomials.There is an important relation between the discriminant of a polynomial and the resultant of a polynomial and its derivative. Here we will only introduce the subject. Further on we will handle it in more detail.

Resultants

We fix $m, n \in \mathbf{N}^*$. Let F be a field, $f \in F_m[X]$, with coefficients $a_0, \ldots, a_m$ and $g \in F_n[X]$, with coefficients $b_0, \ldots, b_n$. We define the square $n + m$ *Sylvester matrix* $S_{m,n}(f, g)$ (or $S(f, g)$), if m and n are understood) as follows:

$$S_{m,n}(f,g) = \begin{bmatrix} a_m & a_{m-1} & a_{m-2} & \ldots & 0 & 0 & 0 \\ 0 & a_m & a_{m-1} & \ldots & 0 & 0 & 0 \\ \vdots & \vdots & \vdots & & & & \\ 0 & 0 & 0 & \ldots & a_1 & a_0 & 0 \\ 0 & 0 & 0 & \ldots & a_2 & a_1 & a_0 \\ b_n & b_{n-1} & b_{n-2} & \ldots & 0 & 0 & 0 \\ 0 & b_n & b_{n-1} & \ldots & 0 & 0 & 0 \\ \vdots & \vdots & \vdots & & & & \\ 0 & 0 & 0 & \ldots & b_1 & b_0 & 0 \\ 0 & 0 & 0 & \ldots & b_2 & b_1 & b_0 \end{bmatrix}$$

We obtain $S_{m,n}(f,g)$ by shifting the line vector of the coefficients of f successively to the right by $0,1,\ldots,n-1$ steps and the vector line of the coefficients of g successively to the right by $0,1,\ldots,m-1$ steps and then filling in the remaining places with 0.

Remark If $0 \leq \deg f = k < m$, then we have $a_m = a_{m-1} = \cdots = a_{k+1} = 0$ and if $f = 0$, then $a_i = 0$, for all i. We have an analogous situation if $\deg g \neq n$.

Here is an example. With $m = 3$ an $n = 2$, we have

$$S_{m,n}(f,g) = \begin{bmatrix} a_3 & a_2 & a_1 & a_0 & 0 \\ 0 & a_3 & a_2 & a_1 & a_0 \\ b_2 & b_1 & b_0 & 0 & 0 \\ 0 & b_2 & b_1 & b_0 & 0 \\ 0 & 0 & b_2 & b_1 & b_0 \end{bmatrix}$$

The *resultant* of f and g, which we note $R_{m,n}(f,g)$, (or $R(f,g)$, if m and n are understood) is the determinant $|S_{m,n}(f,g)|$. Clearly,

$$R_{n,m}(g,f) = (-1)^{mn} R_{m,n}(f,g).$$

Remark We may consider the a_i and b_j as variables. In this way we obtain a mapping from $F^{m+1} \times F^{n+1}$ into F, which is mn-homogeneous.

Discriminants

Let $f(X) = \sum_{i=0}^{m} a_i X^i$ a polynomial with coefficients in a field F. We suppose that the degree m of f is greater than 1 and that f has the roots $\xi_1, \ldots, \xi_m$ in some splitting field E. The *discriminant* of f is defined by

$$\Delta(f) = a_m^{2m-2} \prod_{1 \leq i < j \leq m} (\xi_i - \xi_j)^2.$$

From the theorem which follows this definition is unambiguous: it does not depend on the splitting field chosen.

It is useful to notice that $\Delta(f)$ belongs to F. Indeed, the multivariate polynomial $A = a_m^{2m-2} \prod_{1 \leq i < j \leq m} (X_i - X_j)^2$ is a symmetric polynomial in $F[X_1, \ldots, X_n]$. Consequently, from Corollary B.1, $\Delta(f) \in F$. Using the same corollary, we may also say that, if $f \in R[X]$, where R is an integral domain, then $\Delta(f) \in R$.

The following result links the resultant and the discriminant.

Theorem 8.2 *If char* $F = 0$ *or char* $F = p > 0$ *and* $p \not| m$, *where* $\deg f = m$, *then*

$$\Delta(f) = (-1)^{m(m-1)/2} a_m^{-1} R_{m,m-1}(f, f').$$

Remark The polynomial f has a multiple root if and only if $\Delta(f) = 0$. From the above formula, we see that we are able to determine the existence of a multiple root only taking into account the coefficients of f. We should also notice that the formulas show that the discriminant belongs to the field F.

8.6 The Galois group of a polynomial and of its reduction

In this section we aim to show that the Galois group of the reduction of a monic polynomial $f \in \mathbf{Z}[X]$ may be considered as a subgroup of the Galois group of f. This will give us information about the Galois group of f. We begin with a simple proposition, which we can prove using discriminants, thus justifying their introduction in the last section.

Proposition 8.6 *Let $f \in \mathbf{Z}[X]$ be a monic polynomial, p a prime number and $\bar{f} \in \mathbf{F}_p[X]$ the reduction modulo p of f. Then, if $\bar{f}$ is strongly separable, then so is f.*

PROOF If $M = (m_{ij}) \in \mathcal{M}_n(\mathbf{Z})$ and $\bar{M} = (\bar{m}_{ij}) \in \mathcal{M}_n(\mathbf{F}_p)$, where $\bar{m}_{ij}$ is the congruence class of m_{ij} modulo p, then the $\overline{\det M} = \det \bar{M}$. Hence, if $\deg f = n$, then

$$R_{n,n-1}(f, f') = 0 \Longrightarrow R_{n,n-1}(\bar{f}, \bar{f}') = 0$$

and it follows that, if $\bar{f}$ is strongly separable, then so if f. □

We suppose from here on that $\bar{f}$ is strongly separable and that E, D and K are defined as in Sections 7.3 and 7.4. We define a right action Ψ of $G = Gal(E/\mathbf{Q})$ on $Hom(D, K)$, the set of ring homomorphisms of D into K, by

$$\Psi(\sigma, \phi) = \sigma.\phi = \phi \circ \sigma_{|D},$$

for all $\sigma \in G$ and $\phi \in Hom(D, K)$. (The action is defined, because $\sigma(D) \subset D$.)

Proposition 8.7 *The action Ψ is free and transitive.*

PROOF Let A be the set of roots of f. If $\phi \circ \sigma$ restricted to D is equal to ϕ, then $(\phi \circ \sigma)_{|A} = \phi_{|A}$. In addition, $\sigma(A) \subset A$, so we may write

$$\phi_{|A} = (\phi \circ \sigma)_{|A} = \phi_{|A} \circ \sigma_{|A}.$$

From Proposition 8.5, $\phi_{|A}$ is surjective from A into $\bar{A}$, the set of roots of $\bar{f}$. As $\bar{f}$ is strongly separable, so is f (Proposition 8.6), hence

$$|A| = \deg f = \deg \bar{f} = |\bar{A}|.$$

It follows that $\phi_{|A}$ is a bijection of A on $\bar{A}$ and so invertible. We deduce that $\sigma_{|A}$ is the identity on A, which implies that σ is the identity of the Galois group of f. We have established that Ψ is free.

We now consider the transitivity. Let us fix $\phi \in Hom(D, K)$ and note N the cardinal of the Galois group $G = Gal(E/\mathbf{Q})$, where E is a fixed splitting field of f. We write O for the orbit of ϕ:

$$O = \{\sigma.\phi : \sigma \in G\}.$$

As the action Ψ is free, we have $|O| = N$. We aim to show that $O = Hom(D, K)$. Let us write $\phi_1, \dots, \phi_N$ for the homomorphisms in O. If $O \neq Hom(D, K)$, then there exists $\phi_{N+1} \in Hom(D, K) \setminus O$. We may consider the homomorphisms as characters of the monoïde $(D, \cdot)$ into K. We have

$$N = |Gal(E/\mathbf{Q})| = [E : \mathbf{Q}] = \operatorname{rk} D.$$

(For the last equality see Proposition 8.3.) Hence there is a basis (u_i) of D whose cardinal is N. The system

$$\begin{array}{rcl}
x_1\phi_1(u_1)+\cdots+x_{N+1}\phi_{N+1}(u_1) & = & 0\\
\vdots \qquad \vdots \qquad \vdots \qquad \vdots & & \vdots\\
x_1\phi_1(u_N)+\cdots+x_{N+1}\phi_{N+1}(u_N) & = & 0
\end{array}$$

is composed of N equations and $N+1$ unknowns, therefore has a nonzero solution $(\lambda_1,\ldots,\lambda_{N+1})$. If $a\in D$ and $a=\sum_{j=1}^N a_ju_j$, then

$$\begin{array}{rcl}
\sum_{i=1}^{N+1}\lambda_i\phi_i(a) & = & \sum_{i=1}^{N+1}\lambda_i\phi_i\left(\sum_{j=1}^{N}a_ju_j\right)\\
 & = & \sum_{i=1}^{N+1}\lambda_i\sum_{j=1}^{N}a_j\phi_i(u_j)\\
 & = & \sum_{j=1}^{N}a_j\sum_{i=1}^{N+1}\lambda_i\phi_i(u_j)=0.
\end{array}$$

Therefore $\sum_{i=1}^{N+1}\lambda_i\phi_i(a)=0$, for all $a\in D$, which contredicts Dedekind's lemma (Theorem 8.1). It follows that $O=Hom(D,K)$ and therefore that the action Ψ is transitive. □

We may now prove the principal result of this section. This is particularly important, in that it often gives us important information concerning the Galois group of certain polynomials. It is often referred to as *Dedekind's Theorem.*

Theorem 8.3 *Let $f\in\mathbf{Z}[X]$ be monic and p a prime number. If $\bar f$, the reduction of f modulo p, is strongly separable, then there is an injective group homomorphism g of the Galois group of $\bar f$, $\bar G=Gal(K/\mathbf{F}_p)$, into the Galois group of f, $G=Gal(E/\mathbf{Q})$.*

PROOF As in Section 7.4, we note π the standard projection of D on K. Then $\bar\sigma\circ\pi\in Hom(D,K)$, for all $\bar\sigma$ in the Galois group $\bar G$. As the action Ψ of the previous proposition is free and transitive, there exists a unique $\tau\in G$ such that

$$\bar\sigma\circ\pi=\tau.\pi=\pi\circ\tau.$$

We define $g(\bar\sigma)=\tau$ and so obtain a mapping from $\bar G$ into G. In fact, g is an injective group homomorphism, as we now see. First,

$$\begin{array}{rcl}
\pi\circ g(\bar\sigma_1\circ\bar\sigma_2) & = & (\bar\sigma_1\circ\bar\sigma_2)\circ\pi \;=\; \bar\sigma_1\circ(\bar\sigma_2\circ\pi)\\
 & = & \bar\sigma_1\circ(\pi\circ g(\bar\sigma_2)) \;=\; (\bar\sigma_1\circ\pi)\circ g(\bar\sigma_2)\\
 & = & (\pi\circ g(\bar\sigma_1))\circ g(\bar\sigma_2) \;=\; \pi\circ(g(\bar\sigma_1)\circ g(\bar\sigma_2)).
\end{array}$$

As the action Ψ is free,

$$g(\bar\sigma_1\circ\bar\sigma_2)=g(\bar\sigma_1)\circ g(\bar\sigma_2),$$

i.e., g is a homomorphism. In addition,

$$g(\bar\sigma)=\mathrm{id}_G\Longrightarrow\bar\sigma\circ\pi=\pi.$$

Let $x \in K$. As π is surjective, there exists $y \in D$ such that $\pi(y) = x$, so $\bar{\sigma} \circ \pi(y) = \pi(y)$, i.e., $\pi(x) = x$. Hence, $\bar{\sigma} = \mathrm{id}_{\bar{G}}$. It follows that g is injective. □

Remark We have fixed the splitting field of f over $\mathbf{Q}$ (resp. $\bar{f}$ over $\mathbf{F}_p$) to obtain a given Galois group of f (resp. $\bar{f}$). Changing the splitting fields and thus the Galois groups does not of course affect the result above, because all Galois groups of a given polynomial over a certain field are isomorphic.

From the theorem which we have just proved, for a root α of f, we obtain the relation

$$\gamma(g(\bar{\sigma})(\alpha)) = \bar{\sigma}(\gamma(\alpha)),$$

where γ is the mapping π restricted to A. γ is an invertible function from A into $\bar{A}$, since $\bar{f}$ is strongly separable. Indeed, as a function from A into $\bar{A}$, γ is surjective and the fact that $\bar{f}$ is strongly separable ensures that A and $\bar{A}$ have the same cardinality. Thus on A we have

$$\gamma \circ g(\bar{\sigma}) = \bar{\sigma} \circ \gamma \Longrightarrow g(\bar{\sigma}) = \gamma^{-1} \circ \bar{\sigma} \circ \gamma.$$

From Section 7.7 we know that the Galois group $\bar{G} = Gal(K/\mathbf{F}_p)$ is generated by the Frobenius automorphism $Fr : x \longmapsto x^p$ and is composed of cycles whose length correspond to the degrees of the irreducible polynomials in the decomposition of the reduced polynomial $\bar{f}$. From the relation $g(\bar{\sigma}) = \gamma^{-1} \circ \bar{\sigma} \circ \gamma$, we obtain a permutation in the Galois group of $G = Gal(E/\mathbf{Q})$ with the same cycle structure. By varying the value of the prime p we may find sufficient permutations to characterize the Galois group of f.

Example If $f(X) = 3 + X + X^4 + X^6$, then the factorizations of the reductions of f modulo 2 and 3 are

$$\bar{f}(X) = (1+X)(1+X+X^2)(1+X+X^3) \quad \text{and} \quad \bar{f}(X) = X(2+X)(2+2X+2X^2+X^3+X^4).$$

The reductions have no multiple roots and so are strongly separable. Applying the theorem, we see that G has elements σ and τ such that $\sigma_{|A}$ is a permutation with the cycle structure $(1, 2, 3)$ (a product of a 2-cycle and a 3-cycle) and $\tau_{|A}$ a permutation with the cycle structure $(1, 1, 4)$ (a 4-cycle). Going a little further, we find that the reduction modulo 5 has the form

$$\bar{f}(X) = (3 + X)^2(2 + X + 3X^2 + 4X^3 + X^4)$$

This has a factor which is a square and hence a multiple root, so we cannot apply the theorem.

Chapter 9

Determination of the Galois group

In general, it is difficult to determine the Galois group of a polynomial. However, we can often find certain properties of the group. In some cases this may be enough to determine the group. We will mostly consider irreducible rational polynomials.

9.1 Inclusion in an alternating group A_n

We have seen that a Galois group G of a polynomial having n distinct roots may be considered as a subgroup of the permutation group S_n. It is natural to ask whether permutations of this group are even, i.e., if $G \subset A_n$. We will begin with a criterion applying to this question.

Proposition 9.1 *Let F be a field whose characteristic is not 2 and $f \in F[X]$ strongly separable of degree n. Then the Galois group G of f is isomorphic to a subgroup of A_n, the alternating group of order n, if and only if the discriminant of f, $\Delta(f)$, is a square in F.*

PROOF Let $A = \{\alpha_1, \dots, \alpha_n\}$ be the set of roots of f in a splitting field E of f and $\delta(f) = \prod_{1 \leq i < j \leq n}(\alpha_i - \alpha_j)$. As f is strongly separable, $\delta(f) \neq 0$. Also, $\delta(f) \in F(\alpha_1, \dots, \alpha_n)$ and $\delta(f)^2 = \Delta(f) \in F$. To shorten the notation let us write δ for $\delta(f)$ and Δ for $\Delta(f)$. Clearly, Δ is a square in F if and only if $\delta \in F$.

We now take $\sigma \in Gal(F(\alpha_1, \dots, \alpha_n)/F)$. If $\epsilon_\sigma = \pm 1$ is the sign of the permutation $\sigma = \sigma_{|A}$ of A, then

$$\sigma(\delta) = \prod_{1 \leq i < j \leq n} (\alpha_{\sigma(i)} - \alpha_{\sigma(j)}) = \epsilon_\sigma \prod_{1 \leq i < j \leq n} (\alpha_i - \alpha_j) = \epsilon_\sigma \delta,$$

hence $\sigma(\delta) = \pm\delta$. As char $F \neq 2$, we have $\delta \neq -\delta$ and so $\sigma(\delta) = \delta$ if and only if the permutation σ is even, or, identifying A with $\mathbf{N}_n = \{1, \dots, n\}$, if and only if $\sigma \in A_n$. We thus obtain that the Galois group G fixes δ if and only if $G \subset A_n$, or equivalently, by Theorem 6.2, $\delta \in F$ if and only $G \subset A_n$. As Δ is a square in F if and only if $\delta \in F$, this finishes the proof. □

Example Let $f \in F[X]$ be separable, irreducible and of degree 3. From Theorem 7.2, 3 divides the cardinal of the Galois group G of f over $\mathbf{Q}$. If we now suppose that Δ is a square, then, identifying G with a subgroup of S_n, we have $G \subset A_3$. However, as $|A_3| = 3$, we have G isomorphic to A_3. If, on the other hand, $\Delta(f)$ is not a square in F, then $G \not\subset A_3$. The only other subgroup of S_3 divisible by 3 is S_3 itself, so in this case G is isomorphic to S_3.

We will now consider another criterion which enables us to determine the nature of the Galois group, but this time only over $\mathbf{Q}$.

9.2 A criterion for rational polynomials

In the last section we considered a criterion which was generally applicable. Often criteria can only be used for certain types of field. This is the case with the criterion which we now consider. We will first need to do a little preliminary work on permutations.

Lemma 9.1 *If p is a prime number, then every element of S_p of order p is a p-cycle.*

PROOF Let $\pi \in S_p$ be of order p. We may write

$$\pi = \pi_1 \cdots \pi_r,$$

where the π_i are nontrivial disjoint cycles. We have

$$p = o(\pi) = [o(\pi_1), \ldots, o(\pi_r)].$$

Hence, $o(\pi_i)|p$, for all i. As $o(\pi_i) > 1$, we must have $o(\pi_i) = p$. This implies that all the π_i are p-cycles and so π is a product of p-cycles. However, we cannot have more than one such cycle, because the permutation is on p elements. Therefore, π is a p-cycle. □

It is well-known that the transposition $(1\ 2)$ and the n-cycle $(1 \ldots n)$ generate S_n. This is not in general true for any transposition and n-cycle. For example, the cycles $(1\ 3)$ and $(1\ 2\ 3\ 4)$ in S_4 generate a subgroup G isomorphic to D_8. To see this, it is sufficient to notice that G is a nonabelian group of cardinal 8, with an element of order 4 and an element of order 2 (see Appendix B). However, if n is prime, then any transposition and n-cycle generate S_n. We will prove a related result and then establish this as a corollary.

Proposition 9.2 *For $1 \leq a < b \leq n$, the transposition $(a\ b)$ and the n-cycle $(1\ 2\ \ldots\ n)$ generate S_n if and only if $(b-a, n) = 1$.*

PROOF Let $d = (b-a, n)$. We claim that if $\pi \in \langle (a\ b), (1\ 2\ \ldots\ ) \rangle$, then

$$i \equiv j \pmod{d} \Longrightarrow \pi(i) \equiv \pi(j) \pmod{d}.$$

To prove this, it is sufficient to consider the cases where $\pi = (a\ b)$ and $\pi = (1\ 2\ \ldots\ n)$. We have

- for $i \neq a, b$, $(a\ b)(i) = i$;
- for $i = a$, $(a\ b)(i) = b$;
- for $i = b$, $(a\ b)(i) = a$.

From these equalities, we see that, if $\pi = (a\ b)$, then

$$d|(j-i) \Longrightarrow d|(\pi(i) - \pi(j)),$$

i.e., the assertion is true for $\pi = (a\ b)$. Now let us consider the case where $\pi = (1\ 2\ \ldots\ n)$. We have

$$\pi(i) = i + 1 \pmod{n} \Longrightarrow \pi(i) = i + 1 \pmod{d},$$

because $d|n$. As

$$i \equiv j \pmod d \Longrightarrow i+1 \equiv j+1 \pmod d,$$

the assertion is true for $\pi = (1\ 2\ \dots\ n)$. We have proved the claim.

Now suppose that $d > 1$ and consider the transposition $(1\ 2)$. We have

$$(1\ 2)(1) = 2 \qquad \text{and} \qquad (1\ 2) = 1 + d.$$

However, $1 \equiv 1 + d \pmod d$, but $2 \not\equiv 1 + d \pmod d$. Hence, $(1\ 2) \notin \langle (a\ b), (1\ 2\ \dots\ )\rangle$. Therefore S_n is not generated by $(a\ b)$ and $(1\ 2\ \dots\ n)$.

We now prove the converse. Let $\sigma = (1\ 2\ \dots\ n)$; then $\sigma^i(a) \equiv a + i \pmod n$. Hence

$$\sigma^{b-a}(a) \equiv b \pmod n.$$

As $1 \leq \sigma^{b-a}(a), b \leq n$, we have $\sigma^{b-a}(a) = b$. Next we notice that there exist s and t such that $s(b-a) + tn = 1$, because $b - a$ and n are coprime. This implies that

$$\sigma = \sigma^{(b-a)s}\sigma^{nt} = \sigma^{(b-a)s} \Longrightarrow \langle (a\ b), \sigma\rangle = \langle (a\ b), \sigma^{b-a}\rangle.$$

Now σ^{b-a} is an n-cycle. If this is not the case, then σ^{b-a} can be written as a product of disjoint cycles of length less than n. However,

$$\sigma^{\alpha(b-a)}(1) \equiv 1 + \alpha(b-a) \equiv 1 \pmod n \Longrightarrow n|\alpha(b-a) \Longrightarrow n|\alpha,$$

because $(b-a, n) = 1$. If $1 \leq \alpha < n$, then this is not possible, so $\sigma^{\alpha(b-a)}(1) \neq 1$. This means that 1 belongs to no cycle of length smaller than n and so σ^{b-a} is an n-cycle.

There exists a permutation $\pi \in S_n$ such that $\pi(1\ 2\ \dots\ n)\pi^{-1} = \sigma^{b-a}$ and $\pi(1) = a$, $\pi(2) = b$. Then

$$\begin{aligned} S_n &= \pi S_n \pi^{-1} = \pi\langle (1\ 2), (1\ 2\ \dots\ n)\rangle\pi^{-1} \\ &= \langle \pi(1\ 2)\pi^{-1}, \pi(1\ 2\ \dots\ n)\pi^{-1}\rangle \\ &= \langle (a\ b), \sigma^{b-a}\rangle \\ &= \langle (a\ b), \sigma\rangle. \end{aligned}$$

This finishes the proof. □

Lemma 9.2 *Let p be a prime number. If τ is a transposition and σ a p-cycle in S_p, then $H = \langle \tau, \sigma\rangle$, the subgroup of S_p generated by τ and σ, is the whole group S_p.*

PROOF Let $\tau = (a\ b)$. There is a permutation $\pi \in S_p$ such that $\pi(1\ 2\ \dots\ p)\pi^{-1} = \sigma$. Let $\tau = (a\ b)$ and $\pi(a') = a$, $\pi(b') = b$. Then we have

$$S_p = \pi\langle (a'\ b'), (1\ 2\ \ \dots\ p)\rangle\pi^{-1},$$

because $(b' - a', p) = 1$ (Proposition 9.2). Now

$$\begin{aligned} \pi\langle (a'\ b'), (1\ 2\ \ \dots\ p)\rangle\pi^{-1} &= \langle \pi(a'\ b')\pi^{-1}, \pi(1\ 2\ \ \dots\ p)\pi^{-1}\rangle \\ &= \langle (a\ b), \sigma\rangle = \langle \tau, \sigma\rangle. \end{aligned}$$

We have proved what we set out to establish. □

We now turn to a result which enables us to determine the Galois group of a rational polynomial under certain conditions.

Theorem 9.1 *Let $f \in \mathbf{Q}[X]$ be irreducible and of prime degree p. If f has only two complex roots, α and $\bar{\alpha}$, then the Galois group G of f over $\mathbf{Q}$ is isomorphic to S_p.*

PROOF From Lemma 9.2, it is sufficient to show that G has a transposition and a p-cycle. The mapping conjugate conjugation restricted to the set of roots of f is a transposition. Also, from Theorem 7.2, $p||G|$, so G has an element of order p. From Lemma 9.1, this must be a p-cycle. This finishes the proof. □

Example The polynomial $f(X) = -1 + X + X^3$ is irreducible over $\mathbf{Q}$: If f is reducible over $\mathbf{Q}$, then f is also reducible over $\mathbf{Z}$ and, in this case, $\bar{f}$, the reduction of f modulo 2, has a root in $\mathbf{Z}_2$. However, this is not the case, and so f is irreducible over $\mathbf{Q}$. Also, $f'(X) = 1 + 3X^2$, which does not vanish in $\mathbf{R}$, so f has a unique root in $\mathbf{R}$. This means that f has a pair of complex roots and we may apply the theorem: the Galois group of f is isomorphic to S_3.

Example The polynomial $f(X) = -1-4X+X^5$ is irreducible over $\mathbf{Q}$. To see this it is sufficient to show that $\bar{f}$, the reduction of f modulo 2, is irreducible. This is so, because $\bar{f}$ has no root in $\mathbf{Z}_2$ and no polynôme of degree 2 in $\mathbf{Z}_2[X]$ divides $\bar{f}$. The derivative of f is $f'(X) = -4 + 5X^4$. As a function defined on $\mathbf{R}$, $f$is positive for $x^4 \geq \frac{4}{5}$ and negative for $x^4 \leq \frac{4}{5}$. As $f(0) = -1$, $f(-1) = 2$ and $\lim_{x \mapsto \pm\infty} f(x) = \pm\infty$, f has precisely three real roots. Applying the theorem, we see that the Galois group of f is isomorphic to S_5.

We will now look at a more general polynomial. Let p be a prime number, with $p \geq 7$, and $m, n_1, \ldots, n_{p-2}$ positive even integers such that $n_i < n_{i+1}$ and $\sum_{i=1}^{p-2} n_i^2 - 2m < 0$. We define the polynomial $g \in \mathbf{Z}[X]$ by

$$g(X) = (m + X^2)(-n_1 + x)(-n_2 + X) \cdots (-n_{p-2} + X).$$

The polynomial g has the roots $n_1, \ldots, n_{p-2}$. On an interval $(n_i, n_{i+1}) \subset \mathbf{R}$ the sign of the polynomial function g does not change, because there is no real root in such an interval. Also, as $g'(n_i) \neq 0$, the signs of g on adjacent intervals are opposites. Thus g has $\frac{p-3}{2}$ positive relative maxima and $\frac{p-3}{2}$ negative relative maxima. If k is an odd integer, then it is not difficult to see that $|g(k)| > 2$, hence the relative maxima have a value strictly superior to 2.

We now set $f(X) = g(X) - 2$. From what we have seen, there exist $x_1, \ldots, x_{p-2} \in (n_1, n_{p-2})$ such that for the polynomial fuction f we have $f(x_i)f(x_{i+1}) < 0$, for $i = 1, \ldots, p-4$. Therefore f has a root in each interval (x_i, x_{i+1}). As $f(n_i) = -2$, and $f(x_1)$ and $f(x_{p-3})$ have opposite signs, there must exist a root of f in (n_1, x_1) or in (x_{p-3}, n_{p-2}). In addition, as $f(n_{p-2}) = -2$ and $\lim_{x \mapsto \pm\infty} f(x) = +\infty$, we have another root of f in the interval (n_{p-2}, ∞). We have shown that f has at least $p-2$ real roots.

We will now show that f has two roots in $\mathbf{C} \setminus \mathbf{R}$. We have

$$f(X) = (X + i\sqrt{m})(X - i\sqrt{m})(-n_1 + X)(-n_2 + X) \cdots (-n_{p-2} + X) - 2$$

and the constant term is not divisible by 4 and

$$f(X) = \prod_{i=1}^{p} (-\alpha_i + X),$$

where the α_i are the complex roots of f. If we compare the coefficients of X^{p-1} and X^{p-2} in the two expressions for f, then we obtain

$$\sum_{i=1}^{p} \alpha_i = \sum_{i=1}^{p-2} n_i \qquad \text{and} \qquad \sum_{i<j} \alpha_i \alpha_j = \sum_{i<j} n_i n_j + m.$$

Hence

$$\sum_{i=1}^{p}\alpha_i^2=\left(\sum_{i=1}^{p}\alpha_i\right)^2-2\sum_{i<j}\alpha_i\alpha_j=\left(\sum_{i=1}^{p-2}n_i\right)^2-2\left(\sum_{i<j}n_in_j+m\right)=\sum_{i=1}^{p-2}n_i^2-2m.$$

As $\sum_{i=1}^{p-2}n_i^2-2m<0$, we have $\sum_{i=1}^{p}\alpha_i^2<0$, so at least one $\alpha_i\in\mathbf{C}\setminus\mathbf{R}$. However, as f is a real polynomial, the complex conjugate of α_i is also a root of f. We have shown that f has only real roots except for a pair of complex conjugates.

To complete the discussion we show that f is irreducible over $\mathbf{Q}$. Now, all the coefficients of f, except the leading coefficient, are divisible by 2 and the constant term is not divisible by 4 ($4|mn_1\cdots n_{p-2}\Longrightarrow 4\not|(mn_1\cdots n_{p-2}-2)$). From Eisenstein's critrerion, f is irreducible over $\mathbf{Q}$. We may now apply Theorem 9.1 to see that for the class of polynomials under consideration the Galois group is S_p. It is worth noticing that there is an infinite number of polynomials in this class.

9.3 Possible forms of the Galois group

As we have seen, the Galois group of a polynomial f of degree n may be considered as a subgroup of S_n. However, not all subgroups of S_n are possible. If we suppose that f is separable and irreducible, then the Galois group of f must be transitive and its cardinal a multiple of n (Theorem 7.2). Therefore, if we are considering such polynomials, then we know that the Galois group must belong to a certain finite subclass of subgroups of S_n. For example, if $f\in\mathbf{Q}[X]$ is irreducible and of degree 5 and G is its Galois group, then $5||G|$. If we also know that the discriminant of f is a square in $\mathbf{Q}$, then we can say that G is a subgroup of A_n (Proposition 9.1). This limits considerably the possibilities.

Now we aim to consider the Galois group G of a an irreducible rational polynomial of degree n. If $n=2$ and $|S_n|=2$, in this case there can only be one possibility for the Galois group, namely S_2. Let us now consider the case where $n=3$. We have already seen (in the first section of this chapter) that there are two possibilities, namely S_n and A_n, the first when the discriminant of the polynomial is not a square in $\mathbf{Q}$ and the other when it is. We now turn to the case where $n=4$. This is more instructive and we will need some elementary group theory. We recall that the only subgroup of S_n of index 2 is A_n.

Transitive subgroups of S_4 divisible by 4

Now let us consider the possible Galois groups for irreducible rational polynomials of degree 4. We must find the subgroups of S_4 which are transitive and whose cardinal is divisible by 4. The possible orders for such subgroups are 4, 8, 12 and 24. The only subgroup of order 24 is S_4 and the only subgroup of order 12 is A_4. Therefore we are left with subgroups of order 4 and 8.

If G is a subgroup of order 8, then G must be a Sylow 2-subgroup of S_4. All such subgroups are conjugate and hence isomorphic. Thus, up to isomorphism, there is only one possible subgroup of order 8. If we set

$$\rho=(1\ 2\ 3\ 4)\qquad\text{and}\qquad\sigma=(1\ 3),$$

then we find that

$$\sigma\rho\sigma^{-1}=(1\ 4\ 3\ 2)=\sigma^{-1}$$

and that the set

$$S=\{e,\rho,\rho^2,\rho^3,\sigma,\rho\sigma,\rho^2\sigma,\rho^3\sigma\}$$

is a group (generated by ρ and σ). This group is thus isomorphic to the dihedral group D_8.

Finally we turn to the case where the subgroup G is of order 4. Clearly the subgroup generated by a 4-cycle is a transitive subgroup of S_4 of order 4 and all such subgroups are isomorphic. The other subgroups of S_4 of order 4 are isomorphic to the Klein subgroup, i.e., $\mathbf{Z}_2 \times \mathbf{Z}_2$. In addition to the identity, such a group has elements of order 2 of cycle types $(2, 1, 1)$ or $(2, 2)$. There are three possibilities:

- All the σ_i are transpositions: then we must have $(1\ 2)$, $(1\ 3)$ and $(2\ 3)$ and the product of the first two is the 3-cycle $(1\ 3\ 2)$, a contradiction.
- One of the σ_i is of type $(2, 2)$ and the other two are transpositions: in this case, the two transpositions must be disjoint, otherwise their product is a 3-cycle and the group has the form
$$\{e, (1\ 2), (3\ 4), (1\ 2)(3\ 4)\},$$
which is not transitive.
- Two of the σ_i are of type $(2, 2)$, which implies that the third is also of this type and the group has the form
$$\{e, (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)\},$$
which we note V_4. This subgroup is clearly transitive.

We are now going to consider transitive subgroups of S_5. However, before doing so, we need to introduce a little group theory.

We recall that a group is simple if it has no proper normal subgroup other than $\{e\}$. For $n \geq 5$, A_n is simple. (A proof of this may be found, for example, in [19].)

Exercise 9.1 *Show that A_4 is not simple. What can we say about A_2 and A_3?*

Exercise 9.2 *Show that, for $n \geq 5$, A_n is the unique nontrivial normal subgroup of S_n.*

We need a technical result, which is not standard.

Proposition 9.3 *If G is a finite group and H a nontrivial subgroup such that $|G|$ does not divide $[G : H]!$, then H contains a nontrivial normal subgroup of G.*

PROOF Let $n = [G : H]$. Each $g \in G$ induces a permutation π_g on the quotient set G/H:
$$\pi_g(xH) = gxH.$$
As $[G : H] = n$, we may identify π_g with an element of S_n. The mapping $\phi : g \longmapsto \pi_g$ is a homomorphism:
$$\pi_{gh}(xH) = ghxH = \pi_g(hxH) = \pi_g \circ \pi_h(xH).$$
Now $\ker\phi$ is a normal subgroup of G contained in H:
$$gxH = H \Longrightarrow xH = g^{-1}H.$$
As this is true for all $x \in G$, it is true for the identity element, so we obtain
$$eH = g^{-1}H \Longrightarrow g^{-1} \in H \Longrightarrow g \in H,$$

and it follows that $\ker\phi \subset H$.

Also

$$G/\ker\phi \simeq \operatorname{Im}\phi \Longrightarrow |G/\ker\phi|\,|n! \Longrightarrow |G|\,|\,|\ker\phi|n!$$

If $|G|$ does not divide $n!$, then $|\ker\phi| \neq 1$ and so $\ker\phi$ is not trivial. □

The knowledge of semidirect products needed in the next part of our exposition can be found in Appendix B.

Transitive subgroups of S_5 divisible by 5

Now let us consider the possible Galois groups for irreducible rational polynomials of degree 5. The orders of such groups must be multiples of 5 and divisors of 120. In fact, the transitivity does not enter into the question.

Proposition 9.4 *Let G be a subgroup of S_5 whose order is divisible by 5. Then G is transitive.*

PROOF By Cauchy's Theorem G contains an element of order 5, i.e., a 5-cycle $\sigma = (x_1, \dots, x_5)$. It is not difficult to see there is a power k of σ which sends x_i to x_j, for any pair of numbers x_i and x_j. Therefore G is transitive. □

Remark We can generalize this result to S_p, for any prime p: If p is a prime number and G a subgroup of S_p such that $p||G|$, then G is transitive.

Taking into account what we have seen, the possible orders of subgroups of S_5 which interest us are 5, 10, 15, 20, 30, 40, 60 and 120.

Let us first consider the possible cyclic subgroups. In S_5 the highest possible order of an element is 6; this results from the decomposition of a permutation into distinct cycles. It follows that the only cyclic groups of S_5 whose order is divisible by 5 are those generated by a 5-cycle.

Now we consider subgroups of order 10. If G is such a subgroup, then it is cyclic or isomorphic to D_{10} (Proposition C.4). The first possibility has already been ruled out, so there only remains the second. This occurs: If we set $\sigma = (1\,2\,3\,4\,5)$ and $\tau = (1\,3)(4\,5)$ and then $G \simeq \langle\sigma, \tau\rangle$. If we set $H = \langle\sigma\rangle$ and $K = \langle\tau\rangle$, then it is easy to check that G is isomorphic to the semidirect product of H and K, which is not direct.

Suppose that G is a subgroup of S_5 of order 15. From Theorem C.2, G is cyclic, which is impossible, so there is no subgroup of order 15 in S_5.

We now turn to the case where $|G| = 20$. This is a little more interesting. G has a Sylow 5-subgroup P and a Sylow 2-subgroup Q, with $|P| = 5$ and $|Q| = 4$. Writing s_5 for the number of Sylow 5-subgroups, we have $s_5|4$ and so s_5 can take the values 1, 2 or 4. However, $s_5 \equiv 1 \pmod 5$, so the only possibility is $s_5 = 1$. This implies that P is normal in G. As the order of elements in P and Q are coprime $P \cap Q = \{e\}$ and so $PQ = G$. If Q is normal in P, then G is the direct product of P and Q and so abelian. However, in this case G has an element of order 10, which we have excluded, so G is a semidirect product of P and Q, which is not abelian.

We would like to know a little more about the subgroup Q. We consider the mapping

$$\phi : Q \longrightarrow Aut(P), y \longmapsto \phi_y,$$

where

$$\phi_y(x) = yxy^{-1},$$

for all $x \in P$. If a is a generator of P and $y \in \ker \phi$, then

$$yay^{-1} = a \Longrightarrow ya = ay.$$

As y and a commute, we have $o(ya) = o(y)o(a)$, since the orders of y and a are coprime. If $o(y) = 2$, then $o(ya) = 10$, and if $o(y) = 4$, then $o(ya) = 20$, both of which are impossible. Therefore $o(y) = 1$, which implies that $y = e$. Thus ϕ is injective. As $Aut(P) \simeq \mathbf{Z}_4$, $Q \simeq \mathbf{Z}_4$ and Q is cyclic. It is a simple matter to check the subgroup of S_5 generated by the cycles $(1\ 2\ 3\ 4\ 5)$ and $(2\ 3\ 5\ 4)$ is a subgroup of order 20 of the required type.

What about subgroups G of order 30. The index $[S_5 : G]$ of such a subgroup is 4 and 120, the cardinal of S_5 does not divide $24 = 4!$, so, from Proposition 9.3, G contains a nontrivial normal subgroup N of S_5. However, the only nontrivial normal subgroup of S_5 is A_5 (Exercise 9.2). Thus $N = A_5$, which is impossible, because $|N| < |A_5|$. So there is no subgroup of order 30. We may use an analogous argument to show that there is no subgroup of order 40.

Finally we come to subgroups of order 60 or 120. In the first case there is only A_5 and in the second S_5 itself.

The following theorem sums up our work on the transitive subgroups of S_4 and S_5:

Theorem 9.2 *For S_4 and S_5 we have*

- *The transitive subgroups of S_4 of order divisible by 4 are S_4, A_4, D_8, subgroups generated by a 4-cycle and V_4.*
- *The (transitive) subgroups of S_5 of order divisible by 5 are S_5, A_5, D_{10}, subgroups generated by a 5-cycle and subgroups isomorphic to the nonabelian semidirect product of $\mathbf{Z}_5$ and $\mathbf{Z}_4$.*

The examples of S_4 and S_5 show the difficulty in determining those subgroups of S_n which can be Galois groups of irreducible rational polynomials of degree n. Determining whether such subgroups are actually Galois groups of an irreducible rational polynomial of degree n is another problem. We will come back to this question presently.

In the cases we have considered, the absence of abelian groups has probably been observed. This is not an accident, as we will soon see. We recall that if the group G acts on the set X, then the stabiliser G_x of $x \in X$ is defined as

$$G_x = \{g \in G : g.x = x\}$$

and the orbit O_x of x as

$$O_x = \{g.x : g \in G\}.$$

The orbit-stabilizer theorem asserts, that if G is finite, then

$$|O_x| = \frac{|G|}{|G_x|}.$$

We say that the action is transitive, if for any pair $x, y \in X$, there is a $g \in G$ such that $g.x = y$.

If G is a group of permutations on a set X, then there is a natural action of G on X defined by

$$g.x = g(x),$$

for all $g \in G$ and $x \in X$. We will be interested here in the case where $G \subset S_n$ and $X = \mathbf{N}_n = \{1, \ldots, n\}$.

Proposition 9.5 *If $G \subset S_n$ is transitive and abelian, then $|G| = n$.*

PROOF From the orbit-stabilizer theorem we have

$$|O_x| = \frac{|G|}{|G_x|}.$$

As G is transitive, the action of G on $\mathbf{N}_n$ is transitive and so, for any $x \in \mathbf{N}_n$,

$$|O_x| = n \Longrightarrow |G| = n|G_x|.$$

We claim that $|G_x| = 1$. Let $g \in G_x$ and take $a \in \mathbf{N}_n$. As G is transitive, there exists $h \in G$ such that $h.x = a$. Hence, using the fact that G is abelian,

$$g.a = g.(h.x) = h.(g.x) = h.x = a.$$

As this equality is true for any $a \in \mathbf{N}_n$, $g = e$, which proves our claim. We obtain $|G| = n$. □

Corollary 9.1 *If p is a prime number, and G is a transitive abelian subgroup of S_p, then G is generated by a p-cycle.*

PROOF This is a consequence of Proposition 9.5 and Lemma 9.1. □

We now return to the question of the existence of an irreducible rational polynomial of degree n whose Galois group is isomorphic to a given transitive subgroup of S_n. For S_n itself the answer is always positive.

We now consider the case where $n = 4$.

- If $f(X) = -2 + X^4$, then the Galois group of f is D_8. We give a proof of this in Appendix D.
- From Theorem 7.7 we know that the Galois group $G = Gal(\mathbf{Q}(\mu_5)/\mathbf{Q})$ is isomorphic to $\mathbf{Z}_5^\times$, which is in turn isomorphic to C_4. However, $\mathbf{Q}(\mu_5)$ is a splitting field of $\Phi_5(X) = 1 + X + X^2 + X^3 + X^4$, which is irreducible. Thus the Galois group of Φ_5 is isomorphic to C_4 and so must be generated by a 4-cycle.
- For V_4 we have the following argument. The splitting field of $g(X) = 1 + X^4$ is $\mathbf{Q}(i, \sqrt{2})$, which is also the splitting field of $h(X) = (1 + X^2)(-2 + X^2)$. However, the Galois group of h is isomorphic to $C_2 \times C_2$ (see Example 1 in the next section), so this must be the case for g. Given that V_4 is the only transitive subgroup of S_4 isomorphic to $C_2 \times C_2$, V_4 must be isomorphic to the Galois group of g.
- Finally we consider A_4. We will show that this group is isomorphic to the Galois group of $k(X) = 12 + 8X + X^4$. First we notice that the discriminant $\Delta(k) = 2^{12}3^4$, a square, so the Galois group G of k is a subgroup of A_4, by Proposition 9.1. As $4||G|$, $|G| = 4$ or $|G| = 12$. Now we use Dedekind's Theorem. Factorizing k modulo 5, we find

  $$k(X) = (1 + X)(2 + X + 4X^2 + X^3),$$

  hence the Galois group of k has a permutation of the form $(1,\ 3)$, i.e., an element of order 3. This means that $3||G|$ and it follows that $|G| = 12$. Thus the Galois group of k is isomorphic to A_4.

It is also the case that, for $n = 5$, $n = 6$ and $n = 7$, all transitive subgroups of S_n are isomorphic to the Galois group of an irreducible polynomial in $\mathbf{Q}[X]$ (see [22]); however, for $n > 7$, the question is open.

9.4 Reducible polynomials

In the previous section we were concerned with irreducible polynomials. Here we aim to consider reducible polynomials, in particular, products of two polynomials whose Galois groups are known. We will begin with some examples.

Example 1 Let $f(X) = (1+X^2)(-2+X^2) \in \mathbf{Q}[X]$. The splitting field of $g(X) = 1+X^2$ in $\mathbf{C}$ is $\mathbf{Q}(i)$. As $\mathbf{Q}(i)$ is a Galois extension of $\mathbf{Q}$, we have

$$|Gal(\mathbf{Q}(i)/\mathbf{Q})| = [\mathbf{Q}(i) : \mathbf{Q}] = 2$$

and it follows that the Galois group of g is isomorphic to the cyclic group C_2. A similar argument shows that the Galois group of $h(X) = -2+X^2$ is also isomorphic to C_2. We now consider the Galois group of f. The splitting field of f in $\mathbf{C}$ is $\mathbf{Q}(i, \sqrt{2})$ and

$$[\mathbf{Q}(i,\sqrt{2}) : \mathbf{Q}] = [\mathbf{Q}(i,\sqrt{2}) : \mathbf{Q}(\sqrt{2})][\mathbf{Q}(\sqrt{2}) : \mathbf{Q}] = 2.2 = 4.$$

Using Corollary 7.1, we see that the cardinal of the Galois group G of f is 4, which implies that G is isomorphic to C_4 or $C_2 \times C_2$. If $\sigma \in G$, then

$$\sigma(i)^2 = \sigma(i^2) = \sigma(-1) = -1 \Longrightarrow \sigma(i) = \pm i.$$

In the same way

$$\sigma(\sqrt{2})^2 = \sigma(\sqrt{2}^2) = \sigma(2) = 2 \Longrightarrow \sigma(\sqrt{2}) = \pm\sqrt{2}.$$

Hence $\sigma^2(i) = i$ and $\sigma^2(\sqrt{2}) = \sqrt{2}$ and it follows that $\sigma^2 = \mathrm{id}_G$. This means that all elements of G have order 1 or 2 and so G is isomorphic to $C_2 \times C_2$.

Example 2 We consider the polynomial $f(X) = (1+X+X^2)(3+X^2) \in \mathbf{Q}[X]$. The splitting field of $g(X) = 1+X+X^2$ is $\mathbf{Q}(j)$, where $j = \exp(\frac{2\pi i}{3})$. Hence $\mathbf{Q}(j)$ is a Galois extension of $\mathbf{Q}$. It follows that the cardinal of the Galois group of g is 2 and so this group is isomorphic to C_2. There is no difficulty in seeing that the Galois group of $h(X) = 3+X^2$ is also C_2. What can we say about the Galois group of f? First, the splitting field of f is $\mathbf{Q}(j, i\sqrt{3})$. However, $j = \frac{-1+i\sqrt{3}}{2}$, and so $\mathbf{Q}(j, i\sqrt{3}) = \mathbf{Q}(j) = \mathbf{Q}(\sqrt{3})$, therefore the Galois group of f is isomorphic to C_2.

Example 3 This time we take the polynomial $f(X) = (-2+X^3)(-5+X^3) \in \mathbf{Q}[X]$. From Theorem 9.1, the Galois groups of $g(X) = -2+X^3$ and $h(X) = -5+X^3$ are both isomorphic to S_3. The splitting field of f is

$$\mathbf{Q}(\sqrt[3]{2}, j\sqrt[3]{2}, j^2\sqrt[3]{2}, \sqrt[3]{5}, j\sqrt[3]{5}, j^2\sqrt[3]{5}) = \mathbf{Q}(\sqrt[3]{2}, j\sqrt[3]{2}, \sqrt[3]{5}, j\sqrt[3]{5}) = \mathbf{Q}(\sqrt[3]{2}, j, \sqrt[3]{5}).$$

Clearly $[\mathbf{Q}(\sqrt[3]{2}, j, \sqrt[3]{5}] : \mathbf{Q}] \leq 27$ so the Galois group of f cannot be isomorphic to $S_3 \times S_3$.

In the first example the Galois group of the product of the two polynomials is the product of their Galois groups. In the second and third examples this is not the case. The essential difference is that in the first example the intersection of the splitting fields is $\mathbf{Q}$, while in the other two examples, this is not the case. In the next result we formalize this. (Beforehand it may be useful to briefly look at Appendix A, where semidirect and direct products are handled.)

Theorem 9.3 *Let $f \in F[X]$ be separable. Suppose that $f = gh$, with $g, h \in F[X]$ irreducible, E is a splitting field of f and K (resp. L) a splitting field of g (resp. h) in E. Then*

$$Gal(E/F) \simeq Gal(K/F) \times Gal(L/F)$$

if and only if $K \cap L = F$.

PROOF First it should be noticed that the separability of f, together with Theorem 3.8, ensures that E is a separable extension of F. Let us write $G = Gal(E/F)$, $G_K = Gal(E/K)$ and $G_L = Gal(E/L)$. The extensions K and L are normal, so the Galois groups G_K and G_L are normal subgroups of G.

As K and L are included in E, KL is included in E. On the other hand, if α is a root of f, then α is a root of g or h and so f splits over KL, hence $E \subset KL$. We have shown that $E = KL$. Using Corollary 6.1, we may write

$$[E : F] = [KL : F] = \frac{[K : F][L : F]}{[K \cap L : F]}.$$

If we now suppose that the Galois group of f is the direct product of the Galois groups of g and h, then

$$[E : F] = [K : F][L : F] \Longrightarrow [K \cap L : F] = 1 \Longrightarrow K \cap L = F.$$

We now consider the converse. Setting $\tilde{G}$ for the subgroup of G generated by G_K and G_L, we have, from Theorem 6.9,

$$\mathcal{F}(\tilde{G}) = K \cap L = F \Longrightarrow \tilde{G} = G.$$

From Theorem 6.9 we know that $\mathcal{F}(G_K \cap G_L) = KL = E$. This implies that $G_K \cap G_L = \mathrm{id}_E$. Since G_K and G_L are normal subgroups of G, the elements of G_K commute with those of G_L and it follows that $G = \tilde{G} = G_K G_L$. Thus $G = G_K \times G_L$ and it follows that G_K (resp. G_L) is isomorphic to G/G_L (resp. G/G_K). We have shown that

$$G \simeq G/G_L \times G/G_K \simeq Gal(L/F) \times Gal(K/F),$$

from Theorem 6.6. This ends the proof. □

Remark This result may be easily extended to the case where f is a product of more than two polynomials.

Chapter 10

Norm, trace and discriminant

In this chapter we introduce some important notions which will be used later on in the text, in particular, when we come to study in more detail number fields.

10.1 Norm and trace

Let E be a finite extension of a field F. For $x \in E$, we define a linear endomorphism m_x of E by

$$m_x(y) = xy,$$

for all $y \in E$. We define the *norm* and the *trace* of x, relative to the extension E of F, by

$$N_{E/F}(x) = \det m_x \qquad \text{and} \qquad T_{E/F}(x) = \operatorname{tr} m_x.$$

We also define the *characteristic polynomial* of x. This is just the characteristic polynomial of the endomorphism m_x and we write $\text{char}_{E/F}(x)$ for this polynomial. To simplify the notation, when the fields E and F are understood, we often omit the symbol E/F. From the definitions, if $n = [E : F]$, then,

$$\text{char}_{E/F}(x) = (-1)^n N(x) + \cdots - T(x)X^{n-1} + X^n.$$

As the coefficients of a matrix of m_x belong to F, the coefficients of $\text{char}_{E/F}(x)$ belong to F. In particular, if E is a number field and $x \in K$, then $N_{E/\mathbf{Q}}(x)$ and $T_{E/\mathbf{Q}}(x)$ are rational numbers.

Example Let n be a squarefree integer and $E = \mathbf{Q}(\sqrt{n})$. Then $[K : \mathbf{Q}] = 2$ and $(1, \sqrt{n})$ is a basis of E over $\mathbf{Q}$. If $x = a + b\sqrt{n}$, then

$$m_x(1) = a + b\sqrt{n} \qquad \text{and} \qquad m_x(\sqrt{n}) = a\sqrt{n} + bn,$$

therefore the matrix of m_x in the basis $(1, \sqrt{n})$ is

$$M = \begin{pmatrix} a & bn \\ b & a \end{pmatrix}.$$

Hence

$$N_{E/\mathbf{Q}}(x) = a^2 - b^2 n \qquad \text{and} \qquad T_{E/\mathbf{Q}}(x) = 2a.$$

If n is negative and $a, b \in \mathbf{Z}$, then $N_{E/\mathbf{Q}}(x) \in \mathbf{N}$ and $T_{E/\mathbf{Q}}(x) \in \mathbf{N}$.

If $x \in F$, then the matrix of m_x in any basis is just xI_n and so

$$N(x) = x^n, \qquad T(x) = nx \qquad \text{and} \qquad \text{char}\,(x) = (-x + X)^n.$$

Exercise 10.1 *Show that the norm is multiplicative, i.e.,*

$$N(x_1 x_2) = N(x_1)N(x_2),$$

for all $x_1, x_2 \in E$, and that the trace is F-linear. Also, show that the mapping

$$B : E \times E \longrightarrow F : (x_1, x_2) \longmapsto T(x_1 x_2)$$

is bilinear.

If $x \in F$, then $m(x, F) = -x + X$, so char $(x) = m(x, F)^n$. In the next proposition we generalize this fact.

Proposition 10.1 *If $r = [E : F(x)]$, then*

$$\textit{char}_{\,E/F}(x) = m(x, F)^r.$$

PROOF First let us consider the case $r = 1$. Then $E = F(x)$. From the Cayley-Hamilton Theorem, we know that char $(m_x) = 0$, hence

$$(-1)^n N(x)y + \cdots - T(x)x^{n-1}y + x^n y = 0,$$

for all $y \in E$. If we set $y = 1$, then we see that x is a root of char (x). Hence $m(x, f)|$char (x). Now,

$$n = [E : F] = [F(x) : F] = \deg m(x, F)$$

and so $m(x, F) = $ char (x), hence the result for $r = 1$.

Now let us consider the general case. Let $y_1, \ldots, y_s$ be a basis of $F(x)$ over F and $z_1, \ldots, z_r$ a basis of E over $F(x)$. The elements $y_i z_j$, with $\leq i \leq s$ and $1 \leq j \leq r$, form a basis of E over F. Let $A = (a_{kl})$ be the matrix representing m_x, in the basis (y_i), for the extension $F(x)$ of F. (Notice that $A \in \mathcal{M}_s(F)$.) Then

$$xy_i = \sum_{k=1}^{s} a_{ki} y_k \Longrightarrow x(y_i z_j) = \sum_{k=1}^{s} a_{ki}(y_k z_j).$$

Now we order the basis $(y_i z_j)$ as follows:

$$y_1 z_1, y_2 z_1, \ldots, y_s z_1, y_1 z_2, \ldots, y_s z_2, \ldots, y_s z_r.$$

The matrix representing m_x, in the basis $(y_i z_j)$, for the extension E of F is

$$B = \text{diag}\,(A, \ldots, A).$$

(There are r blocks A.) Thus

$$\text{char}_{\,E/F}(x) = (\det(-A + XI_s))^r = m(x, F)^r,$$

where we have used the case $r = 1$ in the second equality. □

The following result provides an expression for $N_{E/F}(x)$ in terms of the conjugates of x over F.

Corollary 10.1 *Let E be a splitting field of the minimal polynomial $m(x,F)$. If $n=[E:F]$, $[F(x):F]=d$ and $x_1,\ldots,x_d$ are the roots of $m(x,F)$ in E (with repetition of roots possible), then*

$$N_{E/F}(x)=\left(\prod_{i=1}^{d}x_i\right)^{\frac{n}{d}}, \qquad T_{E/F}(x)=\frac{n}{d}\sum_{i=1}^{d}x_i$$

and

$$char_{\ E/F}(x)=\left(\prod_{i=1}^{d}(-x_i+X)\right)^{\frac{n}{d}}.$$

PROOF We have

$$[E:F]=[E:F(x)][F(x):F],$$

hence $[E:F(x)]=\frac{n}{d}$. From Proposition 10.1,

$$\text{char}_{\ E/F}(x)=m(x,F)^{\frac{n}{d}}=\left(\prod_{i=1}^{d}(-x_i+X)\right)^{\frac{n}{d}}.$$

If

$$m(x,F)=a_0+a_1X+\cdots+a_{d-1}X^{d-1}+X^d,$$

then

$$m(x,F)^{\frac{n}{d}}=a_0^{\frac{n}{d}}+\cdots+\frac{n}{d}a_{d-1}X^{n-1}+X^n.$$

It is clear that the constant term is $a_0^{\frac{n}{d}}$; however, the coefficient of X^{n-1} needs an explanation. From the multinomial theorem, with $a_d=1$, we have

$$(a_0+a_1X+\cdots+a_{d-1}X^{d-1}+X^d)^{\frac{n}{d}}=\sum_{k_0+k_1+\cdots+k_d=\frac{n}{d}}\binom{\frac{n}{d}}{k_0,k_1,\ldots,k_d}\prod_{0\le i\le d}(a_iX^i)^{k_i}.$$

To obtain the coefficient of X^{n-1}, first we notice that

$$k_0+k_1+\cdots+k_d=\frac{n}{d} \tag{10.1}$$

and

$$0k_0+1k_1+2k_2+\cdots+dk_d=n-1. \tag{10.2}$$

Multiplying equation (10.1) by d we obtain

$$dk_0+dk_1+\cdots+dk_d=n. \tag{10.3}$$

We now subtract equation (10.2) from equation (10.3). This gives us

$$dk_0+(d-1)k_1+(d-2)k_2+\cdots+(d-(d-1))\,k_{d-1}=1,$$

from which we deduce that $k_i=0$, for $0\le i<d-1$, and $k_{d-1}=1$. To find k_d it is sufficient to use equation (10.3):

$$d+dk_d=n\Longrightarrow k_d=\frac{n}{d}-1.$$

Hence, for the term with X^{n-1} we have

$$\binom{\frac{n}{d}}{0,\ldots 0,1,\frac{n}{d}-1}\left(a_{d-1}X^{d-1}\right)^1\left(X^d\right)^{\frac{n}{d}-1}=\frac{n}{d}a_{d-1}X^{n-1}.$$

We may now continue the proof. Since $a_0 = (-1)^d \prod_{i=1}^d x_i$ and $(-1)^n N(x) = a_0^{\frac{n}{d}}$, we have $N(x) = \left(\prod_{i=1}^d x_i\right)^{\frac{n}{d}}$. In a similar way, $a_{d-1} = -\sum_{i=1}^d x_i$ and $-T(x) = \frac{n}{d} a_{d-1}$ imply that $T(x) = \frac{n}{d} \sum_{i=1}^d x_i$. $\square$

Separable extensions

Suppose now that E is a finite separable extension of the field F. If $[E : F] = n$ and C is an algebraic closure of F, then there are n F-monomorphisms $\sigma_1, \ldots, \sigma_n$ of E into C (Corollary 3.2). (If E is a number field, then it is natural to take $C = A(\mathbf{C}/\mathbf{Q})$, the field of algebraic numbers, from the remark after Theorem 2.6.)

Proposition 10.2 *Suppose that E is a finite separable extension of F. Then, for all $x \in E$,*

$$N_{E/F}(x) = \prod_{i=1}^n \sigma_i(x), \qquad T_{E/F}(x) = \sum_{i=1}^n \sigma_i(x)$$

and

$$char_{\ E/F}(x) = \prod_{i=1}^n (-\sigma_i(x) + X).$$

PROOF We have

$$[E : F] = [E : F(x)][F(x) : F].$$

If $[F(x) : F] = d$, then $[E : F(x)] = \frac{n}{d}$. From Corollary 3.2, we know that there are d F-monomorphisms $\tau_1, \ldots, \tau_d$ of $F(x)$ into C and each one of these F-monomorphisms sends x to a distinct associate x_i. From Theorem 3.2, each τ_i can be extended to an $F(x)$-monomorphism σ_j from E into C. An $F(x)$-monomorphism is an F-monomorphism, thus we obtain n $(= \frac{n}{d} \times d)$ F-monomorphisms σ_j from E into C. As $[E : F] = n$, these F-monomorphisms form the complete set of F-monomorphisms from E into C. Now we have

$$\prod_{i=1}^n \sigma_i(x) = \left(\prod_{i=1}^d \tau_i(x)\right)^{\frac{n}{d}} = \left(\prod_{i=1}^d x_i\right)^{\frac{n}{d}} = N_{E/F}(x)$$

and

$$\sum_{i=1}^n \sigma_i(x) = \frac{n}{d} \sum_{i=1}^d \tau_i(x) = \frac{n}{d} \sum_{i=1}^d x_i = T_{E/F}(x).$$

For the characteristic function we have

$$\prod_{i=1}^n (-\sigma_i(x) + X) = \left(\prod_{i=1}^d (-\tau_i(x) + X)\right)^{\frac{n}{d}} = \left(\prod_{i=1}^d (-x_i + X)\right)^{\frac{n}{d}} = \text{char}_{\ E/F}(x).$$

This finishes the proof. $\square$

The proposition which we have just proved has an important corollary. If we have a tower of fields $F \subset K \subset E$, where E is a finite extension of F, then it makes sense to speak of the compositions $N_{K/F} \circ N_{E/K}$ and $T_{K/F} \circ T_{E/K}$, because $N_{E/K}(x)$ and $T_{E/K}(x)$ are elements of K, for any $x \in E$.

Corollary 10.2 *(transitivity of norm and trace) If K/F and E/K, where E is a finite separable extension of F, then*

$$N_{E/F} = N_{K/F} \circ N_{E/K} \qquad \textit{and} \qquad T_{E/F} = T_{K/F} \circ T_{E/K}.$$

PROOF Let $n = [K : F]$ and $m = [E : K]$. From Proposition 3.5, K is separable over F and E separable over K. Let N be a normal closure of E over F. We saw in Section 5.1 that N may be considered as the splitting field of a polynomial $f \in F[X]$ which is a product of minimal polynomials $m(\alpha, F)$, with $\alpha \in E$. As E is a separable extension of F, the polynomials $m(\alpha, F)$ are separable, and so f is separable. Therefore, from Corollary 3.4, N is a separable extension of F. We have shown that N is a finite Galois extension of F.

Let C be an algebraic closure of N. From Corollary 3.2, there are n F-monomorphisms $\sigma_1, \dots, \sigma_n$ of K into C and m K-monomorphisms from $\tau_1, \dots, \tau_m$ from E into C. Each one of the monomorphisms σ_i and τ_j may be extended to a monomorphism $\hat{\sigma}_i$ or $\hat{\tau}_j$ from N into C (Theorem 3.2). Proposition 5.3 ensures that N is normal over K, since N is normal over F. Applying Proposition 5.2, we see that, for each i and each j, $\hat{\sigma}_i(N) = N$ and $\hat{\tau}_j(N) = N$, hence $\hat{\sigma}_i$ and $\hat{\tau}_j$ are automorphisms of N, for each i and j. Hence we can compose the mappings $\hat{\sigma}_i$ and $\hat{\tau}_j$.

We now use Proposition 10.2. If $x \in E$, then

$$T_{K/F}\left(T_{E/K}(x)\right) = \sum_{i=1}^{n} \sigma_i \left(\sum_{j=1}^{m} \tau_j(x) \right) = \sum_{i=1}^{n} \hat{\sigma}_i \left(\sum_{j=1}^{m} \hat{\tau}_j(x) \right) = \sum_{i=1}^{n} \sum_{j=1}^{m} \hat{\sigma}_i \hat{\tau}_j(x).$$

Each mapping $\hat{\sigma}_i \hat{\tau}_{j|_E}$ is an F-monomorphism of E into C and there are mn such mappings. We claim that for distinct pairs (i, j) these mappings are distinct. Suppose that $\hat{\sigma}_i \hat{\tau}_j = \hat{\sigma}_l \hat{\tau}_k$ on E. Then, as $K \subset E$, this is also true on K. Given that $\hat{\tau}_{j|K} = \hat{\tau}_{k|K} = \mathrm{id}_K$, and $\hat{\sigma}_{i|K} = \sigma_i$ and $\hat{\sigma}_{l|K} = \sigma_l$, we have $\sigma_i = \sigma_l$, i.e., $i = l$. Also, $\hat{\sigma}_i = \hat{\sigma}_l$ and $\hat{\sigma}_i$ is a monomorphism, hence $\hat{\tau}_j(x) = \hat{\tau}_k(x)$, and this is so for any $x \in E$. It follows that $\tau_j = \tau_k$, and thus that $j = k$. We have shown that the F-monomorphisms $\hat{\sigma}_i \hat{\tau}_j$, restricted to E, are distinct and so form the set of F-monomorphisms from E into C. Hence, using Proposition 10.2 again, we have

$$T_{E/F}(x) = \sum_{i=1}^{n} \sum_{j=1}^{m} \hat{\sigma}_i \hat{\tau}_j(x) = T_{K/F}(T_{E/K}(x)),$$

for all $x \in E$.

For the norm we proceed in an analogous way:

$$N_{E/F}(x) = \prod_{i=1}^{n} \prod_{j=1}^{m} \hat{\sigma}_i \hat{\tau}_j(x) = \prod_{i=1}^{n} \hat{\sigma}_i \left(\prod_{j=1}^{m} \hat{\tau}_j(x) \right) = N_{K/F}\left(N_{E/K}(x)\right).$$

This ends the proof. □

Remark Corollary 10.1 supposes that E is a splitting field of the minimal polynomial of x over F. Using Corollary 10.2 we may show that Corollary 10.1 is true if the field E only <u>contains</u> a splitting field K of the minimal polynomial (providing that E is a separable extension of F). Indeed, we have the tower of fields $F \subset K \subset E$ and $N_{E/F}(x) = N_{K/F} \circ N_{E/K}(x)$. As $x \in K$, we have $N_{E/K}(x) = x^{[E:K]}$. Thus

$$N_{E/F}(x) = \left(N_{K/F}(x)\right)^{[E:K]} = \left(\prod_{i=1}^{d} x_i \right)^{\frac{[K:F]}{d}[E:K]} = \left(\prod_{i=1}^{d} x_i \right)^{\frac{[E:F]}{d}}.$$

For the trace the calculation is analogous.

We now suppose that E/F is not only separable but also normal, i.e., E is a Galois extension of F.

Corollary 10.3 *If E is a finite Galois extension of the field F, then for all $x \in E$*

$$N_{E/F}(x) = \prod_{\sigma \in Gal(E/F)} \sigma(x) \qquad \textit{and} \qquad T_{E/F}(x) = \sum_{\sigma \in Gal(E/F)} \sigma(x).$$

PROOF As E is a finite separable extension F, there are $n = [E:F]$ F-monomorphisms $\sigma_1, \ldots, \sigma_n$ of E into an algebraic closure C of F. However, E is a normal extension of F and C an algebraic closure of F, with C/E, therefore $\sigma_i(E) = E$, for $i = 1, \ldots, n$ (Proposition 5.2) and so $\sigma_1, \ldots, \sigma_n \in Gal(E/F)$. As the cardinality of $Gal(E/F)$ is n, the σ_i form the Galois group. The result now follows from Proposition 10.2. □

We conclude this section with a result concerning the bilinear form B defined in Exercise 10.1:

$$B : E \times E \longrightarrow F : (x_1, x_2) \longmapsto T_{E/F}(x_1 x_2).$$

Corollary 10.4 *If E is a finite separable extension of F, then the bilinear form B is nondegenerate.*

PROOF Suppose that B is degenerate, then there exists a nonzero $x_1 \in E$ such that $T(x_1 x_2) = 0$, for all $x_2 \in E$. If $x \in E$, then there exists $x_2 \in E$ such that $x_1 x_2 = x$, so $T(x) = 0$, for all $x \in E$. However, this means that $\sum_{i=1}^n \sigma_i(x) = 0$, for all $x \in E$, which contradicts Dedekind's lemma (Theorem 8.1). Therefore B is nondegenerate. □

10.2 Discriminant of a polynomial

In Section 8.5 we introduced the discriminant of a polynomial. Also, we defined the resultant of two polynomials and stated an important relation between these two concepts. Our aim in this section is to study these concepts in more detail. In order to make the reading easier, we regive the definitions.

Resultants

We fix $m, n \in \mathbf{N}^*$. Let F be a field, $f \in F_m[X]$, with coefficients $a_0, \ldots, a_m$ and $g \in F_n[X]$, with coefficients $b_0, \ldots, b_n$. We define the square $n+m$ *Sylvester matrix* $S_{m,n}(f,g)$ (or $S(f,g)$), if m and n are understood) as follows:

$$S_{m,n}(f,g) = \begin{bmatrix} a_m & a_{m-1} & a_{m-2} & \ldots & 0 & 0 & 0 \\ 0 & a_m & a_{m-1} & \ldots & 0 & 0 & 0 \\ \vdots & \vdots & \vdots & & & & \\ 0 & 0 & 0 & \ldots & a_1 & a_0 & 0 \\ 0 & 0 & 0 & \ldots & a_2 & a_1 & a_0 \\ b_n & b_{n-1} & b_{n-2} & \ldots & 0 & 0 & 0 \\ 0 & b_n & b_{n-1} & \ldots & 0 & 0 & 0 \\ \vdots & \vdots & \vdots & & & & \\ 0 & 0 & 0 & \ldots & b_1 & b_0 & 0 \\ 0 & 0 & 0 & \ldots & b_2 & b_1 & b_0 \end{bmatrix}$$

We obtain $S_{m,n}(f,g)$ by shifting the line vector of the coefficients of f successively to the right by $0, 1, \dots, n-1$ steps and the vector line of the coefficients of g successively to the right by $0, 1, \dots, m-1$ steps and then filling in the remaining places with 0.

Remark If $0 \leq \deg f = k < m$, then we have $a_m = a_{m-1} = \cdots = a_{k+1} = 0$ and if $f = 0$, then $a_i = 0$, for all i. We have an analogous situation if $\deg g \neq n$.

Here is an example. With $m = 3$ an $n = 2$, we have

$$S_{m,n}(f,g) = \begin{bmatrix} a_3 & a_2 & a_1 & a_0 & 0 \\ 0 & a_3 & a_2 & a_1 & a_0 \\ b_2 & b_1 & b_0 & 0 & 0 \\ 0 & b_2 & b_1 & b_0 & 0 \\ 0 & 0 & b_2 & b_1 & b_0 \end{bmatrix}$$

The *resultant* of f and g, which we note $R_{m,n}(f,g)$, (or $R(f,g)$, if m and n are understood) is the determinant $|S_{m,n}(f,g)|$. Clearly,

$$R_{n,m}(g,f) = (-1)^{mn} R_{m,n}(f,g). \tag{10.4}$$

Remark We may consider the a_i and b_j as variables. In this way we obtain a mapping from $F^{m+1} \times F^{n+1}$ into F, which is mn-homogeneous.

Proposition 10.3 *Let $f \in F_m[X]$ et $g \in F_n[X]$. If $m \geq n$ and $h \in F_{m-n}[X]$, then*

$$R(f + hg, g) = R(f,g).$$

In the same way, if $m \leq n$ and $h \in F_{n-m}[X]$, then

$$R(f, g + hf) = R(f,g).$$

PROOF Let us begin with the case $m \geq n$. If $h(X) = c$ is a constant polynomial, then the coefficients of $f + hg$ are

$$a_m, a_{m-1}, \dots, a_n + cb_n, a_{n-1} + cb_{n-1}, \dots, a_0 + cb_0, 0, \dots, 0.$$

From this, we see that the first line of $S(f + hg, g)$ is the first line of $S(f,g)$ plus c multiplied by a line in the bloc of the b_j. This also applies to the lines $2, \dots n$, so in this case we have $R(f + hg, g) = R(f,g)$.

Now suppose that $h = cX$. Then the coefficients of $f + hg$ are

$$a_m, a_{m-1}, \dots, a_{n+1} + cb_n, a_n + cb_{n-1}, \dots, a_1 + cb_0, a_0, 0 \dots, 0.$$

Again the first line $S(f + hg, g)$ is the first line of $S(f,g)$ plus c multiplied by a line in the bloc of the b_j. This also applies to the lines $2, \dots n$, so in this case too we have $R(f + hg, g) = R(f,g)$.

If $h = c_0 + c_1 X$, then

$$R(f + hg, g) = R(f + (c_0 + c_1 X)g, g) = R((f + c_0 g) + c_1 Xg, g) = R(f + c_0 g, g) = R(f,g).$$

Continuing in the same way, we obtain the first result. The second result is obtained in an analogous way. □

In the next proposition we consider the case where $\deg g < n$ or $\deg f < m$. This result is useful in proving the fundamental theorem which follows.

Proposition 10.4 *Let $f \in F_m[X]$ and $g \in F_n[X]$. If $0 \leq \deg g = k \leq m = \deg f$, then*

$$R_{m,n}(f,g) = a_m^{n-k} R_{m,k}(f,g). \tag{10.5}$$

If, on the other hand, $0 \leq \deg f = k \leq n = \deg g$, then

$$R_{m,n}(f,g) = (-1)^{(m-k)n} b_n^{m-k} R_{k,n}(f,g). \tag{10.6}$$

PROOF Let us look at the first equation. If $k = n$, then there is nothing to prove, so let us suppose that $k < n$. Then $b_n = 0$ and the only nonzero element in the first column of the matrix $S_{m,n}(f,g)$ is a_m. The submatrix obtained by eliminating the first line and the first column $S_{m,n}(f,g)$ is $S_{m,n-1}(f,g)$. If we continue the process, then we finally obtain the first formula.

Now we look at the second formula. Using the formulas (10.4) and (10.5) we have

$$\begin{aligned} R_{m,n}(f,g) &= (-1)^{mn} R_{m,n}(g,f) \\ &= (-1)^{mn} b_n^{m-k} R_{n,k}(g,f) \\ &= (-1)^{mn} b_n^{m-k} (-1)^{nk} R_{k,n}(f,g) \\ &= (-1)^{(m-k)n} b_n^{m-k} R_{k,n}(f,g). \end{aligned}$$

This ends the proof. □

We now turn to one of the most important results of this section. We will see that there is a relation between the roots of the polynomials f and g in a splitting field and the resultant.

Theorem 10.1 *Let $f \in F_m[X]$ and $g \in F_n[X]$. If $\deg f = m$, then*

$$R_{m,n}(f,g) = a_m^n \prod_{i=1}^{m} g(\xi_i),$$

where the ξ_i are the roots of f in some splitting field of f. On the other hand, if $\deg g = n$, then

$$R_{m,n}(f,g) = (-1)^{mn} b_n^m \prod_{j=1}^{n} f(\eta_j),$$

where the η_i are the roots of g in some splitting field of g.

PROOF We begin with the first formula and suppose that $n \geq m$ and that f has the roots $\xi_1, \ldots, \xi_m$ in some splitting field. We will use an induction on $s = \deg g$. If $s = 0$, then the matrix $S_{m,n}(f,g)$ is upper triangular and on the diagonal we have a_m n times and b_0 m times, therefore

$$R_{m,n}(f,g) = a_m^n b_0^n = a_m^n \prod_{i=1}^{m} g(\xi_i),$$

so the result is true for $s = 0$.

Now suppose that $0 < s \leq n$ and the result is true up to $s - 1$. Dividing g by f we obtain

$$g = fq + r,$$

with $\deg r < \deg f = m$. Then

$$\deg q = \deg fq - \deg f = \deg(g - r) - m \leq n - m.$$

From Proposition 10.3 we have

$$R_{m,n}(f,g) = R_{m,n}(f,g-fq) = R_{m,n}(f,r).$$

We set $\deg r = k < s$ and use Proposition 10.4 and the induction hypothesis.

Case 1: $r \neq 0$

$$\begin{aligned} R_{m,n}(f,r) &= a_m^{n-k} R_{m,k}(f,r) \\ &= a_m^{n-k} a_m^k \prod_{i=1}^m r(\xi_i) \\ &= a_m^n \prod_{i=1}^m g(\xi_i), \end{aligned}$$

and so the result is true for s.

Case 2: $r = 0$

In this case the last m lines of the matrix $S_{m,n}(f,r)$ are composed of zeros, hence $R_{m,n}(f,r) = 0$. In addition, for any root ξ_i of f, we have $g(\xi_i) = q(\xi_i)f(\xi_i) = 0$, which implies that ξ_i is also a root of g. This implies that the expression $\prod_{i=1}^m g(\xi_i)$ vanishes, so in this case also we have equality. Thus the result is true for s.

In both cases, the result is true for s, so by induction, the result is true for all $s \leq n$.

Now let us suppose that $m > n$. Then $g \in F_m[X]$ and, using Proposition 10.4, we have

$$R_{m,m}(f,g) = a_m^{m-n} R_{m,n}(f,g).$$

In addition, from what we have seen above,

$$R_{m,m}(f,g) = a_m^m \prod_{i=1}^m g(\xi_i).$$

Therefore,

$$a_m^{m-n} R_{m,n}(f,g) = a_m^m \prod_{i=1}^m g(\xi_i) \Longrightarrow R_{m,n}(f,g) = a_m^n \prod_{i=1}^m g(\xi_i).$$

Hence, for $m > n$ also the formula holds.

We now consider the second part of the theorem. We suppose that g has the roots $\eta_1, \ldots, \eta_n$ in some splitting field. Then,

$$\begin{aligned} R_{m,n}(f,g) &= (-1)^{mn} R_{n,m}(g,f) \\ &= (-1)^{mn} b_n^m \prod_{j=1}^n f(\eta_j), \end{aligned}$$

where we have used the first part of the theorem. □

Corollary 10.5 *If* $\deg f = m$, $\deg g = n$ *and, in a splitting field of* f *and* g*, the roots of* f *(resp.* g*) are* $\xi_1, \dots \xi_m$ *(resp.* $\eta_1, \dots, \eta_n$*), then*

$$R_{m,n}(f,g) = a_m^n b_n^m \prod_{i=1}^{m}\prod_{j=1}^{n}(\xi_i - \eta_j).$$

PROOF It is sufficient to notice that

$$g(X) = b_n(X-\eta_1)\cdots(X-\eta_n)$$

and then apply the first part of the theorem. □

Discriminants

Let $f(X) = \sum_{i=0}^m a_i X^i$ a polynomial with coefficients in a field F. We suppose that the degree m of f is greater than 1 and that f has the roots $\xi_1, \dots, \xi_m$ in some splitting field E. The *discriminant* of f is defined by

$$\Delta(f) = a_m^{2m-2}\prod_{1\le i<j\le m}(\xi_i - \xi_j)^2.$$

We will see in the theorem which follows that this definition is unambiguous: it does not depend on the splitting field chosen.

It is useful to notice that $\Delta(f)$ belongs to F. Indeed, the multivariate polynomial $A = a_m^{2m-2}\prod_{1\le i<j\le m}(X_i - X_j)^2$ is a symmetric polynomial in $F[X_1, \dots, X_n]$. Consequently, from Corollary B.1, $\Delta(f) \in F$. Using the same corollary, we may also say that, if $f \in R[X]$, where R is an integral domain, then $\Delta(f) \in R$.

In Section 8.5 we stated the following result linking the discriminant of a polynomial and the resultant of the polynomial and its derivative. Here we prove this result. it.

Theorem 10.2 *If char* $F = 0$ *or char* $F = p > 0$ *and* $p \not| m$*, where* $\deg f = m$*, then*

$$\Delta(f) = (-1)^{m(m-1)/2} a_m^{-1} R_{m,m-1}(f,f').$$

PROOF We have

$$f(X) = a_m\prod_{i=1}^m (X-\xi_i) \Longrightarrow f'(\xi_i) = a_m\prod_{j\neq i}(\xi_i - \xi_j).$$

Hence,

$$\begin{aligned}
R_{m,m-1}(f,f') &= a_m^{m-1}\prod_{i=1}^m f'(\xi_i)\\
&= a_m^{2m-1}\prod_{i=1}^m\prod_{j\neq i}(\xi_i-\xi_j)\\
&= a_m^{2m-1}\prod_{1\le i<j\le m}(\xi_i-\xi_j)(\xi_j-\xi_i)\\
&= a_m^{2m-1}(-1)^{m(m-1)/2}\prod_{1\le i<j\le m}(\xi_i-\xi_j)^2\\
&= (-1)^{m(m-1)/2}a_m\Delta(f)
\end{aligned}$$

and the result follows. $\square$

If char $F = p > 0$ and $p|m$, then $\deg f' = k < m-1$. In this case, if $k \neq -\infty$, then

$$R_{m,m-1}(f,f') = a_m^{m-1-k} R_{m,k}(f,f')$$

and

$$\Delta(f) = (-1)^{m(m-1)/2} a_m^{m-k-2} R_{m,k}(f,f').$$

Remark The polynomial f has a multiple root if and only if $\Delta(f) = 0$. From the formulas here, we see that we are able to determine the existence of a multiple root only taking into account the coefficients of f. We should also notice that the formulas show that the discriminant belongs to the field F.

Example 1: $\Delta(b + aX + X^n)$

Our aim in this section is to determine a formula for the discriminant of the polynomial $f(X) = a + bX + X^n \in F[X]$. We will suppose that E is a field containing F and the roots of f.

Lemma 10.1 *If $f \in F[X]$ is monic and $\alpha_0 \in E$, then*

$$\Delta\big((-\alpha_0 + X)f(X)\big) = f(\alpha_0)^2 \Delta(f(X)).$$

PROOF Let $\alpha_1, \ldots, \alpha_n$ be the roots of f in $\mathbf{C}$. Then the roots of $(-\alpha_0+X)f(X)$ are $\alpha_0, \alpha_1, \ldots, \alpha_n$ and

$$\begin{aligned}
\Delta\big((-\alpha_0 + X)f(X)\big) &= \prod_{0 \leq i < j \leq n} (\alpha_i - \alpha_j)^2 \\
&= \prod_{1 \leq j \leq n} (\alpha_0 - \alpha_j)^2 \prod_{1 \leq i < j \leq n} (\alpha_i - \alpha_j)^2 \\
&= f(\alpha_0)^2 \Delta(f(X)).
\end{aligned}$$

This ends the proof. $\square$

We need a second preliminary result.

Lemma 10.2 *If $f(X) = c + X^n \in F[X]$, then*

$$\Delta(f) = (-1)^{\frac{n(n-1)}{2}} n^n c^{n-1}.$$

PROOF Let $\alpha_1, \ldots, \alpha_n$ be the roots of f in E. Then

$$\alpha_1 \cdots \alpha_n = (-1)^n c. \tag{10.7}$$

Also,

$$f(X) = \prod_{i=1}^n (-\alpha_i + X) \Longrightarrow f'(X) = \sum_{i=1}^n \prod_{j \neq i} (-\alpha_j + X) \Longrightarrow f'(\alpha_i) = \prod_{j \neq i} (-\alpha_j + \alpha_i).$$

It now follows that

$$(-1)^{\frac{n(n-1)}{2}} \Delta(f) = \prod_{i=1}^n f'(\alpha_i) = \prod_{i=1}^n n\alpha_i^{n-1}$$

and, using the identity (10.7), we obtain

$$(-1)^{\frac{n(n-1)}{2}}\Delta(f) = n^n(\alpha_1 \cdots \alpha_n)^{n-1} = n^n(-1)^{n(n-1)}c^{n-1} = n^n c^{n-1},$$

hence the result. □

We are now in a position to consider the polynomial $f(X) = b + aX + X^n \in F[X]$. The following theorem provides a formula for the discriminant of f involving only its coefficients.

Theorem 10.3 *For the polynomial $f(X) = b + aX + X^n \in F[X]$, with $n \geq 2$, we have the formula*

$$\Delta(f) = (-1)^{\frac{(n-1)(n-2)}{2}}(n-1)^{n-1}a^n + (-1)^{\frac{n(n-1)}{2}}n^n b^{n-1}.$$

PROOF For the the case where $a = 0$ we may use Lemma 10.2, so we may suppose that $a \neq 0$. We begin with the case where $b = 0$. Then, using Lemmas 10.1 and 10.2, we have

$$\begin{aligned}
\Delta(f) &= \Delta X(a + X^{n-1}) \\
&= a^2\Delta(a + X^{n-1}) \\
&= a^2(-1)^{\frac{(n-1)(n-2)}{2}}(n-1)^{n-1}a^{n-2} \\
&= (-1)^{\frac{(n-1)(n-2)}{2}}(n-1)^{n-1}a^n \\
&= (-1)^{\frac{(n-1)(n-2)}{2}}(n-1)^{n-1}a^n + (-1)^{\frac{n(n-1)}{2}}n^n b^n,
\end{aligned}$$

because $b = 0$.

Now we turn to the case where $b \neq 0$. The calculations are much longer. If $\alpha_1, \ldots, \alpha_n$ are the roots of f, then, for all i,

$$b + a\alpha_i + \alpha_i^n = 0 \qquad \text{and} \qquad \alpha_1 \cdots \alpha_n = (-1)^n b. \tag{10.8}$$

As $b \neq 0$, none of the roots α_i vanish. Now, proceeding as in the proof of Lemma 10.2, and setting $A = (-1)^{\frac{n(n-1)}{2}}\Delta(f)$, we have

$$A = \prod_{i=1}^{n} f'(\alpha_i) = \prod_{i=1}^{n}(a + n\alpha_i^{n-1}) = \prod_{i=1}^{n}\frac{a\alpha_i + n\alpha_i^n}{\alpha_i}.$$

Using the expressions (10.8), we continue:

$$
\begin{aligned}
A &= \frac{(-1)^n}{b}\prod_{i=1}^{n}(a\alpha_i + n\alpha_i^n) \\
&= \frac{(-1)^n}{b}\prod_{i=1}^{n}(a\alpha_i + n(-b - a\alpha_i)) \\
&= \frac{(-1)^n}{b}\prod_{i=1}^{n}(-bn - a(n-1)\alpha_i) \\
&= \frac{(-1)^n}{b}\prod_{i=1}^{n}\left((-\frac{bn}{a(n-1)} - \alpha_i)a(n-1)\right) \\
&= \frac{(-1)^n}{b}a^n(n-1)^n\prod_{i=1}^{n}\left(-\frac{bn}{a(n-1)} - \alpha_i\right) \\
&= \frac{(-1)^n}{b}a^n(n-1)^n f(-\frac{bn}{a(n-1)}) \\
&= \frac{(-1)^n}{b}a^n(n-1)^n\left(b + a\left(-\frac{bn}{a(n-1)}\right) + \left(-\frac{bn}{a(n-1)}\right)^n\right)
\end{aligned}
$$

We now simplify the expression on the right-hand side:

$$
\begin{aligned}
A &= \frac{(-1)^n}{b}\left((-1)^n b^n n^n - a^n bn(n-1)^{(n-1)} + a^n b(n-1)^n\right) \\
&= (-1)^n\left((-1)^n b^{n-1}n^n - a^n n(n-1)^{n-1} + a^n(n-1)^n\right) \\
&= (-1)^n\left((-1)^n b^{n-1}n^n - a^n(n-1)^{n-1}\right) \\
&= b^{n-1}n^n - (-1)^n(n-1)^{n-1}a^n \\
&= (-1)^{n-1}(n-1)^{n-1}a^n + n^n b^{n-1} \\
&= (-1)^{1-n}(n-1)^{n-1}a^n + n^n b^{n-1}
\end{aligned}
$$

Multiplying through by $(-1)^{\frac{n(n-1)}{2}}$, we obtain the desired result. □

Applications We have

- for $n = 2$, $\Delta(f) = a^2 - 4b$;
- for $n = 3$, $\Delta(f) = -4a^3 - 27b^2$;
- for $n = 4$, $\Delta(f) = -27a^4 + 256b^3$.

Example 2: $\Delta(\Phi_p)$

Proposition 10.5 *If p is an odd prime, then*

$$\Delta(\Phi_p) = (-1)^{\frac{p-1}{2}}p^{p-2}.$$

PROOF Let ζ be a primitive pth root of unity. Then

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

Substituting ζ^i for X, since $\Phi_p(\zeta^i) = 0$, we obtain

$$\begin{aligned}\prod_{i=1}^{p-1} \Phi'_p(\zeta^i) &= \prod_{i=1}^{p-1} \frac{p\zeta^{i(p-1)}}{(-1+\zeta^i)} \\ &= \frac{p^{p-1}}{\prod_{i=1}^{p-1}(-1+\zeta^i)} \\ &= \frac{p^{p-1}}{(-1)^{p-1}\Phi_p(1)} = p^{p-2}.\end{aligned}$$

(The second equality follows from the relations $\sum_{i=1}^{p-1} i = \frac{p(p-1)}{2}$ and $\zeta^p = 1$ and the third from the identity $\Phi_p(X) = 1 + X + \cdots + X^{p-1}$.)
Also,

$$\begin{aligned}\Phi_p(X) = \prod_{i=1}^{p-1}(-\zeta^i + X) &\implies \Phi'_p(X) = \sum_{i=1}^{p-1}\prod_{j\neq i}(-\zeta^j + X) \\ &\implies \Phi'_p(\zeta^i) = \prod_{j\neq i}(-\zeta^j + \zeta^i) \\ &\implies \prod_{i=1}^{p-1} \Phi'_p(\zeta^i) = \prod_{i=1}^{p-1}\prod_{j\neq i}(-\zeta^j + \zeta^i) = \prod_{j\neq i}(-\zeta^j + \zeta^i).\end{aligned}$$

Therefore,

$$\Delta(\Phi_p) = \prod_{j<i}(\zeta^j - \zeta^i)^2 = (-1)^{\frac{(p-2)(p-1)}{2}} \prod_{j\neq i}(\zeta^j - \zeta^i) = (-1)^{\frac{p-1}{2}} p^{p-2}.$$

This ends the proof. □

10.3 General discriminants

We have seen the notion of the discriminant of a polynomial. Here we extend this notion, although at first it will not be clear how the new concept is actually an extension of the previous one. This we will see later.

Let E be a finite separable extension of degree n of a field F. We note $\sigma_1, \ldots, \sigma_n$ the n F-monomorphisms of E into an algebraic closure C of E and we take n elements $\alpha_1, \ldots, \alpha_n$ in E. We define the *discriminant* of the set $\alpha_1, \ldots, \alpha_n$ by

$$\mathrm{disc}_{E/F}(\alpha_1, \ldots, \alpha_n) = |\sigma_i(\alpha_j)|^2,$$

i.e., the square of the determinant of the matrix $S = (\sigma_i(\alpha_j))$. As we take the square of the determinant, the order of the σ_i and α_j do not have an effect on the value of the discriminant. We will also see that the discriminant does not depend on the algebraic closure we use, hence we are justified in speaking of the discriminant.

Exercise 10.2 *Show that*

- *$disc_{E/F}(x\alpha_1, \ldots, \alpha_n) = x^2 disc_{E/F}(\alpha_1, \ldots, \alpha_n)$, for any $x \in F$;*
- *If β is a linear combination of $\alpha_2, \ldots, \alpha_n$, with coefficients in F, then $disc_{E/F}(\alpha_1 + \beta, \alpha_2, \ldots, \alpha_n) = disc_{E/F}(\alpha_1, \ldots, \alpha_n)$.*

The next result is useful as we will see later on.

Proposition 10.6 *Suppose that $U = \{u_1, \ldots, u_n\}$ and $V = \{v_1, \ldots, v_n\}$ are sets of vectors in E such that $u_i = \sum_{j=1}^n a_{ij} v_j$, with $a_{ij} \in F$. Then*

$$disc_{E/F}(u_1, \ldots, u_n) = (\det(a_{ij}))^2 disc_{E/F}(v_1, \ldots, v_n).$$

PROOF By definition

$$\mathrm{disc}_{E/F}(u_1, \ldots, u_n) = (\det(\sigma_i(u_j)))^2 ,$$

where the σ_i are the n F-monomorphisms of E into an algebraic closure of E. Now

$$\sigma_i(u_j) = \sigma_i(\sum_{k=1}^n a_{jk} v_k) = \sum_{k=1}^n a_{jk} \sigma_i(v_k).$$

We define the matrices $X = (\sigma_i(u_j))$, $A = (a_i j)$ and $Y = (\sigma_i(v_j))$. Then $X = YA^t$ and so $(\det(X))^2 = (\det(YA^t))^2$, i.e.,

$$\mathrm{disc}_{E/F}(u_1, \ldots, u_n) = (\det(a_{ij}))^2 \mathrm{disc}_{E/F}(v_1, \ldots, v_n),$$

as required. □

The next result will enable us to show that the discriminant is indeed independant of the algebraic closure of E chosen.

Proposition 10.7 *We have*

$$disc_{E/F}(\alpha_1, \ldots, \alpha_n) = |T_{E/F}(\alpha_i \alpha_j)|,$$

where $|T_{E/F}(\alpha_i \alpha_j)|$ is the determinant of the matrix $T = (T_{E/F}(\alpha_i \alpha_j))$.

PROOF As above let us set $S = (\sigma_i(\alpha_j))$. Then

$$S^t S = \left(\sum_{k=1}^n \sigma_k(\alpha_i \alpha_j) \right) = \left(T_{E/F}(\alpha_i \alpha_j) \right),$$

hence

$$|S|^2 = |T_{E/F}(\alpha_i \alpha_j)|.$$

This ends the proof. □

Remark From the proposition we see that $\mathrm{disc}_{E/F}(\alpha_1, \ldots, \alpha_n)$ is independant of the algebraic closure chosen. Also, as $T_{E/F}(\alpha_i \alpha_j) \in F$, for $1 \leq i, j \leq n$, we have $\mathrm{disc}_{E/F}(\alpha_1, \ldots, \alpha_n) \in F$.

The discriminant can help us to determine whether n elements in an extension of degree n form a basis of the extension.

Proposition 10.8 *The elements $\alpha_1, \dots, \alpha_n$ form a basis of E over F if only if their discriminant does not vanish.*

PROOF Let $\sum_{j=1}^n c_j\alpha_j = 0$, where the $c_j \in F$ and at least one $c_j \neq 0$. Then, for $1 \leq i \leq n$, $\sum_{j=1}^n c_j\sigma_i(\alpha_j) = 0$. This implies that the columns of the matrix $S = (\sigma_i(\alpha_j))$ are dependant. It follows that $\mathrm{disc}_{E/F}(\alpha_1, \dots, \alpha_n) = 0$.

Now suppose that the α_i are independant and so form a basis of E over F. If $\mathrm{disc}_{E/F}(\alpha_1, \dots, \alpha_n) = 0$, then the rows of the matrix S are dependant, hence there exist elements $c_1, \dots, c_n \in F$, with at least one $c_j \neq 0$, such that $\sum_{i=1}^n c_i\sigma_i(\alpha_j) = 0$, for $1 \leq j \leq n$. As the α_j form a basis of E over F, we have $\sum_{i=1}^n c_i\sigma_i(u) = 0$, for all $u \in E$; therefore the monomorphisms σ_i are dependant. However, this contradicts Corollary 8.1. Hence $\mathrm{disc}_{E/F}(\alpha_1, \dots, \alpha_n) \neq 0$. □

In Section 8.5 we defined the discriminant of a polynomial. There is a relation between this notion and the notion of discriminant which we have defined here.

Proposition 10.9 *Let E be a finite separable extension of a field F; then there exists $\alpha \in E$ such that $E = F(\alpha)$ (Proposition 3.4). If $m = m(\alpha, F)$ and $\deg m = n$, then the elements $1, \alpha, \dots, \alpha^{n-1}$ form a basis of E over F. We have*

$$disc_{E/F}(1, \alpha, \dots, \alpha^{n-1}) = \Delta(m) = (-1)^{\frac{n(n-1)}{2}} N_{E/F}\big(m'(\alpha)\big).$$

PROOF Let C be an algebraic closure of E and $\sigma_1, \dots, \sigma_n$ the n F-monomorphisms from E into C. Since $E = F(\alpha)$, each σ_i is determined $\sigma_i(\alpha)$. Moreover, α is a root of $m \in F[X]$, so $\sigma_i(\alpha)$ is also a root of m. If $\alpha = \alpha_1, \alpha_2, \dots, \alpha_n$ are the roots of m, then we may suppose, without loss of generality, that $\sigma_i(\alpha) = \alpha_i$. Consequently, $\sigma_i(\alpha^j) = \alpha_i^j$ and $\mathrm{disc}_{E/F}(1, \alpha, \dots, \alpha^{n-1})$ is the square of the determinant of the matrix

$$S = \begin{pmatrix} 1 & \alpha_1 & \alpha_1^2 & \dots & \alpha_1^{n-1} \\ 1 & \alpha_2 & \alpha_2^2 & \dots & \alpha_2^{n-1} \\ \vdots & \vdots & \vdots & & \vdots \\ 1 & \alpha_n & \alpha_n^2 & \dots & \alpha_n^{n-1} \end{pmatrix}$$

However, S is a Vandermonde matrix, therefore

$$|S|^2 = \prod_{i<j}(\alpha_i - \alpha_j)^2 = \Delta(m).$$

Moreover,

$$\prod_{i<j}(\alpha_i - \alpha_j)^2 = (-1)^{\frac{n(n-1)}{2}} \prod_{i\neq j}(\alpha_i - \alpha_j)$$

and, from Proposition 10.2,

$$N_{E/F}\big(m'(\alpha)\big) = \prod_{i=1}^n \sigma_i\big(m'(\alpha)\big).$$

Now, $\sigma_i\big(m'(\alpha)\big) = m'\big(\sigma_i(\alpha)\big)$, because $m \in F[X]$, thus

$$N_{E/F}\big(m'(\alpha)\big) = \prod_{i=1}^n m'\big(\sigma_i(\alpha)\big) = \prod_{i=1}^n m'(\alpha_i).$$

Finally, as $m(X) = \prod_{i=1}^{n}(-\alpha_i + X)$, we have

$$m'(\alpha_i) = \prod_{j\neq i}(-\alpha_j + \alpha_i)$$

and so

$$\begin{aligned} N_{E/F}\big(m'(\alpha)\big) &= \prod_{i=1}^{n}\prod_{j\neq i}(-\alpha_j + \alpha_i) \\ &= \prod_{j\neq i}(-\alpha_j + \alpha_i) \\ &= (-1)^{\frac{n(n-1)}{2}}\prod_{i<j}(\alpha_i - \alpha_j)^2, \end{aligned}$$

which implies that

$$\Delta(m) = (-1)^{\frac{n(n-1)}{2}} N_{E/F}\big(m'(\alpha)\big).$$

This ends the proof. □

Remark From Proposition 10.9 and the calculation of the discriminant of the pth cyclotomic polynomial Φ_p for p an odd prime (Proposition 10.5), we obtain

$$\mathrm{disc}_{\mathbf{Q}(\zeta)/\mathbf{Q}}(1,\zeta,\ldots,\zeta^{p-2}) = (-1)^{\frac{p-1}{2}}p^{p-2},$$

where ζ is a primitive pth root of unity, because Φ_p is the minimal polynomial of ζ over $\mathbf{Q}$.

We now use the previous proposition and the notion of norm and trace to calculate the discriminant of the p^rth cyclotomic polynomial, where $r \in \mathbf{N}^*$.

Corollary 10.6 *We have*

$$\Delta(\Phi_{p^r}) = (-1)^c p^{p^{r-1}(r(p-1)-1)},$$

where $c = \frac{\phi(p^r)}{2}$*, if* p *is odd or* $r > 1$*, and* $c = 0$ *otherwise. (*ϕ *is the Euler function.)*

PROOF Let ζ be a primitive p^rth root of unity. Setting $n = \phi(p^r) = p^{r-1}(p-1)$, from Proposition 10.9

$$\Delta(\Phi_{p^r}) = \mathrm{disc}_{\mathbf{Q}(\zeta)/\mathbf{Q}}(1,\zeta,\ldots,\zeta^{n-1}) = (-1)^{\frac{n(n-1)}{2}} N_{\mathbf{Q}(\zeta)/\mathbf{Q}}\big(\Phi'_{p^r}(\zeta)\big).$$

We now calculate the norm. First, using Exercise 7.4, we have

$$\Phi_{p^r}(X) = \Phi_p(X^{p^{r-1}}) = \frac{X^{p^r}-1}{X^{p^{r-1}}-1} \Longrightarrow \Phi'_{p^r}(\zeta) = \frac{p^r\zeta^{p^r-1}(\zeta^{p^{r-1}}-1)}{(\zeta^{p^{r-1}}-1)^2},$$

because $\zeta^{p^r} - 1 = 0$. Hence,

$$\Phi'_{p^r}(\zeta) = \frac{p^r\zeta^{p^r-1}}{\zeta^{p^{r-1}}-1}.$$

To calculate $N_{\mathbf{Q}(\zeta)/\mathbf{Q}}\big(\Phi'_{p^r}(\zeta)\big)$ we use the multipliplicity of the norm. To begin, we determine $N_{\mathbf{Q}(\zeta)/\mathbf{Q}}(\zeta^{p^r-1})$. This norm is the product of all the primitive p^rth roots of unity (Corollary

10.1), i.e., $(-1)^n$ times the constant term of Φ_{p^r}. However, $\Phi_{p^r}(X) = \Phi_p(X^{p^{r-1}})$ (Exercise 7.4) and $\Phi_p(X) = 1 + \cdots + X^{p-1}$, hence

$$N_{\mathbf{Q}(\zeta)/\mathbf{Q}}(\zeta^{p^r-1}) = (-1)^n.$$

Let us now calculate $N_{\mathbf{Q}(\zeta)/\mathbf{Q}}(\zeta^{p^{r-1}}-1)$. To do so we initially notice that $\zeta^{p^{r-1}}$ is a primitive pth root of unity. ($\zeta^{p^{r-1}}$ is clearly a pth root of unity; if $(\zeta^{p^{r-1}})^k = 1$, with $k < p$, then there is a power u of ζ less that p^r such that $p^u = 1$, which is impossible, so $\zeta^{p^{r-1}}$ is a primitive pth root of unity.) Let ξ be a primitive pth root of unity. We apply Corollary 10.3 to the tower of fields $\mathbf{Q} \subset \mathbf{Q}(\xi) \subset \mathbf{Q}(\zeta)$ to obtain

$$N_{\mathbf{Q}(\zeta)/\mathbf{Q}}(\zeta^{p^{r-1}} - 1) = N_{\mathbf{Q}(\xi)/\mathbf{Q}} \circ N_{\mathbf{Q}(\zeta)/\mathbf{Q}(\xi)}(\zeta^{p^{r-1}} - 1).$$

Moreover,

$$N_{\mathbf{Q}(\zeta)/\mathbf{Q}(\xi)}(\zeta^{p^{r-1}} - 1) = (\zeta^{p^{r-1}} - 1)^{p^{r-1}},$$

since $\zeta^{p^{r-1}} - 1 \in \mathbf{Q}(\xi)$ and

$$[\mathbf{Q}(\zeta) : \mathbf{Q}(\xi)] = \frac{[\mathbf{Q}(\zeta) : \mathbf{Q}]}{[\mathbf{Q}(\xi) : \mathbf{Q}]} = \frac{\phi(p^r)}{\phi(p)} = p^{r-1}.$$

Hence, we have to consider

$$N_{\mathbf{Q}(\xi)/\mathbf{Q}}\big((\zeta^{p^{r-1}} - 1)^{p^{r-1}}\big) = \big(N_{\mathbf{Q}(\xi)/\mathbf{Q}}(\zeta^{p^{r-1}} - 1)\big)^{p^{r-1}}.$$

Since $\zeta^{p^{r-1}}$ is a primitive pth root of unity, its minimal polynomial over $\mathbf{Q}$ is Φ_p. The minimal polynomial of $\zeta^{p^{r-1}} - 1$ over $\mathbf{Q}$ is $\Phi_p(1 - X)$, which has the splitting field $\mathbf{Q}(\xi)$. Therefore, from Corollary 10.1,

$$N_{\mathbf{Q}(\xi)/\mathbf{Q}}(\zeta^{p^{r-1}} - 1) = \prod_{i=1}^{p-1}(\xi^i - 1) = (-1)^{p-1}\Phi_p(1) = (-1)^{p-1}p$$

and

$$N_{\mathbf{Q}(\zeta)/\mathbf{Q}}(\zeta^{p^{r-1}} - 1) = \big((-1)^{p-1}p\big)^{p^{p-1}} = (-1)^{(p-1)p^{r-1}}p^{p^{r-1}}.$$

To conclude

$$N_{\mathbf{Q}(\zeta)/\mathbf{Q}}\big(\Phi'_{p^r}(\zeta)\big) = \frac{p^{rn}N_{\mathbf{Q}(\zeta)/\mathbf{Q}}(\zeta^{p^r-1})}{N_{\mathbf{Q}(\zeta)/\mathbf{Q}}(\zeta^{p^{r-1}} - 1)} = \frac{p^{rn}(-1)^n}{(-1)^n p^{p^{r-1}}} = p^{p^{r-1}(r(p-1)-1)}.$$

If p is odd or $r > 1$, then $n = \phi(p^r)$ is even and the parity of $\frac{n(n-1)}{2}$ is that of $\frac{n}{2}$. On the other hand, if p is even and $r = 1$, then $n = \phi(2) = 1$, so $(-1)^{\frac{n(n-1)}{2}} = 1$. This finishes the proof. □

Further on we will generalize this result, i.e., we will determine $\Delta(\Phi_n)$, for any $n \in \mathbf{N}^*$.

Part II

Algebraic Number Theory

Chapter 11

Number fields

In our previous work we have already seen number fields, namely finite extensions of the rational numbers $\mathbf{Q}$. In this chapter we will look into these fields in more detail. In particular, we will study a natural subring occurring in such fields, namely that composed of algebraic integers.

11.1 Algebraic integers

We recall that an algebraic number is an element $\alpha \in \mathbf{C}$ for which there is a polynomial $f \in \mathbf{Z}[X]$, such that $f(\alpha) = 0$. The algebraic numbers form an extension of the field $\mathbf{Q}$. We say that $\alpha \in \mathbf{C}$ is an *algebraic integer* if there is a monic polynomial $f \in \mathbf{Z}[X]$, such that $f(\alpha) = 0$. An algebraic integer is an algebraic number, but the converse is not necessarily true; for example, as we will soon see, a rational number is an algebraic integer only if it is an integer.

Lemma 11.1 *Let $f \in \mathbf{Z}[X]$ and $f = gh$, with $g, h \in \mathbf{Q}[X]$. If f and g are monic, then $g, h \in \mathbf{Z}[X]$.*

PROOF Let m (resp. n) be the smallest positive integer such that mg (resp. nh) belongs to $\mathbf{Z}[X]$. Since g and h are monic, we claim that the contents $c(mg)$ and $c(nh)$ have both the value 1. (We recall that the content of a polynomial in $\mathbf{Z}[X]$ is the hcf of its coefficients.) If $c(mg) \neq 1$, then the coefficients of mg have a common divisor $d > 1$, such that $d|m$, since g is monic. If we set $m' = \frac{m}{d} < m$, then $m'g \in \mathbf{Z}[X]$, a contradiction, since m' is a positive integer. A similar argument applies to $c(nh)$. We claim that this in turn implies that $m = n = 1$: If $m > 1$ or $n > 1$, then $mn > 1$; for p a prime divisor of mn, we have

$$mnf = (mg)(nh) \Longrightarrow \bar{0} = \bar{mg}\bar{nh},$$

where the bars indicate the reductions modulo p. As $\mathbf{Z}_p[X]$ is an integral domain, because $\mathbf{Z}_p$ is a field, $\bar{mg} = \bar{0}$ or $\bar{nh} = \bar{0}$, which implies that p divides the coefficients of mg or the coefficients of nh. However, this is impossible, because $c(mg) = c(nh) = 1$. Therefore $m = n = 1$, as claimed. This implies that $g, h \in \mathbf{Z}[X]$. □

Theorem 11.1 *If $\alpha \in \mathbf{C}$ is an algebraic integer, then there is a monic polynomial $f \in \mathbf{Z}[X]$ such that $f(\alpha) = 0$. If f is of minimal degree, then f is irreducible in $\mathbf{Q}[X]$.*

PROOF If f is reducible in $\mathbf{Q}[X]$, then there are nonconstant polynomials $g, h \in \mathbf{Q}[X]$ such that $f = gh$. We may suppose that g and h are monic. From Lemma 11.1, we have $g, h \in \mathbf{Z}[X]$. In addition, $g(\alpha) = 0$ or $h(\alpha) = 0$. However, $\deg g < \deg f$ and $\deg h < \deg f$ and so we have a contradiction to the minimality of f. Thus f is irreducible. □

From this result we obtain an important corollary.

Corollary 11.1 *If $\alpha \in \mathbf{C}$ is an algebraic integer, then the polynomial $m = m(\alpha, \mathbf{Q})$ lies in $\mathbf{Z}[X]$.*

PROOF Let f be a monic polynomial in $\mathbf{Z}[X]$ of minimal degree such that $f(\alpha) = 0$. Then f is irreducible in $\mathbf{Q}[X]$ and $m|f$. It follows that $m = f$. □

Exercise 11.1 *Show that if E is a number field and $x \in E$ is an algebraic integer, then $N_{E/\mathbf{Q}}(x)$ and $T_{E/\mathbf{Q}}(x)$ are integers.*

We now consider the algebraic integers in $\mathbf{Q}$.

Theorem 11.2 *The number $\alpha \in \mathbf{Q}$ is an algebraic integer if and only if α is an integer.*

PROOF If $\alpha \in \mathbf{Z}$, then $f(X) = -\alpha + X \in \mathbf{Z}[X]$ and f is monic. Clearly $f(\alpha) = 0$, so α is an algebraic integer. Now suppose that $\alpha \in \mathbf{Q}$ is algebraic. If $m = m(\alpha, \mathbf{Q})$, then $m \in \mathbf{Z}[X]$ and $m(\alpha) = 0$. As α is a root of m, $g(X) = -\alpha + X$ divides m. Now, m is irreducible and so $g = m$; it follows that $m \in \mathbf{Z}[X]$, which implies that $\alpha \in \mathbf{Z}$. □

We will now establish criteria permitting us to decide whether a complex number is an algebraic integer. This will enable us to show that the collection of algebraic integers, which we will note $\mathcal{O}$, is a subring of the field of algebraic numbers.

Theorem 11.3 *The following conditions are equivalent:*

- **a.** *α is an algebraic integer;*
- **b.** *The additive group of the ring $\mathbf{Z}[\alpha]$ is finitely generated;*
- **c.** *α belongs to a subring R of $\mathbf{C}$ whose additive group is finitely generated;*
- **d.** *There is a finitely generated subgroup $G \neq \{0\}$ of the additive group of $\mathbf{C}$ such that $\alpha G \subset G$.*

PROOF **a.** $\Longrightarrow$ **b.** If α is a root of a monic polynomial $f \in \mathbf{Z}[X]$ and $\deg f = n$, then the additive group of $\mathbf{Z}[\alpha]$ is generated by the elements $1, \alpha, \dots, \alpha^{n-1}$.

b. $\Longrightarrow$ **c.** $\Longrightarrow$ **d.** These implications are elementary.

d. $\Longrightarrow$ **a.** Suppose that $a_1, \dots, a_n$ generate G. Then each term αa_i can be expressed as a linear combination of the a_i with coefficients in $\mathbf{Z}$. Therefore there is a matrix $M \in \mathcal{M}_n(\mathbf{Z})$ such that

$$\begin{pmatrix} \alpha a_1 \\ \vdots \\ \alpha a_n \end{pmatrix} = M \begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix} \Longrightarrow (\alpha I_n - M) \begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix} = 0.$$

As all the a_i are nonzero, $\det(\alpha I - M) = 0$. However, this determinant can be written :

$$\alpha^n + c_{n-1}\alpha^{n-1} + \cdots + c_1\alpha + c_0 = 0,$$

with $c_1 \in \mathbf{Z}$. Hence we have a monic polynomial $f \in \mathbf{Z}[X]$ such that $f(\alpha) = 0$. □

We may now show that the subset $\mathcal{O}$ of $\mathbf{C}$ composed of algebraic integers is a ring.

Corollary 11.2 *The subset $\mathcal{O}$ of $\mathbf{C}$ is a ring.*

PROOF It is sufficient to show that $\alpha + \beta$ and $\alpha\beta$ are in $\mathcal{O}$, when α and β are in $\mathcal{O}$. Let m, n be the degrees of the minimal polynomials of α, β. Then $1, \alpha, \ldots, \alpha^{m-1}$ is a generating set of the additive group of $\mathbf{Z}[\alpha]$ and $1, \beta, \ldots, \beta^{n-1}$ a generating set of the additive group of $\mathbf{Z}[\beta]$. The elements $\alpha^i\beta^j$, for $0 \leq i \leq m$ and $0 \leq j \leq n$, form a generating set of the additive group of the ring $\mathbf{Z}[\alpha, \beta]$. As $\mathbf{Z}[\alpha + \beta]$ is a subring of $\mathbf{Z}[\alpha, \beta]$, from 11.3 **c.**, $\alpha + \beta$ is algebraic. A similar argument shows that $\alpha\beta$ is also algebraic. □

We may generalize the notion of algebraic integer. If R is a commutative ring and S a subring, then we say that $\alpha \in R$ is *integral* over S if there is a monic polynomial $f \in S[X]$ such that $f(\alpha) = 0$. With Theorem 11.3 as model we may establish criteria allowing us to decide whether an element of R is integral over S.

Theorem 11.4 *If S is a subring of the commutative ring R, then the following conditions are equivalent for an element $\alpha \in R$:*

- **a.** *α is integral;*
- **b.** *The S-module $S[\alpha]$ is finitely generated;*
- **c.** *α belongs to a subring U of R containing S which is a finitely generated S-module;*
- **d.** *There is a nonzero finitely generated S-module N in R such that $\alpha N \subset N$.*

PROOF **a.** $\Longrightarrow$ **b**. If α is a root of a monic polynomial $f \in S[X]$ and $\deg f = n$, then α^n and all higher powers of α can be expressed as linear combinations (with coefficients in S) of lower powers of α. Hence $S[\alpha]$ is generated by the elements $1, \alpha, \ldots, \alpha^{n-1}$.

b. $\Longrightarrow$ **c.** $\Longrightarrow$ **d**. These implications are elementary.

d. $\Longrightarrow$ **a**. Suppose that $a_1, \ldots, a_n$ generate N. Then each term αa_i can be expressed as a linear combination of the a_i with coefficients in S. Therefore there is a matrix $M \in \mathcal{M}_n(S)$ such that

$$\begin{pmatrix} \alpha a_1 \\ \vdots \\ \alpha a_n \end{pmatrix} = M \begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix} \Longrightarrow (\alpha I_n - M) \begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix} = 0.$$

As all the a_i are nonzero, $\det(\alpha I - M) = 0$. However, this determinant can be written:

$$\alpha^n + c_{n-1}\alpha^{n-1} + \cdots + c_1\alpha + c_0 = 0,$$

with $c_1 \in S$. Hence we have a monic polynomial $f \in S[X]$ such that $f(\alpha) = 0$. □

Using arguments analogous to those employed in the proof of Corollary 11.2 we see that the collection of elements in R which are integral over S form a subring of R. We call this subring the *integral closure* of S in R. If the integral closure is S itself, then we say that S is integrally closed in R. If S is an integral domain and integrally closed in its field of fractions, then we say that S is integrally closed. Above we saw that $\mathbf{Z}$ is integrally closed in $\mathbf{Q}$, its field of fractions, so $\mathbf{Z}$ is integrally closed.

If S is a subring of the ring R such that every element of R is integral over S, then we say that R is integral over S.

The integral closure of S in R is naturally an S-module. We will now explore some of its properties. We first consider minimal polynomials over integrally closed domains.

Proposition 11.1 *Let R be an integrally closed domain, with field of fractions K, and L an extension of K. If $x \in L$ is integral over R and $\bar{L}$ is a splitting field of the minimal polynomial $m = m(x,K)$, then all the K-conjugates of x belong to $\bar{L}$ and are also integral over R. It follows that $m \in R[X]$. If S is the integral closure of R in L, then $S \cap K = R$.*

PROOF Let us write $\bar{R}$ for the integral closure of R in $\bar{L}$. Then $R \subset \bar{R} \cap K \subset R$, because R is integrally closed. Thus $\bar{R} \cap K = R$.

If $x \in L$ is integral over R, then there exists a monic polynomial $f \in R[X]$ such that $f(x) = 0$. The minimal polynomial $m = m(x,K)$ divides f. It follows that the K-conjugates of x (which are in $\bar{L}$) are also roots of f, hence integral over R and so belong to $\bar{R}$.

The coefficients of m are, up to sign, defined by the elementary symmetric functions evaluated at the K-conjugates of x and so belong to $\bar{R} \cap K = R$, i.e., $m \in R[X]$.

To finish, we consider the integral closure S of R in L. If $x \in S \cap K$, then $x \in R$, because R is integrally closed, so $S \cap K \subset R$. Clearly $R \subset S \cap K$, so we have $S \cap K = R$. □

The next result concerns the field of fractions of an integral closure of an integral domain.

Proposition 11.2 *Let R be an integral domain and K its field of fractions. If L is an algebraic extension of K and S the integral closure of R in L, then the field of fractions F of S is L.*

PROOF Clearly $R \subset S \subset F \subset L$. As $F \subset L$, we only need to show that $L \subset F$. Let $x \in L$. If $x = 0$, then there is nothing to prove, so let us suppose that this is not the case. As L is an algebraic extension of K, x is algebraic over K: there exists a polynomial $f(X) = \sum_{i=0}^{m} a_i X^i \in K[X]$ such that $f(x) = 0$. Then $\sum_{i=0}^{m} \frac{a_i}{a_m^i}(a_m x)^i = 0$. Setting $b_i = \frac{a_i}{a_m^i}$, we obtain a monic polynomial $g \in K[X]$ such that $g(a_m x) = 0$. Hence $s = a_m x \in S$. As K is the field of fractions of R, there exist $r_1, r_2 \in R$ such that $a_m = \frac{r_1}{r_2}$, so $x = \frac{s r_2}{r_1} \in F$, because $r_1, r_2 \in S$. Hence $L \subset F$. □

Corollary 11.3 *If R, K, L and S are as in Proposition 11.2, then every element of x of L has the form $\frac{s}{r}$, where $s \in S$ and $r \in R^*$.*

PROOF For $x = 0$ there is nothing to prove, so we suppose that this is not the case. In the proof of Proposition 11.2 we showed that, if $x \in L$, then $x = \frac{s r_2}{r_1}$, where $r_1, r_2 \in R$ and $s \in S$. As $R \subset S$, we have $s r_2 \in S$, hence the result. □

Exercise 11.2 *Show that there exists a basis of L over K composed of elements in S.*

We now introduce an interesting result, which we will use further on.

Theorem 11.5 *Let R be an integrally closed domain, K its field of fractions and L a separable extension of degree n of K. Suppose that S is the integral closure of R in L. Then there exist free R-modules M and M', of rank n, such that $M' \subset S \subset M$.*

PROOF Let t be a primitive element of L over K, i.e., $L = K(t)$. From Lemma 11.1, we may write $t = \frac{s}{r}$, with $s \in S$ and $r \in R^*$. Thus $L = K(s)$. Since L is an extension of degree n of K, , the degree of the minimal polynomial $m(s,K)$ is also n. Consequently, the elements $1, s, \dots, s^{n-1}$ are K-independant. These elements are also R-independant elements of the R-module S. The R-submodule of S generated by $1, s, \dots, s^{n-1}$ is

$$M' = R \oplus Rs \oplus \cdots \oplus Rs^{n-1},$$

which is a free module of rank n.

It is a little more difficult to show that S is contained in some free R-module. Let $d = \mathrm{disc}_{L/K}(1, s, \dots, s^{n-1})$. As the elements $1, s, \dots, s^{n-1}$ are K-linearly independant, Proposition 10.8 ensures that $d \neq 0$. Then $\frac{1}{d}, \frac{s}{d}, \dots, \frac{s^{n-1}}{d}$ are R-linearly independant elements of the R-module L. The R-module generated by these elements is

$$M = R(\frac{1}{d}) \oplus R(\frac{s}{d}) \oplus \cdots \oplus R(\frac{s^{n-1}}{d}).$$

M is a free R-module of rank n. We aim to show that $S \subset M$. As the set $\{1, s, \dots, s^{n-1}\}$ is a basis of L over K, any $y \in S$ can be written

$$y = \sum_{j=0}^{n-1} c_j s^j = \sum_{j=0}^{n-1} dc_j \left(\frac{s^j}{d}\right),$$

where the $c_j \in K$. We need to show that $dc_j \in R$. Since $dc_j \in K$ and R is an integrally closed domain, it is sufficient to prove that the dc_j are integral over R.

Since L is separable extension of K of degee n, Corollary 3.2 ensures that there are n distinct K-monomorphisms $\sigma_1, \dots, \sigma_n$ from L into an algebraic closure C of K. As $L = K(s)$, each σ_i is entirely determined by $\sigma_i(s)$, hence the elements $\sigma_1(s), \dots, \sigma_n(s)$ are distincts. In addition, for $i = 1, \dots, n$, $\sigma_i(s)$ is a K-conjugate of s and so the set $\{\sigma_1(s), \dots, \sigma_n(s)\}$ is equal to the set of K-conjugates $\{s_1, \dots, s_n\}$ of s. Without loss of generality, we may suppose that $\sigma_i(s) = s_i$, for all i. Applying σ_i to the equality $y = \sum_{j=0}^{n-1} c_j s^j$ we obtain, for all i,

$$\sigma_i(y) = \sum_{j=0}^{n-1} c_j \left(\sigma_i(s)\right)^j = \sum_{j=0}^{n-1} c_j s_i^j.$$

We may express this in matrix form:

$$\begin{pmatrix} \sigma_1(y) \\ \vdots \\ \sigma_n(y) \end{pmatrix} = \begin{pmatrix} 1 & s_1 & \dots & s_1^{n-1} \\ \vdots & \vdots & & \vdots \\ 1 & s_n & \dots & s_n^{n-1} \end{pmatrix} \begin{pmatrix} c_0 \\ \vdots \\ c_{n-1} \end{pmatrix}$$

The matrix $V = (s_i^j)$ is a Vandermonde matrix with all s_i distinct, so its determinant δ does not vanish. Using Cramer's rule, we obtain expressions for the c_j, namely $c_j = \frac{\gamma_j}{\delta}$, where γ_j is the determinant of the matrix V_j obtained from V by replacing the column $j+1$ by the column $(\sigma_1(y), \dots, \sigma_n(y))^t$.

Now, from Proposition 10.9, $d = \mathrm{disc}_{L/K}(1, s, \dots, s^{n-1})$ is the discriminant of the minimal polynomial $m(s, K)$; hence, using the formula for the determinant of a Vandermonde matrix, we obtain

$$d = \prod_{1 \leq i < j \leq n} (s_i - s_j)^2 = \delta^2 \Longrightarrow dc_j = \delta\gamma_j,$$

for $j = 0, \dots, n-1$. As δ and γ_j are determinants of matrices with coefficients in S, because y and s belong to S. Therefore the dc_j are integral over R, as required. □

11.2 Number rings

Let K be a number field and let us note O_K the collection of algebraic integers in K. Clearly $O_K = \mathcal{O} \cap K$ and so, being the intersection of two subrings of $\mathbf{C}$, O_K is a subring of $\mathbf{C}$. We say that O_K is the *number ring* associated to K or the *ring of integers* of K. We will see that this ring has many interesting properties. However, let us first consider a "simple" case, namely that of number rings associated to quadratic number fields. We know that, if K is a quadratic number field, then there is squarefree integer d such that $K = \mathbf{Q}(\sqrt{d}\,)$ (Theorem 3.5). It would be natural to think that associated number ring has the form $\mathbf{Z}[\sqrt{d}\,]$. The next theorem shows that $O_{\mathbf{Q}(\sqrt{d}\,)}$ always contains $\mathbf{Z}[\sqrt{d}\,]$, but inclusion can be strict.

Theorem 11.6 *Let d be a squarefree integer. Then*

$$O_{\mathbf{Q}(\sqrt{d}\,)} = \begin{cases} \mathbf{Z}[\sqrt{d}\,] & \textit{if } d \equiv 2, 3 \ (\textit{mod } 4) \\ \mathbf{Z}[\frac{-1+\sqrt{d}}{2}] & \textit{if } d \equiv 1 \ (\textit{mod } 4). \end{cases}$$

PROOF Case 1: $d = 2, 3$ (mod 4). We take $\alpha = r + s\sqrt{d} \in O_{\mathbf{Q}[\sqrt{d}\,]}$. If $s = 0$, then $\alpha \in \mathbf{Q}$, hence, from Theorem 11.2 $\alpha \in \mathbf{Z}$, and so $\alpha \in \mathbf{Z}[\sqrt{d}\,]$. Now suppose that $s \neq 0$. We note

$$f(X) = (r^2 - ds^2) - 2rX + X^2 \in \mathbf{Q}[X].$$

Then $\Delta(f) = 4ds^2$. As d is squarefree, $\Delta(f)$ is not a square in $\mathbf{Q}$, hence f is irreducible. Now, $f(\alpha) = 0$, therefore $f = m(\alpha, \mathbf{Q})$. From Corollary 11.1, $f \in \mathbf{Z}[X]$ and so $r^2 - ds^2, 2r \in \mathbf{Z}$. This implies that $4ds^2 \in \mathbf{Z}$. Using the fact that d is squarefree, we obtain $2s \in \mathbf{Z}$. Let us note $m = 2r$ and $n = 2s$. Then

$$r^2 - ds^2 = \frac{1}{4}(m^2 - dn^2) \in \mathbf{Z}$$

and so $4|(m^2 - dn^2)$. Then

$$d \equiv 2 \text{ (mod 4)} \Longrightarrow m^2 - dn^2 \equiv m^2 + 2n^2 \text{ (mod 4)}$$

and

$$d \equiv 3 \text{ (mod 4)} \Longrightarrow m^2 - dn^2 \equiv m^2 + n^2 \text{ (mod 4)}.$$

As $m^2 - dn^2 \equiv 0$ (mod 4), in both cases m and n are even, which implies that $r, s \in \mathbf{Z}$. Thus $\alpha \in \mathbf{Z}[\sqrt{d}]$.

Suppose now that $\alpha = r + s\sqrt{d}$, with $r, s \in \mathbf{Z}$. If $s = 0$, then $\alpha \in \mathbf{Z} \subset O_{\mathbf{Q}(\sqrt{d})}$. If $s \neq 0$, then $r^2 - ds^2, 2r \in \mathbf{Z}$ and so $f \in \mathbf{Z}[X]$; as $f(\alpha) = 0$, it follows that $\alpha \in O_{\mathbf{Q}(\sqrt{d})}$.

We have proved the result for the case $d \equiv 2, 3$ (mod 4).

Case 2: $d = 1$ (mod 4). We take $\alpha = r + s\sqrt{d} \in O_{\mathbf{Q}(\sqrt{d}\,)}$. If $s = 0$, then $\alpha \in \mathbf{Q}$, hence, from Theorem 11.2, $\alpha \in \mathbf{Z}$ and so $\alpha \in \mathbf{Z}[\frac{-1+\sqrt{d}}{2}]$. To handle the case where $s \neq 0$, we define $f \in \mathbf{Q}[X]$ as above and proceed as in Case 1 to find $4|(m^2 - dn^2)$, where $m = 2r$ and $n = 2s$.

$$d \equiv 1 \text{ (mod 4)} \Longrightarrow m^2 - dn^2 \equiv m^2 - n^2 \text{ (mod 4)}.$$

Thus we have $4|(m^2 - dn^2)$ and $4|(m^2 - n^2)$, which implies that m and n have the same parity. Now,

$$\alpha = \frac{m + n\sqrt{d}}{2} = \frac{m+n}{2} + n\left(\frac{-1+\sqrt{d}}{2}\right) \in \mathbf{Z}[\frac{-1+\sqrt{d}}{2}].$$

Now suppose that $\alpha = r + s\frac{-1+\sqrt{d}}{2}$, with $r, s \in \mathbf{Z}$. If $s = 0$, then $\alpha \in \mathbf{Z} \subset O_{\mathbf{Q}(\sqrt{d})}$. For the case where $s \neq 0$ we have $2r, r^2 - ds^2 \in Z$, so $f \in \mathbf{Z}[X]$; as $f(\alpha) = 0$, it follows that $\alpha \in O_{\mathbf{Q}(\sqrt{d}\,)}$.

This proves the result for $d \equiv 1$ (mod 4). □

Examples

- $O_{\mathbf{Q}(i)} = \mathbf{Z}[i]$, because $-1 \equiv 3 \pmod 4$;
- $O_{\mathbf{Q}(\sqrt{3})} = \mathbf{Z}[\sqrt{3}]$, because $3 \equiv 3 \pmod 4$;
- $O_{\mathbf{Q}(\sqrt{5})} = \mathbf{Z}[\frac{-1+\sqrt{5}}{2}]$, because $5 \equiv 1 \pmod 4$;
- $O_{\mathbf{Q}(\sqrt{6})} = \mathbf{Z}[\sqrt{6}]$, because $6 \equiv 2 \pmod 4$.

We now consider certain basis properties of number rings. In particular, we will show that the additive group of such a ring is a free abelian group. We begin with a characterization of invertible elements.

Proposition 11.3 *If K is a number field and $\alpha \in O_K$, then $\alpha \in O_K^\times$ if and only if $N_{K/\mathbf{Q}}(\alpha) = \pm 1$.*

PROOF If $\alpha \in O_K^\times$, then $\alpha^{-1} \in O_K^\times$ and

$$1 = N_{K/\mathbf{Q}}(1) = N_{K/\mathbf{Q}}(\alpha)N_{K/\mathbf{Q}}(\alpha^{-1}).$$

As α and α^{-1} are algebraic, $N_{K/\mathbf{Q}}(\alpha)$ and $N_{K/\mathbf{Q}}(\alpha^{-1})$ are integers, hence $N_{K/\mathbf{Q}}(\alpha) = \pm 1$.

Now suppose that $N_{K/\mathbf{Q}}(\alpha) = \pm 1$. Since $\alpha \in O_K$, Proposition 10.1 and Corollary 11.1 ensure that $\mathrm{char}_{K/\mathbf{Q}}(\alpha)$ belongs to $\mathbf{Z}[X]$. Thus we have

$$\mathrm{char}_{K/\mathbf{Q}}(\alpha) = \pm 1 + a_1 X + \cdots + a_{n-1}X^{n-1} + X^n,$$

with $a_i \in \mathbf{Z}$, for $1 \leq i \leq n-1$. From the Cayley-Hamiltonian Theorem, we know that α is a root of $\mathrm{char}_{K/\mathbf{Q}}(\alpha)$.

Now α^{-1} is a root of the reciprocal polynomial

$$f(X) = 1 + a_{n_1}X + \cdots + a_1 X^{n-1} \pm X^n.$$

Since $f \in \mathbf{Z}[X]$, α^{-1} is algebraic and it follows that $\alpha \in O_K^\times$. □

Exercise 11.3 *Show that, if $K = \mathbf{Q}(\sqrt{-2})$, then $O_K^\times$ is finite. Considering the positive powers of $1+\sqrt{2}$, show that the diophantine equation $a^2 - 2b^2 = 1$ has an infinite number of solutions and deduce that, if $K = \mathbf{Q}(\sqrt{2})$, then $O_K^\times$ is infinite.*

As O_K is an integral domain, it has a field of fractions (in $\mathbf{C}$). It is natural to try to determine this field. This we will now do.

Lemma 11.2 *If $\alpha \in \mathbf{C}$ is algebraic over $\mathbf{Q}$, then there is an integer $k \in \mathbf{N}^*$ such that $k\alpha$ is an algebraic integer.*

PROOF If $\alpha = 0$, then there is nothing to prove, so let us suppose that this is not the case. Let $m(X) = \sum_{i=0}^{d-1} a_i X^i + X^d$ be the minimal polynomial of α over $\mathbf{Q}$. If k is the lcm of the denominators of the coefficients a_i, then $ka_i = b_i \in \mathbf{Z}$, for $0 \leq i \leq d-1$. We have

$$k^{d-1}b_0 + k^{d-2}b_1(k\alpha) + \cdots + kb_{d-2}(k\alpha)^{d-2} + b_{d-1}(k\alpha)^{d-1} + (k\alpha)^d = k^d m(\alpha) = 0.$$

As the coefficients $k^{d-1}b_0, \ldots, kb_{d-2}, b_{d-1}$ are integers, $k\alpha$ is an algebraic integer. □

Theorem 11.7 *The field of fractions of O_K is the number field K.*

PROOF Let us write L for the field of fractions of O_K. The clearly $O_K \subset K$. If $L \neq K$, then there exists $\alpha \in K \setminus L$. As K is a finite extension of $\mathbf{Q}$, K is algebraic over $\mathbf{Q}$. In particular, α is algebraic over $\mathbf{Q}$. From Lemma 11.2, there exists $k \in \mathbf{N}^*$ such that $k\alpha$ is an algebraic integer, hence $k\alpha \in O_K \subset L$. As $k \in O_K$, $\alpha = \frac{k\alpha}{k} \in L$, a contradiction. □

We now consider bases of the vector space K over $\mathbf{Q}$. It turns out that there is a basis composed entirely of elements in O_K.

Proposition 11.4 *If K is a number field, and $[K : \mathbf{Q}] = n$, then K has a basis $\alpha_1, \dots, \alpha_n$ composed of elements in O_K.*

PROOF From Lemma 11.2, we know that, if α is nonzero and algebraic over $\mathbf{Q}$, then there in an integer $k \in \mathbf{N}^*$ such that $k\alpha$ is an algebraic integer. Let $(\beta_1, \dots, \beta_n)$ be a basis of K over $\mathbf{Q}$. As K is a finite extension of $\mathbf{Q}$, K is algebraic over $\mathbf{Q}$ and so each β_i is algebraic over $\mathbf{Q}$. For each β_i, we may find $k_i \in \mathbf{N}^*$ such that $k_i\beta_i$ is an algebraic integer. If $\alpha_i = k_i\beta_i$, then clearly $(\alpha_1, \dots, \alpha_n)$ is a basis of K over $\mathbf{Q}$. □

We now turn to the result referred to above concerning the nature of the additive group of O_K. To understand the proof it is necessary to have a knowledge of free abelian groups. We have included an appendix on the subject.

Theorem 11.8 *The additive group of O_K is a free abelian group of rank n.*

PROOF Let $(\alpha_1, \dots, \alpha_n)$ be a basis of K over $\mathbf{Q}$ composed of elements of O_K and $A = \mathbf{Z}\alpha_1 \oplus \cdots \oplus \mathbf{Z}\alpha_n$. (The sum is direct because the α_i are independant over $\mathbf{Q}$.) If we can show that there exists $d \in \mathbf{Z}^*$ such that $dO_K \subset A$, then the theorem is proved. Indeed, in this case, $O_K \subset \frac{1}{d}A$, where $\frac{1}{d}A$ is a free abelian group. Thus, by Theorem E.3, O_K is a free abelian group of rank r, with $r \leq n$. Moreover, A is subgroup of O_K and so, using Theorem E.3 again, the rank of r of O_K is is larger than n. Finally, O_K is a free abelian group of rank n.

Let us now show that this d exists. For any $\alpha \in O_K$, there exist $x_1, \dots, x_n \in \mathbf{Q}$ such that $\alpha = \sum_{i=1}^n x_i\alpha_i$. We set $d = \mathrm{disc}_{K/\mathbf{Q}}(\alpha_1, \dots, \alpha_n)$; then d is nonzero by Proposition 10.8. Using Proposition 10.7 and Exercise 11.1 we see that d is an integer, since the algebraic integers form a ring.

We now show that $dx_i \in \mathbf{Z}$, for $1 \leq i \leq n$, which implies that $d\alpha \in A$. We note $\sigma_1, \dots, \sigma_n$ the $\mathbf{Q}$-monomorphisms of K into $\mathbf{C}$. We have, for $1 \leq i \leq n$,

$$\sigma_i(\alpha) = x_1\sigma_i(\alpha_1) + \cdots + x_n\sigma_i(\alpha_n).$$

This is a system of n equations in n unknowns (the x_j). Applying Cramer's rule we obtain

$$x_j = \frac{\nu_j}{\delta},$$

where δ is the determinant $|\sigma_i(\alpha_j)|$ and ν_j is the determinant of the matrix obtained from the matrix $(\sigma_i(\alpha_j))$ by replacing the jth column by the column composed of the elements $\sigma_i(\alpha)$. Now, $\delta^2 = d$, so δ is an algebraic integer. In the same way, we may show that ν_j is an algebraic integer, since

$$\nu_j^2 = \mathrm{disc}_{K/\mathbf{Q}}(\alpha_1, \dots, \alpha_{j-1}, \alpha, \alpha_{j+1}, \dots, \alpha_n),$$

and $\alpha \in O_K$. To finish, we notice that

$$dx_j = \delta^2 \frac{\nu_j}{\delta} = \delta \nu_j$$

which implies that dx_j is an algebraic integer, since both δ and ν_j are algebraic integers. Moreover, $dx_j \in \mathbf{Q}$. As an algebraic integer in $\mathbf{Q}$ is an integer, dx_j is an integer. This concludes the proof. □

Discriminant of a number ring

Let K be a number field with number ring O_K. As O_K is a free abelian group, O_K has a basis $(\alpha_1, \ldots, \alpha_n)$, where n is the dimension of the vector space K over $\mathbf{Q}$:

$$O_K = \mathbf{Z}\alpha_1 \oplus \cdots \oplus \mathbf{Z}\alpha_n.$$

We call such a basis an *integral basis.* There may be many bases; however, they are related through their discriminants.

Proposition 11.5 *If $(\alpha_1, \ldots, \alpha_n)$ and $(\beta_1, \ldots, \beta_n)$ are integral bases of O_K, then*

$$disc_{K/\mathbf{Q}}(\alpha_1, \ldots, \alpha_n) = disc_{K/\mathbf{Q}}(\beta_1, \ldots, \beta_n).$$

PROOF First we notice that there is a matrix $M = (m_{ij}) \in \mathcal{M}_n(\mathbf{Z})$ such that

$$\begin{pmatrix} \alpha_1 \\ \vdots \\ \alpha_n \end{pmatrix} = M \begin{pmatrix} \beta_1 \\ \vdots \\ \beta_n \end{pmatrix}$$

Let $\sigma_1, \ldots, \sigma_n$ be the $\mathbf{Q}$-monomorphisms of K into $\mathbf{C}$. Then

$$\alpha_i = \sum_{k=1}^{n} m_{ik}\beta_k \Longrightarrow \sigma_j(\alpha_i) = \sum_{k=1}^{n} m_{ik}\sigma_j(\beta_k),$$

for $1 \leq i, j \leq n$. In terms of matrices,

$$(\sigma_j(\alpha_i)) = M\left(\sigma_j(\beta_k)\right),$$

which implies that

$$\mathrm{disc}_{K/\mathbf{Q}}(\alpha_1, \ldots, \alpha_n) = |M|^2 \mathrm{disc}_{K/\mathbf{Q}}(\beta_1, \ldots, \beta_n).$$

As the α_i and β_j are algebraic integers, from Proposition 10.7, the discriminants in the above equations are integers. Given that $M \in \mathcal{M}_n(\mathbf{Z})$, the determinant $|M|$ is an integer and it follows that $\mathrm{disc}_{K/\mathbf{Q}}(\beta_1, \ldots, \beta_n)$ divides $\mathrm{disc}_{K/\mathbf{Q}}(\alpha_1, \ldots, \alpha_n)$. In the same way, $\mathrm{disc}_{K/\mathbf{Q}}(\alpha_1, \ldots, \alpha_n)$ divides $\mathrm{disc}_{K/\mathbf{Q}}(\beta_1, \ldots, \beta_n)$. As the discriminants clearly have the same sign, they are equal. □

We call the common value of the discriminant in the foregoing theorem the *discriminant of the number ring* O_K and we write $\mathrm{disc}(O_K)$ for this. We emphasize that $\mathrm{disc}(O_K) \in \mathbf{Z}$.

Example Let $K = \mathbf{Q}(\sqrt{d})$, where d is a squarefree integer. The Galois group $Gal(K/\mathbf{Q}) = (\sigma_1, \sigma_2)$, where σ_1 is the identity and σ_2 permutes $\sqrt{d}$ and $-\sqrt{d}$. If $d \equiv 2, 3 \pmod 4$, then $O_K = \mathbf{Z}[\sqrt{d}]$ and $(1, \sqrt{d})$ is an integral basis of O_K. It follows that

$$\mathrm{disc}(O_K) = \mathrm{disc}_{K/\mathbf{Q}}(1, \sqrt{d}) = 4d.$$

Exercise 11.4 *Show that, if* $d \equiv 1 \pmod 4$*, then* $disc(O_K) = d$.

We may extend the notion of the discriminant of a number ring. Let K be a number field with ring of integers O_K. An *order* in K is a subring R of O_K such that the index of R in O_K (as additive groups) is finite. The order is said to be maximal if $R = O_K$.

If R is a subring of O_K, from Theorem E.3 we know that R is a free group with rank at most that of O_K.

Proposition 11.6 *A subring* R *of* O_K *is an order if and only if* R *has the same rank as that of* O_K.

PROOF Let n be the rank of O_K and r that of R. From Theorem E.4, O_K has a basis $\{e_1, \ldots, e_n\}$ for which there exist integers $d_1, \ldots, d_r \in N^*$, such that $\{d_1e_1, \ldots, d_re_r\}$ is a basis of R. If $r = n$, then the cosets of R in O_K can be written

$$s_{i_1}e_1 + \cdots + s_{i_n}e_n + R, \quad \text{with} \quad 0 \leq s_{i_1} \leq d_1 - 1, \ldots, 0 \leq s_{i_n} \leq d_n - 1.$$

Thus there are $d_1 \cdots d_n$ cosets, i.e., $[O_K : R] < \infty$ and R is an order. If $r < n$, then the cosets of R in O_K may be written

$$s_{i_1}e_1 + \cdots + s_{i_r}e_r + x_{r+1}e_{r+1} + \cdots + x_ne_n + R,$$

with $0 \leq s_{i_1} \leq d_1 - 1, \ldots, 0 \leq s_{i_r} \leq d_r - 1$ and $x_{r+1}, \ldots, x_n \in \mathbf{Z}$. In this case there is an infinite number of cosets, so $[O_K : R] = \infty$ and R is not an order. □

If $R \subset O_K$ is an order, then we may define the discriminant of R in the same way as we did for O_K. If $(\alpha_1, \ldots, \alpha_n)$ and $(\beta_1, \ldots, \beta_n)$ are integral bases of R, then the argument of Proposition 11.5 shows that

$$\mathrm{disc}_{K/\mathbf{Q}}(\alpha_1, \ldots, \alpha_n) = \mathrm{disc}_{K/\mathbf{Q}}(\beta_1, \ldots, \beta_n).$$

and that the common value is an integer. We call this the discriminant of R and note it $\mathrm{disc}(R)$.

Example Suppose that $K = \mathbf{Q}(\alpha)$, where $\alpha \in O_K$. Then $\mathrm{rk}\, O_K = [\mathbf{Q}(\alpha); \mathbf{Q}]$. However, $\deg m(\alpha, \mathbf{Q}) = n = [\mathbf{Q}(\alpha) : \mathbf{Q}]$, so the set $\{1, \alpha, \ldots, \alpha^{n-1}\}$ is a basis of $\mathbf{Z}[\alpha]$. Thus $\mathbf{Z}[\alpha]$ and O_K have the same rank: $\mathbf{Z}[\alpha]$ is an order in K.

We will return to orders further on.

We say that an integral domain D is a *normal domain* if the integral closure of D in its field of fractions is D itself. It is worth noticing (although we will not prove it here) that the polynomial ring $D[X]$ is a normal domain if D is normal. We aim to show that a number ring is a normal domain. We will first prove a preliminary result, which is interesting in its own right.

Lemma 11.3 *A subgroup of a finitely generated abelian group is finitely generated.*

PROOF We will use an induction on the number of generators. Let G be a finitely generated abelian group: $G = \langle a_1, \ldots, a_n \rangle$. If $n = 1$, then G is cyclic. As a subgroup of a cyclic group is cyclic, the result is true in the case $n = 1$.

Nos suppose that we have proved the result up to n and $G = \langle a_1, \ldots, a_n, a_{n+1} \rangle$. Let H be a subgroup of G and $\pi : G \longrightarrow G/\langle a_{n+1} \rangle$ the canonical quotient mapping. As G is abelian, the quotient $\bar{G} = G/\langle a_{n+1} \rangle$ has a natural group structure and $\bar{G} = \langle \pi(a_1), \ldots, \pi(a_n) \rangle$. From the induction hypothesis, the subgroup $\bar{H} = \pi(H)$ of $\bar{G}$ is finitely generated: $\bar{H} = \langle \bar{h}_1, \dots, \bar{h}_m \rangle$, with $\bar{h}_i = \pi(h_i)$ for some $h_i \in H$.

We now notice that $H \cap \langle a_{n+1} \rangle$ is a subgroup of $\langle a_{n+1} \rangle$, hence cyclic: $H \cap \langle a_{n+1} \rangle = \langle h_{m+1} \rangle$, with $h_{m+1} \in H$. We claim that $H = \langle h_1, \dots, h_m, h_{m+1} \rangle$. If $h \in H$, then there exists $g \in \langle a_1, \dots, h_m \rangle$ such that $\pi(g) = \pi(h)$. Therefore $h = g + k$, with $k \in \operatorname{Ker} \pi = \langle a_{n+1} \rangle$. In addition, $k = h - g \in H$, so $k = sh_{m+1}$, for some $s \in \mathbf{Z}$. To conclude,

$$h = g + sh_{m+1} \in \langle h_1, \dots, h_{m+1} \rangle.$$

We have shown that $H = \langle h_1, \dots, h_{m+1} \rangle$. □

Remark The abelian hypothesis in the previous lemma is important. Here is a counter-example. Theorems 11.2 and 11.3 ensure that the additive group of the ring $\mathbf{Z}[\frac{1}{2}]$ is not finitely generated. Consequently the group of matrices

$$G_0 = \{ \begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix} \in \mathcal{M}_2(\mathbf{Q}), x \in \mathbf{Z}[\frac{1}{2}] \}$$

is not finitely generated. However, the elements of $\mathbf{Z}[\frac{1}{2}]$ are of the form $\frac{p}{2^q}$, with $p \in \mathbf{Z}$ and $q \in \mathbf{N}$, and

$$\begin{pmatrix} 1 & \frac{p}{2^q} \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix}^{-q} \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}^{m_1} \begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix}^{q} \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}^{m_2},$$

where m_2 and m_1 are respectively the quotient and remainder after division of p by 2^q. Hence G_0 is a subgroup of G, the subgroup of $\mathcal{M}_2(\mathbf{Q})$ generated by the matrices

$$S = \begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix} \qquad \text{and} \qquad T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}.$$

Thus we have a subgroup of a finitely generated group which is not finitely generated.

Exercise 11.5 *Find an explicit description of the matrices in G.*

Proposition 11.7 *A number ring O_K is a normal domain.*

PROOF We have seen that O_K has a finite basis. Let $\alpha \in K$ be integral over O_K: there exists a poynomial $f(X) = \sum_{i=0}^{n-1} a_i X^i + X^n$, with $a_i \in O_K$, such that $f(\alpha) = 0$. This implies that

$$\alpha^n = -a_{n-1}\alpha^{n-1} - \cdots - a_1\alpha - a_0.$$

It follows that the additive group of the ring $O_K[\alpha]$ is finitely generated. As $\mathbf{Z}[\alpha] \subset O_K[\alpha]$, the additive subgroup of the ring $\mathbf{Z}[\alpha]$ is also finitely generated (Lemma 11.3). From Theorem 11.3, α is an algebraic integer and so $\alpha \in O_K$. □

Stickelberger's criterion

We may say a little more about the discriminant of a number ring. Let K be a number field of degree n over $\mathbf{Q}$ and $\mathcal{B} = \{\beta_1, \dots, \beta_n\}$ an integral basis of the number ring O_K. There exist n $\mathbf{Q}$-embeddings $\sigma_1, \dots, \sigma_n$ of K in $\mathbf{C}$. By definition,

$$\operatorname{disc}(O_K) = \det(\sigma_i(\beta_j))^2.$$

The determinant is the sum of expressions of the form

$$\operatorname{sgn}(\pi)\sigma_{\pi(1)}(\beta_1)\cdots\sigma_{\pi(n)}(\beta_n),$$

where π is a permutation of the set $\{1,\ldots,n\}$, i.e., $\pi \in S_n$, and $\operatorname{sgn}(\pi)$ is the sign of π. To simplify the notation, let us set $X = A_n$ and $Y = S_n \setminus A_n$. Then

$$\det(\sigma_i(\beta_j)) = \sum_{\pi\in S_n}\prod_{i=1}^{n}\operatorname{sgn}(\pi)\sigma_{\pi(i)}(\beta_i) = \sum_{\pi\in X}\prod_{i=1}^{n}\sigma_{\pi(i)}(\beta_i) - \sum_{\pi\in Y}\prod_{i=1}^{n}\sigma_{\pi(i)}(\beta_i) = P - N.$$

Thus

$$\operatorname{disc}(O_K) = (P-N)^2 = (P+N)^2 - 4PN.$$

Now let L be a normal closure of K over $\mathbf{Q}$. By Exercise 5.1, L is a finite Galois extension of $\mathbf{Q}$. We aim to show that $\phi(P+N) = P+N$ and $\phi(PN) = PN$, for all $\phi \in Gal(L/\mathbf{Q})$, the Galois group of L over $\mathbf{Q}$. First, we extend every embedding σ_i to an embedding $\bar{\sigma}_i$ of L into $\mathbf{C}$. (This is possible by Theorem 2.7.) From the normality of the extension $L/\mathbf{Q}$ we deduce that $\bar{\sigma}_i(L) = L$. (The image of $\bar{\sigma}_i$ is included in the set $A(C/\mathbf{Q})$, which is an algebraic closure of $\mathbf{Q}$, by the remark after Theorem 2.6; therefore, from Proposition 5.2), $\bar{\sigma}_i(L) = L$.) It follows that $\sigma_i(K) \subset L$. Hence, for every σ_i, the mapping $\phi\circ\sigma_i$ is defined and is a $\mathbf{Q}$-embedding of K into $\mathbf{C}$.

We now notice that the mapping $\sigma_i \longmapsto \phi\circ\sigma_i$ is a bijection on the set $S = \{\sigma_1,\ldots,\sigma_n\}$, so we can find a permutation $\tau \in S_n$ such that $\phi\circ\sigma_i = \sigma_{\tau(i)}$, for every $i \in \{1,\ldots,n\}$. We distinguish two cases:

Case 1: τ even

Here we have $\tau X = X$ and

$$\begin{aligned}
\phi\left(\sum_{\pi\in X}\prod_{i=1}^{n}\sigma_{\pi(i)}(\beta_i)\right) &= \sum_{\pi\in X}\prod_{i=1}^{n}\phi\circ\sigma_{\pi(i)}(\beta_i)\\
&= \sum_{\pi\in X}\prod_{i=1}^{n}\sigma_{\tau\pi(i)}(\beta_i)\\
&= \sum_{\pi\in \tau X}\prod_{i=1}^{n}\sigma_{\pi(i)}(\beta_i)\\
&= \sum_{\pi\in X}\prod_{i=1}^{n}\sigma_{\pi(i)}(\beta_i).
\end{aligned}$$

Hence $\phi(P) = P$. In a similar way, using the fact that $\tau Y = Y$, we may show that $\phi(N) = N$.

Case 2: τ odd

Now we have $\tau X = Y$ and $\tau Y = X$ and so $\phi(P) = N$ and $\phi(N) = P$.

From what we have seen, in both cases we have $\phi(P+N) = P+N$ and $\phi(PN) = PN$. This applies for any $\phi \in Gal(L/\mathbf{Q})$, so $P+N$ and PN belong to the fixed field of $Gal(K/\mathbf{Q})$, i.e., $\mathbf{Q}$. Now the β_i are algebraic integers; since the elements $\sigma_{\pi(i)}(\beta_i)$ are roots of the minimal polynomial $m(\beta_i,\mathbf{Q})$, these elements are also algebraic integers. This means that P and N are algebraic integers in $\mathbf{Q}$, i.e., integers. From the formula

$$\operatorname{disc}(O_K) = (P+N)^2 - 4PN,$$

we may deduce the following: If P and N have the same parity, then $P + N \equiv 0 \pmod 2 \Longrightarrow (P + N)^2 \equiv 0 \pmod 4$; if P and N have different parities, then $P + N \equiv 1 \pmod 2 \Longrightarrow (P + N)^2 \equiv 1 \pmod 4$. Thus we have:

Theorem 11.9 *(Stickelberger's criterion) If K is a number field, with number ring O_K, then*

$$disc(O_K) \equiv 0\ (mod\, 4) \quad or \quad disc(O_K) \equiv 1\ (mod\, 4).$$

Remark In a certain sense Stickelberger's theorem generalizes Exercise 11.4 and the remark preceding it.

11.3 Roots of unity in number fields

In any commutative ring with identity, the roots of unity form a multiplicative group. In a number field, as we will soon see, this group is cyclic. If K is a number field and x is a root of unity, then $-1 + x^n = 0$, for some $n \in \mathbf{N}^*$, so x lies in the number ring O_K.

Proposition 11.8 *Let K be a number field and $c \in \mathbf{R}_+^*$. Then there are only a finite number of elements $x \in O_K$ such that $|x^{(i)}| \leq c$, for all conjugates $x^{(i)}$ of x.*

PROOF Let $[K : \mathbf{Q}] = n$ and $\Sigma_1, \ldots, \Sigma_n$ be the elementary symmetric polynomials in n variables. We set

$$c' = \max\{nc, \binom{n}{2}c^2, \ldots, \binom{n}{k}c^k, \ldots, c^n\}.$$

Let S be the set of monic polynomials of degree at most n, whose coefficients are integers a such that $|a| \leq c'$. Then S is finite. Now let T be the set of elements of K which are roots of some polynomial belonging to S; T is also a finite set. If $|x^{(i)}| \leq c$, for all conjugates of x in K, then $|\Sigma_k(x^{(1)}, \ldots, x^{(n)})| \leq c'$, for $k = 1, \ldots, n$. Since x is an algebraic integer, $\Sigma_k(x^{(1)}, \ldots, x^{(n)}) \in \mathbf{Z}$ and so the polynomial $f(X) = \prod_{i=1}^{n}(-x^{(i)} + X)$ belongs to S. As x is a root of f, x belongs to T. □

We may now prove a fundamental result.

Theorem 11.10 *The group W of roots of unity of a number field K is a finite multiplicative cyclic group.*

PROOF It is sufficient to notice that W is a finite subgroup of the multiplicative group of K and apply Theorem 3.3. □

The next result gives us a criterion for determining roots of unity.

Proposition 11.9 *If $f \in \mathbf{Z}[X]$ is monic and is such that all its roots in $\mathbf{C}$ have absolute value 1. Then these roots are all roots of unity.*

PROOF Let $z_1, \ldots, z_k$ be the roots of f in $\mathbf{C}$ repeated according to their multiplicities. For every $l \in \mathbf{N}^*$ we set

$$f_l(X) = (-z_1^l + X) \cdots (-z_k^l + X).$$

From Exercise B.1, $f_l \in \mathbf{Z}[X]$ for all l. If

$$f_l(X) = a_0 + a_1 X + \cdots a_{k-1}X^{k-1} + X^k,$$

then, taking into account the fact that $|z_i| = 1$ for all i, we find that

$$|a_j| \leq \binom{k}{j}$$

for $j = 0, 1, \ldots, k-1$. There are only a finite number of monic polynomials $g \in \mathbf{Z}[X]$ with $\deg g = k$ and jth coefficient bounded by $\binom{k}{j}$ for $j = 0, 1, \ldots, k-1$, hence there exist $l < m$ such that $f_l = f_m$. It follows that the roots of these two polynomials are the same. If $z_1^l, \ldots, z_r^l$ are the distinct roots of f_l and $z_1^m, \ldots, z_r^m$ the distinct roots of f_m, then there exists a permutation $\sigma \in \Sigma_r$ such that $z_i^l = z_{\sigma(i)}^m$, for $i = 1, \ldots, r$. We claim that $z_i^{l^k} = z_{\sigma^k(i)}^m$, for $k \in \mathbf{N}^*$. For this we give a proof by induction. For $k = 1$, there is nothing to prove. Suppose now that the result is true for k and consider the case $k+1$. We have

$$z_{\sigma^{k+1}(i)}^m = z_{\sigma(\sigma^k(i))}^m = (z_{\sigma^k(i)}^l)^m = (z_{\sigma^k(i)}^m)^l = (z_i^{l^k})^l = z_i^{l^{k+1}},$$

so the result is true for $k+1$ and, by induction, for all $k \in \mathbf{N}^*$. In particular, it is true for $k = r!$, the cardinal of the symmetric group Σ_r and hence $z_i^{l^{r!}} = z_i^m$. From this we deduce that z_i is root of unity. □

Corollary 11.4 *x is a root of unity in a number field K if and only if $x \in O_K$ and $|x^{(i)}| = 1$, for every conjugate of x.*

PROOF Let x be a root of unity. We have already seen that a root of unity must lie in O_K. There exists a positive integer m such that $x^m = 1$. As the conjugates $x^{(i)}$ of x are also roots of the polynomial $f(X) = -1 + X^m$, we must have $|x^{(i)}|^m = 1$, which implies that $|x^{(i)}| = 1$.

Now suppose that $x \in O_K$ and $|x^{(i)}| = 1$, for all conjugates $x^{(i)}$ of x. The conjugates are the roots of the minimal polynomial $m(x, \mathbf{Q})$, so by Proposition 11.9 they are roots of unity; in particular, x is a root of unity. □

Exercise 11.6 *Let K be a number field, $x \in K$ and $m \in \mathbf{N}^*$. Show that the conjugates of x^m are mth powers of the conjugates of x.*

If p is an odd prime, $\zeta = e^{\frac{2\pi i}{p}}$ and $K = \mathbf{Q}(\zeta)$, then we can be more precise with respect to the roots of unity of K.

Theorem 11.11 *If p is an odd prime and $\zeta = e^{\frac{2\pi i}{p}}$, then the roots of unity in $K = \mathbf{Q}(\zeta)$ are of the form $\pm\zeta^j$, with $1 \leq j \leq p$.*

PROOF From Theorem 11.10 we know that the roots of unity form a finite cyclic group C. If $|C| = m$, then there is a generator $z = e^{\frac{2\pi i t}{m}}$ of C. (It is sufficient to take t coprime to m.) If $x \in C$, then $-x \in C$, because $x^k = 1$ implies that $(-x)^{2k} = 1$, hence $-\zeta \in C$ and so there exists $s \in \mathbf{N}^*$ such that $z^s = -\zeta$, i.e., $e^{\frac{2\pi i s}{m}} = e^{\frac{2\pi i}{p} + \pi i}$. From this we deduce that there exists $k \in \mathbf{Z}$ such that

$$\frac{2\pi i s}{m} = \frac{2\pi i}{p} + \pi i + 2k\pi i \Longrightarrow 2sp = m(2 + p(2k+1)) \Longrightarrow 2p|m,$$

because neither 2 nor p divide $2 + p(2k+1)$.

As z is a generator of C, ζ is a power of z and so $\mathbf{Q}(\zeta) \subset \mathbf{Q}(z)$. However, $z \in \mathbf{Q}(\zeta)$ and so we also have $\mathbf{Q}(z) \subset \mathbf{Q}(\zeta)$ and it follows that $\mathbf{Q}(\zeta) = \mathbf{Q}(z)$. This being the case, we have

$$\phi(m) = [\mathbf{Q}(z) : \mathbf{Q}] = [\mathbf{Q}(\zeta) : \mathbf{Q}] = \phi(p) = p - 1,$$

where ϕ is Euler's totient function. We may write $m = 2^\alpha p^\beta m'$, with $\alpha \geq 1$, $\beta \geq 1$ and $2 \not| m'$, $p \not| m'$, and

$$p - 1 = \phi(m) = 2^{\alpha-1}p^{\beta-1}(p-1)\phi(m') \Longrightarrow 1 = 2^{\alpha-1}p^{\beta-1}\phi(m').$$

Therefore $\alpha = \beta = \phi(m') = 1$. As $m' \neq 2$, we have $m' = 1$ and so $m = 2p$. Thus the cardinal of C is $2p$. Since the elements $\pm\zeta^i$, with $1 \leq i \leq p$, belong to C and are distinct, these are the roots of unity in K. □

Exercise 11.7 *Show that a number field of odd degree has just two roots of unity.*

11.4 Composita of number fields

We recall that, if K and L are subfields of a field E, then the compositum of K and L in E, which we write KL, is the smallest subfield of E containing both K and L. In this section we consider the case where K and L are number fields (considered as subfields of $\mathbf{C}$.) We will be particularly interested in the number ring O_{KL} of KL.

Let K and L be number fields and O_K, O_L the associated number rings. From Proposition 6.4 we know that

$$[KL : \mathbf{Q}] \leq [K : \mathbf{Q}][L : \mathbf{Q}],$$

with equality when $[K : \mathbf{Q}]$ and $[L : \mathbf{Q}]$ are coprime, or said otherwise, when K and L are linearly disjoint. We set $R = O_K$, $S = O_L$ and

$$RS = \big\{ \sum_{i \in I} r_i s_i : r_i \in R, s_i \in S, |I| < \infty \big\}$$

RS is clearly a subring of O_{KL}. The following result provides a sufficient condition for equality.

Theorem 11.12 *Let K and L be linearly disjoint number fields and $d = \gcd(disc(R), disc(S))$. Then $O_{KL} \subset \frac{1}{d}RS$. Thus, if $d = 1$, then $O_{KL} = RS$.*

PROOF Let $m = [K : \mathbf{Q}]$, $n = [L : \mathbf{Q}]$ and $\{\alpha_1, \ldots, \alpha_m\}$, $\{\beta_1, \ldots, \beta_n\}$ integral bases respectively of R and S. These bases are bases over $\mathbf{Q}$ of respectively K and L. As K and L are linearly disjoint over $\mathbf{Q}$, the set

$$A = \{\alpha_i\beta_j : 1 \leq i \leq m, 1 \leq j \leq n\}$$

is a basis of KL over $\mathbf{Q}$. (See the discussion on linear disjointness after Proposition 6.4.) Hence, if $x \in O_{KL}$, then there exist rational numbers q_{ij}, for $1 \leq i \leq m$ and $1 \leq j \leq n$, such that

$$x = \sum_{i,j} q_{ij}\alpha_i\beta_j.$$

We aim to show that $dq_{ij} \in \mathbf{Z}$,for all i and j. If this is the case, then we may write

$$x = \frac{1}{d}\sum_{i,j}(dq_{ij})\alpha_i\beta_j \in \frac{1}{d}RS$$

and it follows that $O_{KL} \subset \frac{1}{d}RS$. To establish that $dq_{ij} \in \mathbf{Z}$ it is sufficient to show that $\mathrm{disc}(R)q_{ij} \in \mathbf{Z}$. If we can do this, then with an analogous argument we may show that $\mathrm{disc}(S)q_{ij} \in \mathbf{Z}$. As there exist $u, v \in \mathbf{Z}$ such that $d = u\mathrm{disc}(R) + v\mathrm{disc}(S)$, $dq_{ij} \in Z$.

From Corollary 3.2 we know that there are exactly $[K:\mathbf{Q}]$ $\mathbf{Q}$-monomorphisms of K into $\mathbf{C}$. Let σ be such a monomorphism. Theorem 3.2 ensures that there are exactly $[KL:K]$ monomorphic extensions $\tilde{\sigma}$ of σ into $\mathbf{C}$. Restricting the $\tilde{\sigma}$ to L, we obtain $[KL:K]$ distinct monomorphisms σ' from L into $\mathbf{C}$. (If two such restrictions σ'_1 and σ'_2 are equal, then the corresponding mappings $\tilde{\sigma}_1$ and $\tilde{\sigma}_2$ are equal on K and L and consequently on KL, contradicting the fact that $\tilde{\sigma}_1$ and $\tilde{\sigma}_2$ are distinct.) As K and L are linearly disjoint $[KL:K]=[L:\mathbf{Q}]$, therefore the considered restrictions are the $\mathbf{Q}$-monomorphisms from L into $\mathbf{C}$. In particular, one such restriction is the identity on L. Consequently, for the corresponding $\tilde{\sigma}$, we have

$$\tilde{\sigma}(x)=\sum_{i=1}^{m}\sum_{j=1}^{n}\tilde{\sigma}(q_{ij})\tilde{\sigma}(\alpha_i)\tilde{\sigma}(\beta_j)=\sum_{i=1}^{m}x_i\sigma(\alpha_i),$$

where $x_i=\sum_{j=1}^{n}q_{ij}\beta_j$. We may use the same procedure for each of the $[K:\mathbf{Q}]$ $\mathbf{Q}$-monomorphisms $\sigma_1,\ldots,\sigma_m$ from K into $\mathbf{C}$ and obtain the corresponding extensions $\tilde{\sigma}_1,\ldots,\tilde{\sigma}_m$. In this way we obtain a system of m equations in m unknowns, the x_i:

$$\begin{array}{rcl}\tilde{\sigma}_1(x) & = & \sigma_1(\alpha_1)x_1+\cdots+\sigma_1(\alpha_m)x_m\\ \tilde{\sigma}_2(x) & = & \sigma_2(\alpha_1)x_1+\cdots+\sigma_2(\alpha_m)x_m\\ \vdots & & \vdots \qquad\quad \vdots \qquad\quad \vdots\\ \tilde{\sigma}_m(x) & = & \sigma_m(\alpha_1)x_1+\cdots+\sigma_m(\alpha_m)x_m.\end{array}$$

Applying Cramer's rule we find the expression for the x_i:

$$x_i=\frac{\nu_i}{\delta},$$

where δ is the determinant of the matrix $\big(\sigma_i(\alpha_j)\big)$ and ν_i the determinant of the matrix obtained from the previous matrix by replacing the ith column by that composed of the elements $\tilde{\sigma}_i(x)$. (As the α_j are independant , $\delta\neq 0$, from Proposition 10.8.) As $x\in O_{KL}$, x is an algebraic integer and so $\tilde{\sigma}_i(x)$ is an algebraic integer; also, the α_j belong to R and so are algebraic integers, which implies that the $\sigma_i(\alpha_j)$ are algebraic integers. It follows that δ and the ν_i are algebraic integers. Now, we have

$$\delta^2x_i=\delta\nu_i=u_i\in O_{KL}.$$

However, $\delta^2=\mathrm{disc}(R)\in\mathbf{Z}$, so

$$u_i=\mathrm{disc}(R)x_i=\sum_{i=1}^{m}\mathrm{disc}(R)q_{ij}\beta_j.$$

Hence, u_i is an algebraic integer in R and its coefficients in the basis (β_j) are $\mathrm{disc}(R)q_{ij}$. It follows that the elements $\mathrm{disc}(R)q_{ij}$ are integers. This finishes the proof. □

We now consider the relation between the discriminants of the number rings R and S and the discriminant of O_{KL}.

Theorem 11.13 *Let K and L be linearly disjoint number fields whose number rings have coprime discriminants. Then*

$$disc(O_{KL})=disc(R)^{[L:\mathbf{Q}]}disc(S)^{[K:\mathbf{Q}]}.$$

PROOF Let $m = [K : \mathbf{Q}]$, $n = [L : \mathbf{Q}]$, and $(a_1, \dots, a_m)$, $(b_1, \dots, b_n)$ be integral bases of respectively R, S. As the a_i and b_j are algebraic integers, so are the products a_ib_j, hence $a_ib_j \in O_{KL}$, for all i and j. From the previous theorem, the a_ib_j generate O_{KL} over $\mathbf{Z}$. Moreover, as K and L are linearly disjoint, the elements a_ib_j form a basis of KL over $\mathbf{Q}$ and hence are independant over $\mathbf{Z}$. Thus, the a_ib_j form an integral basis of O_{KL} and we can use this basis to calculate the discriminant of O_{KL}.

From Proposition 10.7 the discriminant of O_{KL} is the determinant of the matrix

$$M = \left(T_{KL/\mathbf{Q}}(a_ib_k \cdot a_jb_l)\right).$$

We now apply Corollary 10.3 to the tower of fields $\mathbf{Q} \subset K \subset KL$ to obtain

$$\begin{aligned} T_{KL/\mathbf{Q}}(a_ib_k \cdot a_jb_l) &= T_{K/\mathbf{Q}} \circ T_{KL/K}(a_ib_k \cdot a_jb_l) \\ &= T_{K/\mathbf{Q}}\left(T_{KL/K}(a_ia_jb_kb_l)\right) \\ &= T_{K/\mathbf{Q}}\left(a_ia_jT_{KL/K}(b_kb_l)\right), \end{aligned}$$

because $a_ia_j \in K$.

We claim that, for $l \in L$, we have $T_{KL/K}(l) = T_{L/\mathbf{Q}}(l)$. Let us consider the $[KL : K]$ K-monomorphisms from KL into $\mathbf{C}$. Restricting these monomorphisms to L we obtain $[KL : K]$ distinct $\mathbf{Q}$-monomorphisms from L into $\mathbf{C}$. As K and L are linearly disjoint over $\mathbf{Q}$, we have $[KL : K] = [L : \mathbf{Q}]$, hence the restrictions to L of the $[KL : K]$ K-monomorphisms of K into $\mathbf{C}$ are precisely the $\mathbf{Q}$-monomorphisms of L into $\mathbf{C}$. Applying Proposition 10.2 establishes the claim.

Since $b_kb_l \in L$, we have

$$T_{KL/K}(b_kb_l) = T_{L/\mathbf{Q}}(b_kb_l) \in \mathbf{Q}$$

and so

$$T_{KL/\mathbf{Q}}(a_ib_k \cdot a_jb_l) = T_{K/\mathbf{Q}}\left(a_ia_jT_{L/\mathbf{Q}}(b_kb_l)\right) = T_{L/\mathbf{Q}}(b_kb_l)T_{K/\mathbf{Q}}(a_ia_j).$$

Setting $T_{K/\mathbf{Q}}(a_ia_j) = \bar{a}_{ij}$ and $T_{L/\mathbf{Q}}(b_kb_l) = \bar{b}_{kl}$, we obtain

$$\det M = \det(\bar{a}_{ij}\bar{b}_{kl}) = \det\left((\bar{a}_{ij}) \otimes (\bar{b}_{kl})\right).$$

From Theorem H.1, we have

$$\det\left((\bar{a}_{ij}) \otimes (\bar{b}_{kl})\right) = \det(\bar{a}_{ij})^n \det(\bar{b}_{kl})^m,$$

as required. □

Application to cyclotomic fields

We now apply the previous theorems to the study of cyclotomic fields, i.e., cyclotomic extensions of the rationals. We have already studied these fields in Chapter 7. Here we will be particularly interested in the form of the associated number rings and their discriminants. We begin with the case $\mathbf{Q}(\zeta)$, where ζ is a primitive p^rth root of unity, p being a prime number and r a positive integer.

Lemma 11.4 *If ζ is a primitive nth root of unity, then the set $A = \{1, \zeta, \dots, \zeta^{\phi(n)-1}\}$ is a basis of $\mathbf{Q}(\zeta)$ over $\mathbf{Q}$. (ϕ is the Euler totient function.)*

PROOF In the proof of Theorem 7.7 we observed that $[\mathbf{Q}(\zeta):\mathbf{Q}] = \phi(n)$. As $|A| = \phi(n)$, we only need to show that the set A is linearly independant over $\mathbf{Q}$. If

$$\lambda_0 + \lambda_1\zeta + \cdots \lambda_{\phi(n)-1}\zeta^{\phi(n)-1} = 0,$$

where the λ_i are elements of $\mathbf{Q}$, which are not all zero, then ζ is a root of a nonzero polynomial $f \in \mathbf{Q}[X]$, whose degree is less than $\phi(n)$. However, the minimal polynomial of ζ over $\mathbf{Q}$ is Φ_n, whose degree is $\phi(n)$, so we have a contradiction. Hence A is a basis of $\mathbf{Q}(\zeta)$ over $\mathbf{Q}$. □

Proposition 11.10 *If p is a prime number, $r \in \mathbf{N}^*$ and ζ a primitive p^rth root of unity, then*

$$O_{\mathbf{Q}(\zeta)} = \mathbf{Z}[\zeta].$$

PROOF From Lemma 11.4 the set $A = \{1, \zeta, \ldots, \zeta^{\phi(p^r)-1}\}$ is a basis of $\mathbf{Q}(\zeta)$ over $\mathbf{Q}$. Also, the elements of this set belong to $O_{\mathbf{Q}(\zeta)}$, because ζ is an algebraic integer. The proof of Theorem 11.8 shows that

$$dO_{\mathbf{Q}(\zeta)} \subset \mathbf{Z} \oplus \mathbf{Z}\zeta \oplus \cdots \oplus \mathbf{Z}\zeta^{\phi(p^r)-1},$$

where $d = \mathrm{disc}_{\mathbf{Q}(\zeta)/\mathbf{Q}}(1, \zeta, \ldots, \zeta^{\phi(p^r)-1})$. Thus, $O_{\mathbf{Q}(\zeta)} \subset \frac{1}{d}\mathbf{Z}[\zeta]$. Moreover, from Corollary 10.6, d is a power of p (up to sign). Therefore there exists $m \in \mathbf{N}^*$ such that $p^m O_{\mathbf{Q}(\zeta)} \subset \mathbf{Z}[\zeta]$.

If

$$\mathbf{Z}[\zeta] \cap pO_{\mathbf{Q}(\zeta)} = p\mathbf{Z}[\zeta], \tag{11.1}$$

then, as $p^m O_{\mathbf{Q}(\zeta)} \subset \mathbf{Z}[\zeta]$, we have

$$p^m O_{\mathbf{Q}(\zeta)} \subset \mathbf{Z}[\zeta] \cap pO_{\mathbf{Q}(\zeta)} \subset p\mathbf{Z}[\zeta] \Longrightarrow p^{m-1}O_{\mathbf{Q}(\zeta)} \subset \mathbf{Z}[\zeta].$$

If $m = 1$, then we immediately have $O_{\mathbf{Q}(\zeta)} \subset \mathbf{Z}[\zeta]$; if not, then it is sufficient to iterate the process to obtain the same inclusion. As $\mathbf{Z}[\zeta]$ is clearly contained in $O_{\mathbf{Q}(\zeta)}$, we only need to establish the identity (11.1) to finish the proof. This is what we now do.

Our first step is to show that

$$O_{\mathbf{Q}(\zeta)}p = O_{\mathbf{Q}(\zeta)}(-\zeta + 1)^{\phi(p^r)} \tag{11.2}$$

To begin,

$$\Phi_{p^r}(X) = \prod_{1 \le i < p^r, (i,p)=1} (-\zeta^i + X) \Longrightarrow \Phi_{p^r}(1) = \prod_{1 \le i < p^r, (i,p)=1} (-\zeta^i + 1).$$

However, from Exercise 7.4, we know that

$$\Phi_{p^r}(X) = \Phi_p(X^{p^{r-1}})$$

so

$$p = \Phi_{p^r}(1) = \prod_{1 \le i < p^r, (i,p)=1} (-\zeta^i + 1).$$

Next we observe that the elements $\frac{-\zeta^i+1}{-\zeta+1}$, with $1 \le i < p^r$ and $(i,p) = 1$, are units in $O_{\mathbf{Q}(\zeta)}$. We have

$$\frac{-\zeta^i + 1}{-\zeta + 1} = 1 + \zeta + \cdots + \zeta^{i-1} \in O_{\mathbf{Q}(\zeta)}.$$

As ζ^i is a primitive p^rth root of unity, there exists $s \in \mathbf{N}^*$ such that $\zeta = \zeta^{is}$, hence

$$\frac{-\zeta+1}{-\zeta^i+1} = \frac{-\zeta^{is}+1}{-\zeta^i+1} = 1 + \zeta^i + \cdots + \zeta^{i(s-1)} \ \in \ O_{\mathbf{Q}(\zeta)},$$

so $\frac{-\zeta^i+1}{-\zeta+1}$ is a unit in $O_{\mathbf{Q}(\zeta)}$.

We may write

$$-\zeta^i + 1 = \frac{-\zeta^i+1}{\zeta+1} \cdot (-\zeta+1) = u_i(-\zeta+1),$$

so

$$p = \prod_{1 \le i < p^r, (i,p)=1} u_i(-\zeta+1) = u(-\zeta+1)^{\phi(p^r)},$$

where u is a unit in $O_{\mathbf{Q}(\zeta)}$. As p and $(-\zeta+1)^{\phi(p^r)}$ are associates in $O_{\mathbf{Q}(\zeta)}$, they generate the same ideal, i.e.,

$$O_{\mathbf{Q}(\zeta)}p = O_{\mathbf{Q}(\zeta)}(-\zeta+1)^{\phi(p^r)},$$

as asserted.

Our second step is to show that

$$O_{\mathbf{Q}(\zeta)}(-\zeta+1) \cap \mathbf{Z} = \mathbf{Z}p. \tag{11.3}$$

From the identity (11.2) we obtain $p \in (-\zeta+1)O_{\mathbf{Q}(\zeta)}$, and so $p\mathbf{Z} \subset (-\zeta+1)O_{\mathbf{Q}(\zeta)} \cap \mathbf{Z}$. Now the reverse inclusion. If $x \in (-\zeta+1)O_{\mathbf{Q}(\zeta)}$, then $x = y(-\zeta+1)$, with $y \in O_{\mathbf{Q}(\zeta)}$, and

$$N_{\mathbf{Q}(\zeta)/\mathbf{Q}}(x) = N_{\mathbf{Q}(\zeta)/\mathbf{Q}}(y)N_{\mathbf{Q}(\zeta)/\mathbf{Q}}(-\zeta+1).$$

As $y \in O_{\mathbf{Q}(\zeta)}$, $N_{\mathbf{Q}(\zeta)/\mathbf{Q}}(y) \in \mathbf{Z}$ (Exercise 11.1). Also, from Corollary 10.1,

$$N_{\mathbf{Q}(\zeta)/\mathbf{Q}}(-\zeta+1) = \prod_{1 \le i < p^r, (i,p)=1} (-\zeta^i+1) = p,$$

because $\mathbf{Q}(\zeta)$ is the splitting field of the polynomial $\Phi_{p^r}(1-X)$, whose roots are $-\zeta^i+1$, with $1 \le i < p^r$ and $(i,p) = 1$. Finally, as $x \in \mathbf{Z}$, $N_{\mathbf{Q}(\zeta)/\mathbf{Q}}(x) = x^{\phi(p^r)}$, so $p|x$, i.e., $x \in p\mathbf{Z}$. This concludes the second step. We have

$$O_{\mathbf{Q}(\zeta)}(-\zeta+1) \cap \mathbf{Z} = \mathbf{Z}p,$$

as required.

We are now in a position to prove the identity (11.1). There is no difficulty in seeing that

$$\mathbf{Z}[\zeta]p \subset \mathbf{Z}[\zeta] \cap O_{\mathbf{Q}(\zeta)}p.$$

For the reverse inclusion, let us take $x \in \mathbf{Z}[\zeta] \cap O_{\mathbf{Q}(\zeta)}p$. Using the fact that $A = \{1, \zeta, \ldots, \zeta^{\phi(p^r)-1}\}$ is a basis of $\mathbf{Q}(\zeta)$ over $\mathbf{Q}$, we see that the set $B = \{1, -\zeta+1, \ldots, (-\zeta+1)^{\phi(p^r)-1}\}$ is also a basis of $\mathbf{Q}(\zeta)$ over $\mathbf{Q}$. The set B is included in $\mathbf{Z}[\zeta]$ and is independant over $\mathbf{Z}$, because it is independant over $\mathbf{Q}$. As A is a generating set of $\mathbf{Z}[\zeta]$ and the elements of A can be written as linear combinations of those of B with coefficients in $\mathbf{Z}$, B is a generating set of $\mathbf{Z}[\zeta]$. Thus B is a basis of the $\mathbf{Z}$-module $\mathbf{Z}[\zeta]$. Therefore there exist integers $c_0, c_1, \ldots, c_{\phi(p^r)-1}$ such that

$$x = c_0 + c_1(-\zeta+1) + \cdots + c_{\phi(p^r)-1}(-\zeta+1)^{\phi(p^r)-1}.$$

Moreover, from the identity (11.2), there exists $v \in O_{\mathbf{Q}(\zeta)}$ such that $x = (-\zeta+1)^{\phi(p^r)}v$. Thus $c_0 \in O_{\mathbf{Q}(\zeta)}(-\zeta+1) \cap \mathbf{Z}$, which from the identity (11.3) is equal to $\mathbf{Z}p$. Therefore $c_0 \in p\mathbf{Z}$. Using the identity (11.2) again, we see that $p \in (-\zeta+1)^{\phi(p^r)}O_{\mathbf{Q}(\zeta)}$, hence $x - c_0 \in (-\zeta+1)^{\phi(p^r)}O_{\mathbf{Q}(\zeta)}$. We may write $x - c_0 = (-\zeta+1)x_1$, where

$$x_1 = c_1 + c_2(-\zeta+1)\cdots + c_{\phi(p^r)-1}(-\zeta+1)^{\phi(p^r)-2} \ \in \ (-\zeta+1)^{\phi(p^r)-1}O_{\mathbf{Q}(\zeta)}.$$

As for c_0, we find that $c_1 \in \mathbf{Z}p$. Continuing in the same way, we obtain that $c_i \in \mathbf{Z}p$, for all i and so $x \in \mathbf{Z}[\zeta]p$. This ends the proof. □

We have shown that $O_{\mathbf{Q}(\zeta)} = \mathbf{Z}[\zeta]$ when ζ is a p^rth root of unity. We now turn to the general case. Here Theorem 11.12 plays an important role. We will need a preliminary result.

Lemma 11.5 *If ζ is a primitive nth root of unity, then the discriminant $disc_{\mathbf{Q}(\zeta)/\mathbf{Q}}(1,\zeta,\ldots,\zeta^{\phi(n)-1})$ divides $n^{\phi(n)}$.*

PROOF From Proposition 10.9

$$\mathrm{disc}_{\mathbf{Q}(\zeta)/\mathbf{Q}}(1,\zeta,\ldots,\zeta^{\phi(n)-1}) = (-1)^{\frac{\phi(n)(\phi(n)-1)}{2}} N_{\mathbf{Q}(\zeta)/\mathbf{Q}}(\Phi'_n(\zeta)).$$

Since Φ_n is the minimal polynomial of ζ over $\mathbf{Q}$ and $\zeta^n = 1$. there exists $g \in \mathbf{Q}[X]$ such that

$$-1 + X^n = \Phi_n(X)g(X).$$

As Φ_n is monic, g is also monic and Lemma 11.1 ensures that $g \in \mathbf{Z}[X]$. Differentiating both sides of the previous equation and evaluating at ζ leads to

$$n\zeta^{n-1} = \Phi'_n(\zeta)g(\zeta) \Longrightarrow n = \zeta\Phi'_n(\zeta)g(\zeta).$$

Taking the norm on both sides, we obtain

$$n^{\phi(n)} = N_{\mathbf{Q}(\zeta)/\mathbf{Q}}\big(\Phi'_n(\zeta)\big)N_{\mathbf{Q}(\zeta)/\mathbf{Q}}\big(\zeta g(\zeta)\big).$$

However, $\Phi'_n(\zeta)$ and $\zeta g(\zeta)$ are elements of $\mathbf{Z}[\zeta]$, which is included in $O_{\mathbf{Q}(\zeta)}$. Applying Exercise 11.1 we obtain the result. □

Theorem 11.14 *If ζ is a primitive nth root of unity, then*

$$O_{\mathbf{Q}(\zeta)} = \mathbf{Z}[\zeta].$$

PROOF We will use an induction on s, the number of prime factors in the decomposition of n. For $s = 1$, we have already proved the result, so we consider the induction step. Let us suppose that the result is true up to $s-1$. We now consider the case s. We have

$$n = p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_s^{\alpha_s} = m_1m_2,$$

where $m_1 = p_1^{\alpha_1}$ and $m_2 = p_2^{\alpha_2}\cdots p_s^{\alpha_s}$. As m_1 and m_2 are coprime, from Proposition 7.6

$$\mathbf{Q}(\zeta_{m_1})\mathbf{Q}(\zeta_{m_2}) = \mathbf{Q}(\zeta_n),$$

where ζ_u is a primitive uth root of unity. From Proposition 11.10 (or the induction hypothesis),

$$\mathrm{disc}(O_{\mathbf{Q}(\zeta_{m_1})}) = \mathrm{disc}_{\mathbf{Q}(\zeta_{m_1})/\mathbf{Q}}(1,\zeta_{m_1},\ldots,\zeta_{m_1}^{\phi(m_1)-1}),$$

because $\{1, \zeta_{m_1}, \ldots, \zeta_{m_1}^{\phi(m_1)-1}\}$ is an integral basis of $O_{\mathbf{Q}(\zeta_{m_1})}$. Also, by the induction hypothesis,

$$\operatorname{disc}(O_{\mathbf{Q}(\zeta_{m_2})}) = \operatorname{disc}_{\mathbf{Q}(\zeta_{m_2})/\mathbf{Q}}(1, \zeta_{m_2}, \ldots, \zeta_{m_2}^{\phi(m_2)-1}),$$

because $\{1, \zeta_{m_2}, \ldots, \zeta_{m_2}^{\phi(m_2)-1}\}$ is an integral basis of $O_{\mathbf{Q}(\zeta_{m_2})}$. From Lemma 11.5, as $m_1^{\phi(m_1)}$ and $m_2^{\phi(m_2)}$ are coprime, so are the discriminants $\operatorname{disc}(O_{\mathbf{Q}(\zeta_{m_1})})$ and $\operatorname{disc}(O_{\mathbf{Q}(\zeta_{m_2})})$. In addition, $\mathbf{Q}(\zeta_{m_1})$ and $\mathbf{Q}(\zeta_{m_2})$ are linearly disjoint over $\mathbf{Q}$, because $\phi(m_1 m_2) = \phi(m_1)\phi(m_2)$. Applying Theorem 11.12 and the induction hypothesis, we obtain

$$O_{\mathbf{Q}(\zeta_n)} = O_{\mathbf{Q}(\zeta_{m_1})} O_{\mathbf{Q}(\zeta_{m_2})} = \mathbf{Z}[\zeta_{m_1}]\mathbf{Z}[\zeta_{m_2}].$$

Given that $\zeta_n^{m_2}$ is a primitive m_1th root of unity, $\zeta_{m_1} \in \mathbf{Z}[\zeta_n]$. In the same way, $\zeta_{m_2} \in \mathbf{Z}[\zeta_n]$, so $\mathbf{Z}[\zeta_{m_1}]\mathbf{Z}[\zeta_{m_2}] \subset \mathbf{Z}[\zeta_n]$. Moreover, as m_1 and m_2 are coprime, there exist integers u and v such that $m_1 u + m_2 v = 1$. Thus,

$$\zeta_n = (\zeta_n^{m_2})^v (\zeta_n^{m_1})^u \in \mathbf{Z}[\zeta_{m_1}]\mathbf{Z}[\zeta_{m_2}] \Longrightarrow \mathbf{Z}[\zeta_n] \subset \mathbf{Z}[\zeta_{m_1}]\mathbf{Z}[\zeta_{m_2}],$$

therefore

$$\mathbf{Z}[\zeta_n] = \mathbf{Z}[\zeta_{m_1}]\mathbf{Z}[\zeta_{m_2}] = O_{\mathbf{Q}(\zeta_n)},$$

as required. □

We now turn to the discriminant of a cyclotomic number ring $O_{\mathbf{Q}(\zeta)}$. Proposition 10.9 ensures that

$$\Delta(\Phi_n) = \operatorname{disc}_{\mathbf{Q}(\zeta)/\mathbf{Q}}(1, \zeta, \ldots, \zeta^{\phi(n)-1}) = \operatorname{disc}(O_{\mathbf{Q}(\zeta)}),$$

so, in finding $\operatorname{disc}(O_{\mathbf{Q}(\zeta)})$, we find $\Delta(\Phi_n)$, or vice-versa. In fact, we have already found $\Delta(\Phi_{p^r})$, where p is a prime number and r a positive integer (Corollary 10.6). We now generalize this result. Theorem 11.13 will play an important role.

Theorem 11.15 *Let ζ be a primitive nth root of unity. Then*

$$\Delta(\Phi_n) = disc(O_{\mathbf{Q}(\zeta)}) = \frac{(-1)^{c_n} n^{\phi(n)}}{\prod_{p|n} p^{\frac{\phi(n)}{p-1}}},$$

where $c_n = \frac{\phi(n)}{2}$, if $n \neq 2$ and $c_2 = 0$.

PROOF We will use an induction on s, the number of prime factors in n. First, if n has a single prime factor p, the $n = p^r$, for some $r \in \mathbf{N}^*$. In Corollary 10.6 we found the expression

$$\Delta(\Phi_{p^r}) = (-1)^c p^{p^{r-1}(r(p-1)-1)},$$

where $c = \frac{\phi(p^r)}{2}$, if p is odd or $r > 1$, and $c = 0$ otherwise. However,

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

and

$$\prod_{p|p^r} p^{\frac{\phi(p^r)}{p-1}} = \prod_{p|p^r} p^{p^{r-1}} = p^{p^{r-1}}.$$

Hence, if $n = p^r$, i.e., $s = 1$, then the expression for $\Delta(\Phi_n)$ given in the statement of the theorem is correct.

Let us now suppose that $s \geq 2$ and that the result is true up to $s-1$. We have

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_s^{\alpha_s} = m_1 m_2,$$

where $m_1 = p_1^{\alpha_1}$ and $m_2 = p_2^{\alpha_2} \cdots p_s^{\alpha_s}$. As in the proof of Theorem 11.14, we find that $\mathrm{disc}(O_{m_1})$ and $\mathrm{disc}(O_{m_2})$ are coprime. Using the induction hypothesis and Theorem 11.13 we obtain

$$\begin{aligned}
\mathrm{disc}(O_{\mathbf{Q}(\zeta_n)}) &= \left(\frac{(-1)^{c_{m_1}} m_1^{\phi(m_1)}}{\prod_{p|m_1} p^{\frac{\phi(m_1)}{p-1}}}\right)^{\phi(m_2)} \times \left(\frac{(-1)^{c_{m_2}} m_2^{\phi(m_2)}}{\prod_{p|m_2} p^{\frac{\phi(m_2)}{p-1}}}\right)^{\phi(m_1)} \\
&= \frac{(-1)^{c_{m_1}\phi(m_2)+c_{m_2}\phi(m_1)} n^{\phi(n)}}{\prod_{p|n} p^{\frac{\phi(n)}{p-1}}}.
\end{aligned}$$

To finish the induction step we only need to consider the term $(-1)^{c_{m_1}\phi(m_2)+c_{m_2}\phi(m_1)}$. If all the primes in n are odd, then

$$c_{m_1}\phi(m_2) = c_{m_2}\phi(m_1) \Longrightarrow (-1)^{c_{m_1}\phi(m_2)+c_{m_2}\phi(m_1)} = (-1)^{2\frac{\phi(n)}{2}} = 1.$$

If $p_1 = 2$ and $\alpha_1 \geq 2$, then we have an analogous argument. To finish, suppose that $p_1 = 2$ and $\alpha_1 = 1$. Then

$$c_{m_1}\phi(m_2) + c_{m_2}\phi(m_1) = \frac{\phi(m_1)\phi(m_2)}{2} = \frac{\phi(n)}{2} = c_n,$$

because n has at least two factors. This ends the induction step. □

We have seen in Theorem 11.14 that if α is a primitive nth root of unity, then the number ring of $\mathbf{Q}(\alpha)$ is $\mathbf{Z}[\alpha]$. In Theorem 11.6 we observed a similar phenomenon for the case where α is the square root of a square-free integer $d = 2, 3 \pmod 4$. In the next proposition we give another criterion.

Proposition 11.11 *If K is a number field, then there is an algebraic integer s such that $K = \mathbf{Q}(s)$. If the discriminant of the minimal polynomial $m(s, \mathbf{Q})$ is a square-free integer, then $O_K = \mathbf{Z}[s]$.*

PROOF The primitive element theorem (Theorem 3.4) ensures that for any number field K, there is an element $t \in K$ such that $K = \mathbf{Q}(t)$. Since t is an algebraic number, because K is a finite extension of $\mathbf{Q}$, Lemma 11.2 ensures that $t = \frac{s}{k}$, where s is an algebraic integer and k a positive integer. Consequently, $K = \mathbf{Q}(s)$, for some algebraic integer s.

As $s \in O_K$, we must have $\mathbf{Z}[s] \subset O_K$. We now aim to show that the condition on the discriminant of the minimal polynomial $m(s, \mathbf{Q})$ ensures the reverse inclusion. From Theorem 11.8 we obtain that the number ring O_K has an integral basis $\{x_0, \ldots, x_{n-1}\}$, where $n = [K : \mathbf{Q}]$. Since $s \in O_K$, there is a matrix $M \in \mathcal{M}_n(\mathbf{Z})$ such that

$$\begin{pmatrix} 1 \\ s \\ \vdots \\ s^{n-1} \end{pmatrix} = M \begin{pmatrix} x_0 \\ x_1 \\ \vdots \\ x_{n-1} \end{pmatrix},$$

Let $\sigma_1, \ldots, \sigma_n$ be the $\mathbf{Q}$-monomorphisms from K into $\mathbf{C}$. For $j = 1 \ldots, n$, we have

$$\begin{pmatrix} \sigma_j(1) \\ \sigma_j(s) \\ \vdots \\ \sigma_j(s^{n-1}) \end{pmatrix} = M \begin{pmatrix} \sigma_j(x_0) \\ \sigma_j(x_1) \\ \vdots \\ \sigma_j(x_{n-1}) \end{pmatrix},$$

We may write this expression in matrix form:

$$\left(\sigma_j(s^i)\right) = M\left(\sigma_j(x_i)\right).$$

Taking determinants and squaring we obtain

$$\mathrm{disc}_{K/\mathbf{Q}}(1, s, \ldots, s^{n-1}) = (\det M)^2 \mathrm{disc}_{K/\mathbf{Q}}(x_0, x_1, \ldots, x_{n-1}).$$

Now Proposition 10.9 ensures that $\mathrm{disc}_{K/\mathbf{Q}}(1, s, \ldots, s^{n-1})$ is the discriminant of the minimal polynomial $m(s, \mathbf{Q})$, which, by hypothesis, is a square-free integer. In addition, the discriminant $\mathrm{disc}_{K/\mathbf{Q}}(x_0, x_1, \ldots, x_{n-1})$ belongs to $\mathbf{Z}$. (Clearly, $\mathrm{disc}_{K/\mathbf{Q}}(x_0, x_1, \ldots, x_{n-1}) \in \mathbf{Q}$; it is integral over $\mathbf{Z}$, because each x_i is integral over $\mathbf{Z}$.) Since $\det M \in \mathbf{Z}$, because $M \in \mathcal{M}_n(\mathbf{Z})$, we have $\det M = \pm 1$, and it follows that the entries of M^{-1} are integers. As

$$\begin{pmatrix} x_0 \\ x_1 \\ \vdots \\ x_{n-1} \end{pmatrix} = M^{-1} \begin{pmatrix} 1 \\ s \\ \vdots \\ s^{n-1} \end{pmatrix},$$

and the x_i generate O_K, the s^i also generate O_K over $\mathbf{Z}$, which proves that $O_K \subset \mathbf{Z}[s]$, as required, and so $O_K = \mathbf{Z}[s]$.

As the set $\{1, s, \ldots, s^{n-1}\}$ is independant over $\mathbf{Z}$, it is an integral basis of O_K. □

Example Let $K = \mathbf{Q}(\alpha)$, where $-1 - \alpha + \alpha^3 = 0$. The minimal polynomial of α over $\mathbf{Q}$ is $f(X) = -1 - X + X^3$, whose discriminant is -23. As -23 is square-free, we have $O_K = \mathbf{Z}[\alpha]$.

Remark We should notice that, if the discriminant of the minimal polynomial of α is not square-free, then O_K may or may not be equal to $\mathbf{Z}[\alpha]$; it is sufficient to consider the case where d is square-free and $\alpha = \sqrt{d}$.

11.5 Ideals in number rings

In this section we concentrate on the properties of ideals in number rings. Our first result concerns the factor ring O_K/I for an nonzero ideal. We recall that n denotes the dimension of K over $\mathbf{Q}$.

Proposition 11.12 *If I is a nonzero ideal in a number ring O_K, then the factor ring O_K/I is finite.*

PROOF Let I be a nonzero ideal in the number ring O_K and α a nonzero element of I. We set $m = N_{K/\mathbf{Q}}(\alpha)$. As $\alpha \in O_K$, α is an algebraic integer and so $m \in \mathbf{Z}$. From the definition of the norm, $m \neq 0$. We claim that $m \in I$: From Proposition 10.2, $m = \alpha\beta$, where β is a product of conjugates of α (in $\mathbf{C}$); as $m, \alpha \in K$, $\beta = \frac{m}{\alpha} \in K$. As a conjugate of an algebraic integer is also an algebraic integer, β is an algebraic integer. Thus $\beta \in O_K$ and it follows that $m \in I$, as claimed.

As $m \in I$, the principal ideal (m) is included in I. Since the rank of the free abelian group O_K is n, then it is easy to see that $O_K/(m)$ is isomorphic to $\mathbf{Z}_m^n$, hence $|O_K/(m)| = m^n$. Also, $(m) \subset I$ implies that the mapping

$$\phi : O_K/(m) \longrightarrow O_K/I, x + (m) \longmapsto x + I$$

is a well-defined surjective homomorphism. Therefore O_K/I is finite. □

Corollary 11.5 *If I is a nonzero ideal in a number ring O_K, then the rank of I as a free abelian group is the same as that of O_K.*

PROOF If $\operatorname{rk} O_K = n$ and $\operatorname{rk} I = r$, then $r \leq n$ (Theorem E.3). There is a basis $(e_1, \ldots, e_n)$ of O_K and elements $d_1, \ldots, d_r \in \mathbf{Z}$, with $d_i \leq d_{i+1}$, such that $(d_1 e_I, \ldots, d_r e_r)$ is a basis of I. We define a mapping ϕ from O_K onto $\mathbf{Z}_{d_1} \times \cdots \times \mathbf{Z}_{d_r} \times \mathbf{Z}^{n-r}$ by

$$\phi(x_1 e_1 + \cdots x_n e_n) = (x_1 + d_1\mathbf{Z}, \ldots, x_r + d_r\mathbf{Z}, x_{r+1}, \ldots, x_n).$$

It is clear that ϕ is a surjective group homomorphism. Also,

$$\operatorname{Ker} \phi = \{x_1 e_1 + \cdots + x_n e_n : x_1 \in d_1\mathbf{Z}, \ldots, x_r \in d_r\mathbf{Z}, x_{r+1} = \cdots = x_n = 0\} = I.$$

Hence, as groups,

$$O_K/I \simeq \mathbf{Z}_{d_1} \times \cdots \times \mathbf{Z}_{d_r} \times \mathbf{Z}^{n-r}.$$

However, O_K/I is finite, so the last term on the right-hand side must be $\{0\}$, i.e., $r = n$. □

The next property of ideals in number rings is useful.

Proposition 11.13 *If I is a nonzero ideal in a number ring O_K, then there is a nonzero integer α in I.*

PROOF Let α be a nonzero element of I. There exists a monic polynomial $f \in \mathbf{Z}[X]$ such that $f(\alpha) = 0$. We may suppose that the constant term of f is nonzero. (If not, we may write $f(X) = X^s g(X)$, with $g(0) \neq 0$ and $g(\alpha) = 0$ and replace f by g.) Then,

$$\alpha | f(\alpha) - f(0) \Longrightarrow f(\alpha) - f(0) \in I.$$

Now, $f(\alpha) - f(0) = -f(0) \in \mathbf{Z}^*$, therefore I has a nonzero integer α. □

Remark As $\mathbf{Z} \subset O_K$, the set $\mathbf{Z}\alpha \subset I$, so there is an infinite number of nonzero integers in I.

We now consider prime ideals in a number ring.

Theorem 11.16 *If I is a nonzero prime ideal in a number ring O_K, then I is a maximal ideal.*

PROOF From Proposition 11.12 we know that O_K/I is a finite ring. If I is a prime ideal, then the quotient ring O_K/I is an integral domain. However, a finite integral domain is a field. This implies that I is a maximal ideal. □

We recall that a ring R is noetherian if every ascending sequence of ideals $I_0 \subset I_1 \subset \cdots$ is finally stationary, i.e., there exists an ideal I_k in the sequence such that $I_k = I_{k+1} = \cdots$. This condition is equivalent to showing that every ideal I in R is finitely generated.

Theorem 11.17 *A number ring O_K is noetherian.*

PROOF We will show that every ideal I in O_K is finitely generated. If $I = \{0\}$, then there is nothing to prove, so let us suppose that I is nonzero. I is a free abelian group of rank n, the rank of O_K. Thus I has a finite basis and so is finitely generated. □

An integral domain D is said to be a *Dedekind domain* if it has the following properties:

- D is normal;
- D is noetherian;
- every nonzero prime ideal in D is maximal.

We have shown above that a number ring is a Dedekind domain. As many of the properties of number rings are derived from their properties as Dedekind domains, for the moment we will handle the more general case. Later we will return to the more specific case of number rings.

Chapter 12

Dedekind domains

In the last chapter we defined the notion of a Dedekind domain and we saw that number rings are examples of such domains. Dedekind domains are not in general UFDs. However, we will see that the ideals have an interesting factorization similar to that found in UFDs. This statement will be made more precise in the following. We will begin with some preliminary results.

Exercise 12.1 *Show that* $\mathbf{Z}[\sqrt{-5}]$ *is a Dedekind domain. Prove that* 2 *is irreducible in* $\mathbf{Z}[\sqrt{-5}]$*, but not prime, and so deduce that* $\mathbf{Z}[\sqrt{-5}]$ *is not a UFD.*

12.1 Elementary results

We have seen in the last chapter that number rings are Dedekind domains. There is another large class of Dedekind domains.

Theorem 12.1 *A principal ideal domain is a Dedekind domain.*

PROOF Let R be a PID. As every ideal in R is generated by a unique element, R is noetherian.

Next we show that R is a normal domain. Let $x = \frac{a}{b}$ be an element of the field of fractions of R. We suppose that a and b are coprime. If x is algebraic over R, then there exists an equation of the form

$$a_0 + a_1\left(\frac{a}{b}\right) + \cdots + a_{n-1}\left(\frac{a}{b}\right)^{n-1} + \left(\frac{a}{b}\right)^n = 0,$$

where the a_i belong to R. Multiplying by b^n we obtain an equation

$$bc + a^n = 0$$

with $c \in R$. Hence $bc = -a^n$. As R is a UFD and a and b are coprime, b is a unit and it follows that $b^{-1} \in R$. Hence $x = \frac{a}{b} \in R$. Therefore R is a normal domain.

It remains to show that a nonzero prime ideal is maximal. Let (a) be a prime ideal in R. (a) is included in a maximal ideal (b) and there exists $k \in R$ such that $a = kb$. As a is prime, a is irreducible, which implies that k is invertible and it follows that $(a) = (b)$. □

To continue, we need two lemmas, the second depending on the first.

Lemma 12.1 *In a Dedekind domain* D *every nonzero ideal* I *contains a product of nonzero prime ideals.*

PROOF Suppose that the proposition is not true and let $\mathcal{C}$ be the collection of nonzero ideals in D which do not contain a product of nonzero prime ideals. As D is noetherian, $\mathcal{C}$ contains a maximal element M. (If not, then it would be possible to create an infinite chain of distinct ideals, contradicting the noetherian hypothesis.) As $M \in \mathcal{C}$, M is not a prime ideal, hence there exist $x, y \in D \setminus M$ such that $xy \in M$. Clearly, M is strictly contained in the ideals $M + (x)$ and $M + (y)$, which are not elements of $\mathcal{C}$, because M is maximal. It follows that $M + (x)$ and $M + (y)$ both contain products of nonzero prime ideals, so the ideal $(M + (x))(M + (y))$ also contains a product of nonzero prime ideals. As this ideal is included in M, which is an element of $\mathcal{C}$, we have a contradiction. □

The proof of the second lemma is a little longer.

Lemma 12.2 *Let D be a Dedekind domain, with fraction field K, and I a proper ideal in D. Then there exists $\alpha \in K \setminus D$ such that $\alpha I \subset D$.*

PROOF If $I = \{0\}$, then the result is obvious, so let us suppose that this is not the case. We fix $a \neq 0$ in I. From Lemma 12.1, the principal ideal (a) contains a product of nonzero prime ideals. We take such a product $P_1 \dots P_r$, with r minimal. If $r = 1$, then we have

$$P_1 \subset (a) \subset I = P_1,$$

because P_1 is maximal, hence $I = (a)$. Since I is a proper ideal in D, we can take $b \in D \setminus (a)$; then $\alpha = \frac{b}{a} \notin D$, because in this case we would have $b \in (a)$, a contradiction. If $x \in I$ then there exists $s \in D$, such that $x = sa$, hence

$$\alpha x = \frac{b}{a} x = \frac{b}{a} sa = b \in D,$$

so for $r = 1$ the statement is true.

Now suppose that $r > 1$. Since I is a proper ideal in D, Zorn's lemma ensures that there exists a maximal ideal M such that $I \subset M$. The ideal M contains at least one of the ideals P_i. (If not, then, for all i, there exists $a_i \in P_i \setminus M$; however, the product $a_1 \cdots a_r \in M$, which is prime, implying that a certain $a_j \in M$, a contradiction.) If P_j is a prime ideal contained in M, then $P_j = M$, because all nonzero prime ideals are maximal. Without loss of generality let us suppose that $j = 1$. As r is minimal, there exists $b \in (P_2 \cdots P_r) \setminus (a)$. We consider $\alpha = \frac{b}{a}$. As above $\alpha \notin D$, hence $\alpha \in K \setminus D$. Then

$$IP_2 \cdots P_r \subset MP_2 \cdots P_r = P_1 P_2 \cdots P_r \subset (a) \Longrightarrow Ib \subset (a).$$

Hence, if $x \in I$ then there exists $s \in D$, such that $xb = sa$, which implies that

$$\alpha x = \frac{b}{a} x = s \in D$$

and so $\alpha I \subset D$. □

We may now establish a result which will prove important further on, but is also interesting in its own right.

Theorem 12.2 *If I is an ideal in a Dedekind domain, then there is a nonzero ideal J in D such that IJ is a principal ideal.*

PROOF If $I = \{0\}$, then we may take any ideal in D for J, because in this case $IJ = \{0\}$, which is a principal ideal. So let us now take I nonzero. We choose $a \in I$, with $a \neq 0$ and set $J = \{b \in D : bI \subset (a)\}$. Then J is a nonzero ideal and $IJ \subset (a)$.

Let us now consider the set $A = \frac{1}{a}IJ$. As $IJ \subset (a)$, $A \subset D$; also A is an ideal in D. If $A = D$, then $IJ = (a)$ and we have the result we are looking for. If this is not the case, then A is a proper ideal in D and we can apply Lemma 12.2: there exists $\gamma \in K \setminus D$ such that $\gamma A \subset D$.

We now notice that A contains J: as $a \in I$, $1 = \frac{1}{a}a \in \frac{1}{a}I$, hence $J \subset \frac{1}{a}IJ$. It follows that $\gamma J \subset \gamma A \subset D$. This allows us to show that $\gamma J \subset J$:

$$\gamma A \subset D \Longrightarrow \gamma IJ \subset (a) \Longrightarrow (\gamma J)I \subset (a) \Longrightarrow \gamma J \subset J.$$

As D is noetherian, the ideal J has a finite generating set $a_1, \ldots, a_m$. Using the relation $\gamma J \subset J$, we may find a matrice $M \in \mathcal{M}_n(D)$ such that

$$\gamma \begin{pmatrix} a_1 \\ \vdots \\ a_m \end{pmatrix} = M \begin{pmatrix} a_1 \\ \vdots \\ a_m \end{pmatrix},$$

which implies that

$$(\gamma I_m - M) \begin{pmatrix} a_1 \\ \vdots \\ a_m \end{pmatrix} = \begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix}.$$

As the a_i are not all 0, we have $\det(\gamma I_m - M) = 0$. Thus γ is the root of a polynomial $f \in D[X]$. However, D is a normal domain, so $\gamma \in D$, a contradiction. We have shown that $IJ = (a)$, i.e., IJ is principal. □

The result which we have just proved has two immediate consequences. The first of these is a cancellation rule for ideals in a Dedekind domain.

Corollary 12.1 *If A, B and C are ideals in a Dedekind domain D, with A nonzero, then*

$$AB = AC \Longrightarrow B = C.$$

PROOF There exists a nonzero ideal J such that AJ is principal: $AJ = (a)$, with $a \neq 0$, because A and J are nonzero. Hence,

$$AB = AC \Longrightarrow AJB = AJC \Longrightarrow (a)B = (a)C \Longrightarrow aB = aC.$$

Multiplying by a^{-1}, we obtain $B = C$. □

In a commutative ring R we may define a division on ideals in a natural way. If I and J are ideals, then we say that I divides J, and write $I|J$, if there exists an ideal K such that $IK = J$. In Dedekind domains this is equivalent to an inclusion condition.

Corollary 12.2 *If A and B are ideals in a Dedekind domain, then*

$$A|B \Longleftrightarrow A \supset B.$$

PROOF If A divides B, then there exists an ideal C such that $AC = B$. If $b \in B$, then there exist $a_1, \ldots, a_s \in A$ and $c_1, \ldots, c_s \in C$ such that $b = a_1c_1 + \cdots + a_sc_s$. However, $a_ic_i \in A$, for all i, and so $b \in A$. Therefore $B \subset A$.

Now suppose that $A \supset B$. If $A = \{0\}$, then $B = \{0\}$ and it is clear that A divides B. Suppose now that $A \neq \{0\}$. There exists a nonzero ideal J and $a \in D^*$ such that $AJ = (a)$. Let us set $C = \frac{1}{a}JB$. Then

$$B \subset A \Longrightarrow \frac{1}{a}JB \subset \frac{1}{a}JA = \frac{1}{a}(a) = D.$$

It is easy to see that C is an ideal in D. We have

$$AC = A\frac{1}{a}JB = DB = B$$

and so A divides B. □

12.2 Prime factorization of ideals

We have seen that a nonzero ideal in a Dedekind domain contains a product of nonzero prime ideals. In fact, we can strengthen this statement.

Theorem 12.3 *In a Dedekind domain D, every ideal $I \neq \{0\}, D$ can be expressed in a unique way as a product of nonzero prime ideals.*

PROOF Suppose that there exists an ideal $I \neq \{0\}, D$ which cannot be expressed as a product of prime ideals. As D is noetherian, the collection of such ideals has a maximal element M. The ideal proper M is included in a maximal ideal P. As P is a maximal ideal, P is a prime ideal. However, from Corollary 12.2, $P \supset M$ implies that $P|M$, i.e., there exists an ideal I such that $PI = M$. Using Corollary 12.2 again, we obtain $I \supset M$. If $I = M$, then, using Corollary 12.1,

$$DM = DPI = PDM = PM \Longrightarrow D = P,$$

a contradiction. Hence we have $M \subsetneqq I$ and so I is a product of prime ideals. As $M = PI$, M is also a product of prime ideals, which is a contradiction. It follows that an any ideal $I \neq \{0\}, D$ is a product of prime ideals.

We now consider the uniqueness. Suppose that

$$P_1P_2\cdots P_r = Q_1Q_2\cdots Q_s,$$

where the P_i and Q_j are nonzero prime ideals (not necessarily distinct). Then

$$P_1|Q_1Q_2\cdots Q_s \Longrightarrow P_1 \supset Q_i,$$

for some i (see the proof of Lemma 12.2). Without loss of generality, let us suppose that $i = 1$. As Q_1 is maximal, $P_1 = Q_1$. Using Corollary 12.1 we obtain

$$P_2\cdots P_s = Q_2\cdots Q_r.$$

Continuing in the same way we obtain the postulated uniqueness. □

Corollary 12.3 *In a Dedekind domain a countable intersection of distinct nonzero prime ideals is trivial.*

PROOF Let $(P_n)_{n\in\mathbf{N}}$ be a collection of distinct nonzero prime ideals in a Dedekind domain D and $I = \cap_{n\in\mathbf{N}} P_n$. We have

$$P_n \supset I \Longrightarrow P_n|I,$$

for each n. If I is nontrivial, then I has a unique decomposition into prime ideals and each P_n must appear in this decomposition. This is impossible, because the decomposition is composed of a finite number of prime ideals. Hence the result. □

An integral domain which is principal ideal domain (PID) is always a unique factorization domain (UFD). For a Dedekind domain the converse is also true. This is a corollary of the theorem which we have just proved.

Corollary 12.4 *A Dedekind domain which is a UFD is a PID.*

PROOF Let D be a Dedekind domain and I an ideal in D. If $I = \{0\}$ or $I = D$, then I is clearly principal, so let us suppose that this is not the case. From Theorem 12.2, I divides a nonzero principal ideal (a). As D is a UFD, we may write a as a product of irreducible elements: $a = p_1 \cdots p_s$. Each principal ideal (p_i) is a prime ideal and we have

$$(a) = (p_1)\cdots(p_s).$$

As I divides (a), there exists an ideal C such that

$$IC = (p_1)\cdots(p_s).$$

By Theorem 12.3 there exist $(p_{i_1}), \ldots, (p_{i_u})$ such that

$$I = (p_{i_1})\cdots(p_{i_u}) = (p_{i_1}\cdots p_{i_u}).$$

We have shown that I is a principal ideal. □

Remark We might be tempted to think that the ideals in a Dedekind domain form a UFD. However, the ideals in a nontrivial ring do not form an additive group: If I is a nonzero ideal, then $I + I = I$, which would not be possible if I had an additive inverse. We can only affirm that the ideals form a monoid.

12.3 Ideal classes

If R is an integral domain, then we may define a relation $\mathcal{R}$ on the nonzero ideals in R as follows: $I\mathcal{R}J$ if and only if there exist elements $\alpha, \beta \in R \setminus \{0\}$ such that $\alpha I = \beta J$. It is easy to see that $\mathcal{R}$ is an equivalence relation, so we will write $\sim$ for $\mathcal{R}$. We define a multiplication on the equivalence classes in an obvious way:

$$[I][J] = [IJ].$$

This multiplication is well-defined, since $I \sim I'$ and $J \sim J'$ implies that $IJ \sim I'J'$. We will show that the equivalence classes with this multiplication form a monoid and, in the case of a Dedekind domain, a group.

Lemma 12.3 *If R is an integral domain, I an ideal in R and there exists $\alpha \neq 0$ such that αI is principal, then I is principal.*

PROOF Let $\alpha I = (a)$. Then there exists $u \in I$ such that $a = \alpha u$. If $s \in I$, then we may find $v \in R$ such that $\alpha s = va$. We have

$$\alpha s = v\alpha u \Longrightarrow \alpha(s - vu) = 0 \Longrightarrow s = vu.$$

It follows that $I \subset (u)$. As $u \in I$, $(u) \subset I$ and so we have $I = (u)$. □

We now consider a particular equivalence class.

Proposition 12.1 *If R is an integral domain, then the nonzero principal ideals form an equivalence class.*

PROOF Let I be a nonzero principal ideal: $I = (a)$. If J is also a nonzero principal ideal and $J = (b)$, then

$$b(a) = a(b) \Longrightarrow I \sim J,$$

hence $J \in [I]$.

Now suppose that J is a nonzero ideal in R and $I \sim J$: there exist $\alpha, \beta \in R \setminus \{0\}$ such that $\alpha I = \beta J$. If $I = (a)$, then $\beta J = \alpha(a) = (\alpha a)$. From Lemma 12.3, J is principal. Therefore the class of I is composed of the nonzero principal ideals in R. □

We will note the set of equivalence classes $Cl(R)$. Clearly, $Cl(R)$ contains a unique element if and only if R is a PID.

Theorem 12.4 *$Cl(R)$ is a monoid. If R is a Dedekind domain, then $Cl(R)$ is a group.*

PROOF It is clear that the multiplication which we have defined is associative. We claim that the class of nonzero principal ideals, which we note E, is a neutral element. To see this, let (a) be a nonzero principal ideal and I any nonzero ideal. Then $(a)I = aI$. As $aI = 1aI$, $I \sim aI$ and it follows that $E[I] = [I]$. Thus $Cl(R)$ is a monoid.

Now suppose that R is a Dedekind domain and I a nonzero ideal. From Theorem 12.2 we know that there is a nonzero ideal J such that IJ is principal. Moreover, $IJ \neq \{0\}$, since $I \neq \{0\}$ and $J \neq \{0\}$. Hence the class $[I]$ has an inverse $[J]$. Therefore $Cl(R)$ is a group. □

The group of classes $Cl(D)$ of a Dedekind domain D is called the *ideal class group* of D.

12.4 hcf and lcm

We have seen above that division of ideals in a Dedekind domain may be characterized by a simple inclusion condition: $I|J \Longleftrightarrow I \supset J$. Keeping this in mind, we will now study in more detail the division of ideals in a Dedekind domain.

We define a *highest common factor* (hcf) and a *lowest common multiple* (lcm) of two ideals in the same way as we do in an integral domain. Let I and J be nontrivial, proper ideals in a Dedekind domain D. An ideal U is an hcf of I and J if

- $U|I$, $U|J$;
- $X|I, X|J \Longrightarrow X|U$.

An ideal V is an lcm of I and J if

- $I|V,\ J|V$;
- $I|Y, J|Y \Longrightarrow V|Y$.

Exercise 12.2 *Show that the hcf and the lcm are unique; hence we can speak of* <u>*the*</u> *hcf and* <u>*the*</u> *lcm of two ideals.*

Another point is worth making. We say that two elements in an integral domain are coprime if they have 1 as an hcf. If R is a PID and x and y are coprime, then there exist $a, b \in R$ such that $ax + by = 1$. This is equivalent to saying that $(x) + (y) = R$. This suggests the following generalization: if I and J are ideals in ring R, then we say that these ideals are *coprime*, if $I + J = R$.

Proposition 12.2 *If I and J are nontrivial, proper ideals in a Dedekind domain D, then*

$$hcf(I, J) = I + J \qquad \text{and} \qquad lcm(I, J) = I \cap J.$$

PROOF First the hcf. We have

$$I + J \supset I, J \Longrightarrow I + J|I, I + J|J$$

and

$$X|I, X|J \Longrightarrow X \supset I, X \supset J \Longrightarrow X \supset I + J \Longrightarrow X|I + J,$$

hence $\text{hcf}(I, J) = I + J$.

Now we consider the lcm. We have

$$I, J \supset I \cap J \Longrightarrow I|I \cap J, J|I \cap J$$

and

$$I|Y, J|Y \Longrightarrow I \supset Y, J \supset Y \Longrightarrow I \cap J \supset Y \Longrightarrow I \cap J|Y,$$

hence $\text{lcm}(I, J) = I \cap J$. □

The following characterizations of the hcf and lcm are not difficult to establish:

Proposition 12.3 *Let D be a Dedekind domain and I, J nontrivial, proper ideals in D. We note $P_1, \dots P_s$ the prime ideals appearing in the factorization into products of prime ideals in either I or J:*

$$I = \prod_{i=1}^{s} P_i^{m_i} \qquad \text{and} \qquad J = \prod_{i=1}^{s} P_i^{n_i},$$

where the m_i and the n_i are elements of $\mathbf{N}$ and, for any given i, m_i and n_i are not both equal to 0. Then

$$hcf(I, J) = \prod_{i=1}^{s} P_i^{\min(m_i, n_i)} \qquad \text{and} \qquad lcm(I, J) = \prod_{i=1}^{s} P_i^{\max(m_i, n_i)}.$$

Corollary 12.5 *If I, J are nontrivial, proper ideals in a Dedekind domain D, then*

$$hcf(I, J)lcm(I, J) = IJ.$$

Remark Propositions 12.2 and 12.3 can be naturally generalized to a finite number of ideals.

The following result is also useful:

Proposition 12.4 *In a commutative ring R, if the ideals I and J are coprime, then $I \cap J = IJ$. If R is a Dedekind domain and I, J are nontrivial, proper ideals, then the converse is also true.*

PROOF Let R be a commutative ring with ideals I and J. If $I + J = R$, then

$$I \cap J = (I \cap J)R = (I \cap J)(I + J) = (I \cap J)I + (I \cap J)J \subset JI + IJ = IJ.$$

Clearly $IJ \subset I \cap J$, so $I \cap J = IJ$.

Now suppose that R is a Dedekind domain. Then

$$IJ = I \cap J \Longrightarrow (I + J)(IJ) = (I + J)(I \cap J) = IJ,$$

because $I + J = \mathrm{hcf}(I, J)$ and $I \cap J = \mathrm{lcm}(I, J)$. If $I + J$ is a nontrivial, proper ideal, then we have a contradiction to the unique factorization of ideals. On the other hand, clearly $I + J \neq \{0\}$, so $I + J = D$, i.e., I and J are coprime. □

We may slightly strengthen Theorem 12.2. To do so we need a preliminary result.

Lemma 12.4 *Let I be a nonzero ideal in a Dedekind domain D. If P is a prime ideal, then $PI \subset I$ and the inclusion is strict.*

PROOF The inclusion is clear. If $I = D$, then the strict inclusion is clear. On the other hand, if $I \neq D$, if the inclusion is not strict, then we have a contradiction to the unicity of the factorization of ideals, so the inclusion must be strict. □

Theorem 12.5 *If I and Q are nonzero ideals in a Dedekind domain D, then there exists an ideal J of D such that IJ is principal and J and Q are coprime.*

PROOF If $I = D$, then it is sufficient to take $J = \{0\}$. On the other hand, if $Q = D$, then, from Theorem 12.2, there is a nonzero ideal J such that IJ is principal; as $J + D = D$, J and D are coprime. Let us now suppose that $I \neq D$ and $Q \neq D$.

Let $P_1, \ldots, P_s$ be the prime ideals which occur in the decomposition into prime ideals of I and Q. Then

$$I = P_1^{m_1} \cdots P_s^{m_s},$$

with $m_i \geq 0$,for $i = 1, \ldots, s$. If $m_i = 0$, then $P_i^{m_i} = D$. From Lemma 12.4, for each $i \in \{1, \ldots, s\}$, we can find $y_i \in P_i^{m_i} \setminus P_i^{m_i+1}$. Also, if $i \neq j$, then from Proposition 12.3

$$\mathrm{hcf}(P_i^{i+1}, P_j^{j+1}) = P_i^0 P_j^0 = D,$$

so P_i^{i+1} and P_j^{j+1} are coprime. From the Chinese remainder theorem (Theorem F.1), we see that there exists $x \in D$ such that $x \equiv y_i \mod P_i^{m_i+1}$, for each $i \in \{1, \ldots, s\}$. Thus, for all $i \in \{1, \ldots, s\}$,

$$x \in P_i^{m_i},\ x \notin P_i^{m_i+1} \Longrightarrow P_i^{m_i} | (x),\ P_i^{m_i+1} \nmid (x).$$

This implies that $I|(x)$ and so there exists an ideal J in D such that $IJ = (x)$. J and Q are coprime, since no prime ideal divides both J and Q. Indeed, any prime ideal dividing both J and Q is a P_i for some $i \in \{1, \ldots, s\}$. This contradicts the fact that $x \notin P_i^{m_i+1}$. □

Dedekind domains are 'almost principal', i.e., their ideals are generated by at most two elements.

Corollary 12.6 *If I is an ideal in a Dedekind domain D, then there exist $x, y \in I$ such that $I = (x, y)$.*

PROOF From Theorem 12.2 we know that there is a nonzero ideal Q in D such that IQ is principal: there exists $y \in D$ such that $IQ = (y)$. In addition, Theorem 12.5 ensures the existence of an ideal J in D such that IJ is principal and J and Q coprime: $IJ = (x)$, for some $x \in IJ$. We have

$$(x, y) = (x) + (y) = IJ + IQ = I(J + Q) = ID = I,$$

the result we were looking for. □

We have seen above in Corollary12.4 that a Dedekind domain which is a UFD is a PID. We can use Theorem 12.5 to obtain another criterion for a Dedekind domain to be a PID.

Corollary 12.7 *A Dedekind domain with only a finite number of prime ideals is a PID.*

PROOF Let D be a Dedekind domain with only a finite number of prime ideals. We write Q for the product of these ideals. If I is a nonzero ideal in D, then from Theorem 12.5 there is an ideal J such that IJ is a principal ideal (a), with J and Q coprime. As J and Q are coprime, we must have $J = D$. Hence

$$(a) = IJ = ID = I,$$

therefore I is principal. □

12.5 Fractional ideals

If R is a commutative ring, then by definition R is an R-module and an ideal of R is an R-submodule. In an integral domain we may extend the notion of ideal. This proves to be particularly useful in Dedekind domains. Let R be an integral domain with field of fractions K. If J is an R-submodule of K such that $rJ \subset R$, for some $r \in R^*$, then we say that J is a *fractional ideal*. We call r a *denominator* of J. Setting $r = 1$, we see that an ordinary ideal is a fractional ideal, so the notion of fractional ideal does indeed generalize that of ideal. When handling fractional ideals we sometimes refer to ordinary ideals as *integral ideals* to distinguish them.

Example $\frac{2}{3}\mathbf{Z}$ is a fractional ideal of $\mathbf{Z}$, but not an integral ideal.

The ring R is a fractional ideal, but in general its field of fractions K is not. If K is a fractional ideal, then there exists $r \in R^*$ such that $rK \subset R$. As r is inversible in K, we have $K = \frac{1}{r}R$. Now, $\frac{1}{r^2} \in K$, so $\frac{1}{r^2} = \frac{1}{r}s$, with $s \in R$. This implies that $s = \frac{1}{r}$, i.e., $\frac{1}{r} \in R$, and so $K = R$. We will suppose that $K \neq R$.

We define the addition and multiplication of fractional ideals in the same way as we do for ideals, i.e.,

$$I + J = \{x + y : x \in I, y \in J\} \quad \text{and} \quad I \cdot J = \{\sum_{i=1}^{n} x_i y_i : n \geq 1, x_i \in I, y_i \in J\}.$$

As in general for multiplication, we write IJ for $I \cdot J$.

Proposition 12.5 *If I and J are fractional ideals with denominators r and s respectively, then $I \cap J$, $I + J$ and IJ are fractional ideals with respective denominators r or s, rs and rs.*

PROOF There is no difficulty in seeing that $I \cap J$, $I + J$ and IJ are R-submodules of K. In addition,

$$r(I \cap J) \subset rI \subset R, \quad rs(I + J) \subset rI + sJ \subset R \quad \text{and} \quad rs(IJ) = (rI)(sJ) \subset R.$$

This ends the proof. □

Proposition 12.6 *Let R be an integral domain. The nonzero fractional ideals of R are the expressions of the form $J = \alpha I$, where I is a nonzero ideal of R and $\alpha \in K^*$.*

PROOF Let $J = \alpha I$, where I is a nonzero ideal of R and $\alpha \in K^*$. If $\alpha = \frac{a}{b}$, with $a, b \in R^*$, then $bJ = aI \subset I \subset R$, therefore J is a nonzero fractional ideal of R.

Now let J be a nonzero fractional ideal of R. There exists $r \in R^*$ such that $rJ \subset R$. Moreover, $J = \frac{1}{r}(rJ)$ and rJ is an ideal of R. As $\frac{1}{r} \in K^*$, J has the required form. □

Remark An R-submodule is not necessarily a fractional ideal. For example, $\mathbf{Z}[\frac{1}{2}]$ is a $\mathbf{Z}$-submodule contained in $\mathbf{Q}$, but is not a fractional ideal of $\mathbf{Z}$. (There is no positive integer n such that $n\mathbf{Z}[\frac{1}{2}] \subset \mathbf{Z}$).

Exercise 12.3 *Let R be an integral domain. Prove the following statements:*

- **a.** *If J is a fractional ideal of R and r a denominator, then rJ is an integral ideal of R.*
- **b.** *If a fractional ideal J of a ring R is contained in R, then J is an integral ideal of R.*

The next result enables us to characterize fractional ideals in the case where the ring R is noetherian.

Proposition 12.7 *Let R be a noetherian domain. The nonzero fractional ideals of R are the nonzero finitely generated R-submodules of K, where K is the field of fractions of R.*

PROOF Let J be a nonzero finitely generated R-submodule of K:

$$J = Rx_1 + \cdots + Rx_n,$$

where $x_i = \frac{a_i}{b_i}$, with $a_i \in R$ and $b_i \in R^*$. If we set $b = b_1 \cdots b_n$, then $bJ \subset R$ and so J is a nonzero fractional ideal of R.

Reciprocally, let J be a nonzero fractional ideal of R and r a denominator of J. Then $J \subset \frac{1}{r}R$. As an R-module, $\frac{1}{r}R$ is isomorphic to R, hence $\frac{1}{r}R$ is a noetherian R-module. Since J is a submodule of $\frac{1}{r}R$, J is a finitely generated R-module. □

The product of two nonzero fractional ideals is a nonzero fractional ideal and the multiplication is associative. If J is a fractional ideal, then, using the fact that J is an R-module, we have

$$RJ \subset J = 1J \subset RJ,$$

and so R is an identity for the multiplication. It follows that the nonzero fractional ideals form a semigroup. In the case of a Dedekind domain the nonzero fractional ideals form a group, as we will presently see.

Proposition 12.8 *Every nonzero fractional ideal in a Dedekind domain D has an inverse in the set of fractional ideals. More explicitly, if I is a nonzero fractional ideal of D and $J = \{x \in K, xI \subset D\}$, then J is a fractional ideal and $IJ = D$.*

PROOF Let us first suppose that I is a nonzero integral ideal. It is easy to see that J is a nonzero D-submodule of K, the field of fractions of D. If r is a nonzero element of I (and so of R) and $x \in J$, then $rx \in D$, so there exists $r \in D^*$ such that $rJ \subset D$. Thus J is a nonzero fractional ideal.

Let $a \in I$, with $a \neq 0$, and $J_a = \{b \in D : bI \subset (a)\}$. The proof of Theorem 12.2 shows that $IJ_a = (a)$. In addition, $\frac{1}{a}J_a = J$. Indeed, $\frac{1}{a}J_a$ is clearly included in J and every $c \in J$ can be written $c = \frac{1}{a}ca$ and $ca \in J_a$. Thus

$$IJ = I\frac{1}{a}J_a = \frac{1}{a}(a) = D,$$

therefore J is an inverse of I.

Now let us consider the more general case, i.e, I is a nonzero fractional ideal, which is not necessarily integral. There exists a nonzero integral ideal A and $\alpha \in K^*$, where K is the field of fractions of D, such that $I = \alpha A$ (Proposition 12.6). If we set $B = \alpha^{-1}A^{-1}$, then B is a fractional ideal and $IB = D$, so I has an inverse, namely B. It remains to show that $B = J = \{x \in K, xI \subset D\}$. From the first part of the proof we know that $A^{-1} = \{x \in K : xA \subset D\}$. If $u \in I^{-1}$, then $u = \alpha^{-1}x$, where $xA \subset D$, which implies that $u\alpha A \subset D$ and it follows that $u \in J$. We have shown that $I^{-1} \subset J$. To complete the proof, we show that $J \subset I^{-1}$. If $u \in J$, then $uI \subset D$, i.e., $u\alpha A \subset D$. This implies that $u\alpha \in A^{-1}$ and so $u \in \alpha^{-1}A^{-1} = I^{-1}$. Therefore $J \subset I^{-1}$. □

Corollary 12.8 *The nonzero fractional ideals of a Dedekind domain form an abelian group.*

In fact, Proposition 12.8 has a converse. If R be an integral domain, then the nonzero fractional ideals form a monoid, with identity R. The nonzero invertible fractional ideals form an abelian group. If R is a Dedekind domain, then every nonzero fractional ideal is invertible, hence the result of Corollary 12.8. However, the converse is also true.

Proposition 12.9 *If R is an integral domain such that every nonzero fractional ideal is invertible, then R is a Dedekind domain.*

PROOF We must show that R is noetherian, that prime ideals are maximal and that R is normal. Let K be the field of fractions of R.

Let I be a nonzero (integral) ideal of R. Then I is invertible and $J = \{x \in K : xI \subset R\}$ is the inverse of I. (We can easily verify that $IJ = R$ and in a monoid, if an element has an inverse, then this inverse is unique.)

As $IJ = R$, there exist $a_1, \ldots, a_n \in I$ and $b_1, \ldots, b_n \in J$ such that $a_1b_1 + \cdots + a_nb_n = 1$. If $a \in I$, then

$$a = a_1(b_1a) + \cdots + a_n(b_na) \in (a_1, \ldots, a_n),$$

because $b_ia \in R$, for $i = 1, \ldots, n$. It follows that $I \subset (a_1, \ldots, a_n)$. Clearly $(a_1, \ldots, a_n) \subset I$, so we have equality. As every ideal is finitely generated, R is noetherian.

Let P be a prime ideal in R and M a maximal ideal containing P. As M is invertible, there exists an ideal J such that $P = JM$. ($J = M^{-1}P \subset R$, because $P \subset M$; from Exercise 12.6 the fractional ideal J is an integral ideal.) Since P is a prime ideal, we have $J \subset P$ or $M \subset P$. (If $J \not\subset P$ and $M \not\subset P$, then there exist $x \in J \setminus P$ and $y \in M \setminus P$; but $xy \in JM = P$, a contradiction.) If $J \subset P$, then $P = JM \subset PM$; multiplying by P^{-1}, we obtain $R \subset M$, a contradiction. Therefore $M \subset P$ and it follows that $M = P$. Hence P is a maximal ideal.

It remains to show that R is a normal domain. Let $x \in K$ be integral over R. Then there exist elements $c_0, c_1, \ldots, c_{n-1} \in R$ such that $x^n = c_0 + c_1x + \cdots c_{n-1}x^{n-1}$. Let

$$A = \{y \in K : y = \sum_{i=0}^{n-1} u_i x^i, u_i \in R\}.$$

A is clearly an R-module. The element $x = \frac{r}{s}$, with $r \in R$ and $s \in R^*$, so $s^{n-1}A$ is a subset of R. Hence A is a fractional ideal of R. Since $x^n \in A$, we have $xA \subset A$. By hypothesis A is invertible, so multiplying by A^{-1} we obtain $x \in R$. Therefore R is integrally closed in K, i.e., R is a normal domain. □

Remark Propositions 12.8 and 12.9 provide us with a useful characterization of Dedekind domains, which will use further on.

Decomposition of fractional ideals

We have seen that in a Dedekind domain D an ideal $I \neq \{0\}, D$ can be written in a unique way as a product of prime ideals. We may extend this result to fractional ideals.

Theorem 12.6 *If J is a fractional ideal in a Dedekind domain and $J \neq \{0\}, D$, then*

$$J = P_1^{n_1} \cdots P^{n_r},$$

where the P_i are distinct nonzero prime ideals of D and the n_i integers (possibly negative). This decomposition is unique.

PROOF We first observe that such a decomposition exists. As J is a fractional ideal there is an $r \in D^*$ such that $rJ \subset D$. Clearly rJ is a nonzero ideal of D. There are two cases to consider: 1. r is a unit of D, 2. r is not a unit of D.

Case 1. If r is a unit of R, then J is subset of D, hence an ideal of D (Exercise 12.6). By hypothesis, $J \neq D$, so we have the required decomposition.

Case 2. If r is not a unit, then rD is a nonzero proper ideal in D and so there exists a decomposition

$$rD = P_1^{n_1} \cdots P_n^{n_r},$$

where the P_i are distinct prime ideals and the n_i positive integers. From Proposition 12.8 each P_i has an inverse in the set of fractional ideals. Consequently, rD has an inverse in the set of fractional ideals:

$$(rD)^{-1} = P_1^{-n_1} \cdots P_r^{-n_r}. \tag{12.1}$$

As rJ is an integral ideal of D (Exercise 12.6), we have $DrJ = rJ$, thus

$$r^{-1}DrJ = J \Longrightarrow (rD)^{-1}rJ = J.$$

If $rJ = D$, then $(rD)^{-1} = J$ and, using Equation (12.1), we obtain a decomposition of J of the required type. On the other hand, if $rJ \neq D$, then rJ is a nonzero proper ideal of D and it follows that J has a decomposition of the required type.

We now consider the unicity of the decomposition. If

$$P_1^{m_1}\cdots P_r^{m_r} = Q_1^{n_1}\cdots Q_s^{n_s}$$

and all the exponents are positive, then there is no difficulty as we have an ideal in D. The P_i and Q_j are the same with the same positive powers. Suppose now that there are negative powers in the expression. If, for example, $n_s < 0$, then we may multiply both sides of the expression by $Q_s^{-n_1}$. If we do this for all prime ideals with negative powers, then we obtain an expression with positive powers of the P_i and the Q_j on both sides. If we now have a Q_j on the lefthand side, then we must have a P_i on the righthand side such that $Q_j = P_i$ and $-n_j = -m_i$, which implies that $n_j = m_i$. If a Q_j remains on the righthand side, then there must be a P_i on the lefthand side such that $Q_j = P_i$ and $n_j = m_i$. We may use an analagous argument for the P_i and so obtain the uniqueness of the decomposition. □

We may distinguish the integral ideals among the fractional ideals in a simple way, as the next result shows.

Corollary 12.9 *A nonzero fractional ideal J of a Dedekind domain D, such that $J \neq D$, is an integral ideal if and only if the powers of all the prime ideals in its decomposition are positive.*

PROOF If all the powers are positive, then we have a product of ideals, which is an ideal.

Suppose now that at least one power m_i is negative:

$$J = P_1^{m_1}\cdots P_i^{m_i}\cdots P_r^{m_r},$$

with $m_i < 0$. If J is an ideal, then we may write

$$J = Q_1^{n_1}\cdots Q_s^{n_s},$$

where the Q_j are ideals and $n_j > 0$, for all j. Given the uniqueness of the factorization of I, we must have $P_i = Q_j$ for some j, and $m_i = n_j$. However, this is impossible, because

$$P_i^{m_i} = Q_j^{n_j} \Longrightarrow P_i^{n_j - m_i} = D$$

and $n_j - m_i \geq 2$ and P_i is a proper ideal. Hence, if a power of a prime ideal in the decomposition is negative, J is not an ideal. □

Further properties of fractional ideals

Certain properties of ideals may be generalized to fractional ideals. First we consider divisibility. Let I and J be fractional ideals in a Dedekind domain D. We say that I divides J if there exists an integral ideal H such that $IH = J$.

Exercise 12.4 *Show that division defines an order relation on fractional ideals.*

Exercise 12.5 *Show that division of fractional ideals is equivalent to inclusion, i.e., if I and J are fractional ideals of a Dedekind domain D, then I divides J if and only if I contains J.*

It is also interesting to notice that inclusion is reversed by inversion:

Exercise 12.6 *Let I and J be nonzero (integral) ideals in a Dedekind domain D. Show that if $I \subset J$ then $J^{-1} \subset I^{-1}$. Deduce that this is also the case for any pair of nonzero fractional ideals.*

If $R \subset S$ are commutative rings and I an ideal in R, then we define an ideal SI in S, *the extension of I in S* , by letting SI be the collection of finite sums of the form $\sum_{i=1}^{m} s_i x_i$, with $s_i \in S$ and $x_i \in I$. This is the smallest ideal in S containing I (or the ideal in S generated by I). We may generalize this idea to fractional ideals.

Let C be Dedekind domain and D a commutative ring containing D. We note K the field of fractions of C. If $J \subset K$ is a fractional ideal of D, then we write DJ for the collection of finite sums of the form $\sum_{i=1}^{m} d_i x_i$, with $d_i \in D$ and $x_i \in J$. We claim that, if D is an integral domain, then DJ is a fractional ideal of D. Indeed, DJ is clearly a D-module of the field of fractions of D and any denominator of J is a denominator of DJ. This fractional ideal is the smallest fractional ideal of D containing J.

If $R \subset S$ are commutative rings and I an ideal in R, then it is not necessarily the case that $SI \cap R = I$. For example, if $R = \mathbf{Z}$, $S = \mathbf{Q}$ and $I = (2)$, then $SI = S$, because $\mathbf{Q}$ is the only nonzero ideal in $\mathbf{Q}$. As $\mathbf{Q} \cap \mathbf{Z} = \mathbf{Z} \neq (2)$, in this case $SI \cap R \neq I$. This example also shows that, even if R and S are Dedekind domains, it may not be true that $SI \cap R = I$. The following result provides a framework where this property holds.

Theorem 12.7 *Let C be Dedekind domain, D a commutative ring containing C and K the field of fractions of C. In addition, we suppose that $C \cap D \subset K$.*

- **a.** *If J is a fractional ideal of C, then $DJ \cap K = J$;*
- **b.** *If I is an (integral) ideal of C, then $DI \cap C = I$.*

PROOF **a.** To begin with, $DJ \cap K$ is always a fractional ideal of C. Indeed, it is clearly a C-submodule of K and any denominator of J is a denominator of $DJ \cap K$, because $D \cap K \subset C$. If $J = \{0\}$, then the result is evident, so suppose that this is not the case. Proposition 12.8 ensures that J has an inverse. Then

$$D = DC = D(JJ^{-1}) = (DJ)(DJ^{-1}),$$

hence

$$C \supset D \cap K = \big((DJ)(DJ^{-1})\big) \cap K \supset (DJ \cap K)(DJ^{-1} \cap K).$$

Since $DJ \cap K$ is a fractional ideal of C, from Proposition 12.8 again, $DJ \cap K$ has an inverse. We have

$$C = (DJ \cap K)(DJ \cap K)^{-1} \Longrightarrow (DJ \cap K)(DJ \cap K)^{-1} \supset (DJ \cap K)(DJ \cap^{-1} \cap K).$$

Now, using Exercise 12.5, we obtain

$$(DJ \cap K)^{-1} \supset DJ^{-1} \cap K.$$

Since $J \subset DJ \cap K$, from Exercise 12.6,

$$D(J^{-1}) \cap K \supset J^{-1} \supset (DJ \cap K)^{-1}$$

and so

$$(DJ \cap K)^{-1} = DJ^{-1} \cap K = J^{-1} \Longrightarrow DJ \cap K = J,$$

as required.

b. Let I be an (integral) ideal in C. Since I is also a fractional ideal, the part **a.** ensures that

$$DI \cap K = I.$$

Taking the intersection with D on both sides leads to

$$DI \cap (K \cap D) = I.$$

Clearly $C \subset K \cap D$ and we have seen in part **a.** that $K \cap D \subset C$, so $K \cap D = C$ and it follows that $DI \cap C = I$. □

Example If D is integral over C, then $D \cap K$ is included in the integral closure of C in K. As C is a normal domain, its integral closure in K, its field of fractions, is C itself. Thus $D \cap K \subset C$ and so Theorem 12.7 applies.

If R is an integral domain, then we may extend the equivalence relation defined in Section 12.3 to fractional ideals. In the same way as for the nonzero integral ideals, we define a relation $\mathcal{R}$ on the nonzero fractional ideals of R as follows: $I\mathcal{R}J$ if and only if there exist elements $\alpha, \beta \in R \setminus \{0\}$ such that $\alpha I = \beta J$. There is no difficulty in seeing that $\mathcal{R}$ is an equivalence relation and so we write $\sim$ for $\mathcal{R}$.

Proposition 12.10 *If R is a Dedekind domain and I is a nonzero fractional ideal in R, then there is a nonzero integral ideal J such that $I \sim J$.*

PROOF Let I be a nonzero fractional ideal. From the decomposition of fractional ideals we obtain the existence of integral ideals B and C such that $I = \frac{B}{C}$, with C nontrivial. We take $t \in C$, with $t \neq 0$. Then $C \supset Rt \Longrightarrow C|Rt$. Hence there exists an integral ideal $E \subset R$ such that $CE = Rt$. Therefore we have

$$(Rt)I = Rt\frac{B}{C} = \frac{CEB}{C} = EB \Longrightarrow tI = 1EB,$$

hence $I \sim EB$. □

Remark From the above proposition, every equivalence class contains an integral ideal.

12.6 Localization in a Dedekind domain

Before studying localization in a Dedekind domain, we will first revise (or introduce, for those not familiar with localization) the basic notions of localization in a commutative ring.

Let R be a commutative ring. A subset U of R is said to be multiplicative if

- $1 \in U$;
- $x, y \in U \Longrightarrow xy \in U$.

We define a relation $\mathcal{R}$ on $R \times U$ by

$$(r, u)\mathcal{R}(r', u'),$$

if there exists $t \in U$ such that

$$t(ru' - r'u) = 0.$$

It is easy to show that $\mathcal{R}$ is an equivalence relation, so we will write $\sim$ for $\mathcal{R}$. Also, we write $\frac{r}{u}$ for the equivalence class of (r, u). In general, we write $U^{-1}R$ for the collection of equivalence classes.

We may give $U^{-1}R$ a ring structure:

$$\frac{r}{u} + \frac{r'}{u'} = \frac{ru' + r'u}{uu'} \qquad \text{and} \qquad \frac{r}{u} \cdot \frac{r'}{u'} = \frac{rr'}{uu'}.$$

It is easy to check that these operations are well-defined and that $U^{-1}R$ with these operations is a commutative ring. (The element $\frac{0}{1}$ (resp. $\frac{1}{1}$) is the identity for the addition (resp. multiplication).) The ring we have obtained is called the *localization of R with respect to U*. Clearly, the procedure we have used generalizes the construction of the rational numbers, with $R = \mathbf{Z}$ and $U = \mathbf{Z}^*$.

Exercise 12.7 *Show that $U^{-1}R$ is a zero ring if and only if $0 \in U$.*

From now on we suppose that $0 \notin U$.

Exercise 12.8 *Show that, if R is an integral domain and K its field of fractions, then the mapping*

$$\phi : U^{-1}R \longrightarrow K, \frac{r}{u} \longmapsto \frac{r}{u}$$

is an injective ring homomorphism. It follows that, if R is an integral domain, then so is $U^{-1}R$,

For a commutative ring R, the mapping

$$\pi : R \longrightarrow U^{-1}R, r \longmapsto \frac{r}{1}$$

is a ring homomorphism. In addition, if $u \in U$, then

$$\frac{u}{1} \cdot \frac{1}{u} = \frac{u}{u} = \frac{1}{1},$$

so the elements of $\pi(U)$ are invertible in $U^{-1}R$.

Exercise 12.9 *Show that the mapping π defined above is injective if and only if U has no zero divisors. It follows that, if R is an integral domain, then π is injective.*

If X is a subset of R, then we set

$$U^{-1}X = \{\frac{x}{u} : x \in X, u \in U\}.$$

Clearly, if I is an ideal in R, then $U^{-1}I$ is an ideal in $U^{-1}R$. It is not difficult to see that $U^{-1}I$ is the collection of all finite sums of the form $\sum_{i=1}^n y_i\pi(x_i)$, where $y_i \in U^{-1}R$ and $x_i \in I$, which is the ideal in $U^{-1}R$ generated by $\pi(I)$. If π is injective, then we may consider I as a subset of $U^{-1}R$ and we write $(U^{-1}R)I$ for $U^{-1}I$.

Remark We may extend this idea. Suppose that A and B are commutative rings with identity and $f : A \longrightarrow B$ a homomorphism. If I is an ideal in A, then $f(I)$ is not necessarily an ideal in B, even if f is injective (for example, the image of the ideal $2\mathbf{Z}$ in $\mathbf{Z}$ by inclusion of the ring of integers $\mathbf{Z}$ in the rationals $\mathbf{Q}$ is not an ideal in $\mathbf{Q}$.) However, if we let I^e be the collection of all finite sums of the form $\sum_{i=1}^n y_i f(x_i)$, where $y_i \in B$ and $x_i \in I$, then I^e is an ideal in B, called the *extension of I (under f) in B*. I^e is the ideal in B generated by $f(I)$. If f is an injection, then we write BI for I^e.

Lemma 12.5 *Let I be an ideal in R. Then $U^{-1}I$ is a proper ideal in $U^{-1}R$ if and only if $I \cap U = \emptyset$.*

PROOF If $u \in I \cap U$, then $\frac{1}{1} = \frac{u}{u} \in U^{-1}I$, so $U^{-1}I$ is not a proper ideal. On the other hand, if $U^{-1}I = U^{-1}R$, then $\frac{1}{1} = \frac{r}{u}$, for some $r \in I$ and $u \in U$, hence there exists $t \in U$ such that

$$t(u - r) = 0 \Longrightarrow tu = tr.$$

However, $tu \in U$, because $t, u \in U$, and $tr \in I$, because $r \in I$, so $I \cap U \neq \emptyset$. $\square$

The next result is elementary, but important.

Proposition 12.11 *If I and J are ideals in R, then*

- **a.** $U^{-1}(I + J) = U^{-1}I + U^{-1}J$;
- **b.** $U^{-1}(I \cap J) = U^{-1}I \cap U^{-1}J$;
- **c.** $U^{-1}(IJ) = (U^{-1}I)(U^{-1}J)$.

PROOF It is clear that in all three cases the lefthand side is contained in the righthand side, so we only need to show that the righthand side is included in the lefthand side.

a. If $\frac{r}{u} \in U^{-1}I$ and $\frac{r'}{u'} \in U^{-1}J$, then

$$\frac{r}{u} + \frac{r'}{u'} = \frac{ru' + r'u}{uu'} \in U^{-1}(I + J),$$

because $ru' \in I$ and $r'u \in J$. Thus

$$U^{-1}I + U^{-1}J \subset U^{-1}(I + J).$$

b. If $\frac{r}{u} \in U^{-1}I \cap U^{-1}J$, then there exist $r_1 \in I$, $u_1 \in U$ and $t_1 \in U$ such that

$$t_1(ru_1 - r_1u) = 0 \Longrightarrow t_1ru_1 = t_1r_1u \in I$$

and $r_2 \in J$, $u_2 \in U$ and $t_2 \in U$ such that

$$t_2(ru_2 - r_2u) = 0 \Longrightarrow t_2ru_2 = t_2r_2u \in J.$$

It follows that

$$t_1t_2ru_1u_2 \in I \cap J.$$

Thus there exists $\bar{u} \in U$ such that $r\bar{u} \in I \cap J$. Now $\frac{r}{u} = \frac{r\bar{u}}{u\bar{u}} \in U^{-1}(I \cap J)$, so

$$U^{-1}I \cap U^{-1}J \subset U^{-1}(I \cap J).$$

c. Let $\frac{r_1}{u_1}, \ldots, \frac{r_n}{u_n} \in U^{-1}I$ and $\frac{r'_1}{u'_1}, \ldots, \frac{r'_n}{u'_n} \in U^{-1}J$. Then

$$\frac{r_1}{u_1}\frac{r'_1}{u'_1} + \cdots + \frac{r_n}{u_n}\frac{r'_n}{u'_n} = \frac{r}{u_1u'_1 \cdots u_nu'_n},$$

where $r \in IJ$, so

$$(U^{-1}I)(U^{-1}J) \subset U^{-1}(IJ).$$

This ends the proof. $\square$

Above we introduced the mapping

$$\pi : R \longrightarrow U^{-1}R, r \longmapsto \frac{r}{1}.$$

As π is a ring homomorphism, if J is an ideal in $U^{-1}R$, then $\pi^{-1}(J)$ is an ideal in R. Also, we have seen that, if I is an ideal in R, then $U^{-1}I$ is an ideal in $U^{-1}R$. It follows that $U^{-1}\left(\pi^{-1}(J)\right)$ is an ideal in $U^{-1}R$. In fact, we have a stronger result.

Proposition 12.12 *If J is an ideal in $U^{-1}R$, then*

$$U^{-1}\left(\pi^{-1}(J)\right) = J.$$

PROOF If $\frac{r}{u} \in U^{-1}\left(\pi^{-1}(J)\right)$, then there exist $r' \in \pi^{-1}(J)$, $u' \in U$ and $t \in U$ such that

$$t(ru' - r'u) = 0 \Longrightarrow tru' = tur' \in \pi^{-1}(J) \Longrightarrow \frac{tru'}{1} \in J.$$

Therefore

$$\frac{r}{u} = \frac{tru'}{tuu'} = \frac{tru'}{1} \cdot \frac{1}{tuu'} \in J.$$

Hence

$$U^{-1}\left(\pi^{-1}(J)\right) \subset J.$$

To prove the converse, let us take $\frac{r}{u} \in J$. Then

$$\frac{r}{1} = \frac{r}{u} \cdot \frac{u}{1} \in J \Longrightarrow r \in \pi^{-1}(J) \Longrightarrow \frac{r}{u} \in U^{-1}\left(\pi^{-1}(J)\right).$$

Thus

$$J \subset U^{-1}\left(\pi^{-1}(J)\right).$$

This completes the proof. $\square$

Let us write $\mathcal{I}_R$ (resp. $\mathcal{I}_{U^{-1}R}$) for the collection of ideals in R (resp. $U^{-1}R$).

Proposition 12.13 *The mapping*

$$\pi^{-1} : \mathcal{I}_{U^{-1}R} \longrightarrow \mathcal{I}_R, J \longmapsto \pi^{-1}(J)$$

is injective.

PROOF If $\pi^{-1}(J_1) = \pi^{-1}(J_2)$, then from Proposition 12.12 we have

$$J_1 = U^{-1}\left(\pi^{-1}(J_1)\right) = U^{-1}\left(\pi^{-1}(J_2)\right) = J_2$$

and the injectivity follows. $\square$

The main object of this section is to show that the localization of a Dedekind domain is a Dedekind domain. We have already observed that the localization of an integral domain D is an integral domain (Exercise 12.8). We now show that the noetherian property carries over to a localization.

Proposition 12.14 *If R is a noetherian ring and U a multiplicative subset of R, then the localization $U^{-1}R$ is a noetherian ring.*

PROOF Let $\pi : R \longrightarrow U^{-1}R$ be the standard ring homomorphism taking r to $\frac{r}{1}$. We take an ascending sequence of ideals in $U^{-1}R$:

$$J_0 \subset J_1 \subset J_2 \subset \cdots$$

The inverse images under π of these ideals form an ascending chain of ideals in R:

$$\pi^{-1}(J_0) \subset \pi^{-1}(J_1) \subset \pi^{-1}(J_2) \subset \cdots$$

As R is noetherian, this chain eventually stabilizes, i.e., there exists k such that

$$\pi^{-1}(J_k) = \pi^{-1}(J_{k+1}) = \cdots$$

However, the mapping π^{-1} is injective (Proposition 12.13), so we have

$$J_k = J_{k+1} = \cdots$$

and it follows that $U^{-1}R$ is noetherian. □

Our next step is to show that

Proposition 12.15 *If R is a normal domain and $0 \notin U$, then $U^{-1}R$ is a normal domain.*

PROOF Let α be an element of the fraction field of $U^{-1}R$ which is integral over $U^{-1}R$, i.e., there exists a polynomial $f(X) = \sum_{i=0}^{k-1} a_i X^i + X^k \in U^{-1}R[X]$ such that $f(\alpha) = 0$. We take $u \in U$ such that u is a multiple of the denominators of the a_i, then $ua_0, ua_1, \ldots, ua_{k-1} \in R$. Setting $\bar{f}(X) = \sum_{i=0}^{k-1} u^{k-i} a_i X^i + X^k$, we have $\bar{f} \in R[X]$ and $\bar{f}(u\alpha) = 0$, so $u\alpha$ is integral over R. We may also choose u such that $u\alpha$ lies in the field of fractions of R. To see this, notice that

$$\alpha = \frac{r_1}{u_1} / \frac{r_2}{u_2} \Longrightarrow u\alpha = u\frac{r_1}{u_1} / \frac{r_2}{u_2} = \frac{ur_1u_2}{u_1} / r_2.$$

If we choose $u \in U$ to be a multiple of u_1, then $u\alpha$ belongs to the field of fractions of R. As R is a normal domain, $u\alpha \in R$, which implies that $\alpha = \frac{u\alpha}{u} \in U^{-1}R$. It follows that $U^{-1}R$ is a normal domain. □

To show that $U^{-1}D$ is a Dedekind domain if D is a Dedekind domain we must show that prime ideals are maximal. To do so, we first consider the mapping π^{-1} restricted to prime ideals.

Lemma 12.6 *If I is an ideal in R, then*

$$I \subset \pi^{-1}(U^{-1}I),$$

with equality if I is a prime ideal disjoint from U.

PROOF If $r \in I$, then $\frac{r}{1} \in U^{-1}I$, hence $r \in \pi^{-1}(U^{-1}I)$. This proves the first part of the lemma.

Now suppose that I is a prime ideal in R such that $I \cap U = \emptyset$ and let $r \in \pi^{-1}(U^{-1}I)$. Then $\pi(r) = \frac{r}{1} \in U^{-1}I$, so $\frac{r}{1} = \frac{r'}{u'}$, for some $r' \in I$ and $u' \in U$. Thus there exists $t \in U$ such that

$$t(ru' - r') = 0 \Longrightarrow tru' = tr',$$

with $tu' \notin I$, because $U \cap I = \emptyset$. (If $tu' \in I$, then $t \in I$ or $u' \in I$, a contradiction.) Since $tr' \in I$, also $tru' \in I$. Given that $tu' \notin I$ and I is prime, we must have $r \in I$. Hence $\pi^{-1}(U^{-1}I) \subset I$. □

We will write $\mathcal{P}_{U^{-1}R}$ for the set of prime ideals in $U^{-1}R$ and $\mathcal{P}_{R\setminus U}$ for the set of prime ideals in R disjoint from U.

Theorem 12.8 *The mapping π^{-1} restricted to $\mathcal{P}_{U^{-1}R}$ defines a bijection onto $\mathcal{P}_{R\setminus U}$.*

PROOF We have already observed that, if J is an ideal in $U^{-1}R$, then $\pi^{-1}(J)$ is an ideal in R and that the mapping π^{-1} is injective (Proposition 12.13). It is elementary to show that $\pi^{-1}(J)$ is prime when J is prime. We must show that $\pi^{-1}(J) \cap U = \emptyset$. From Lemma 12.5 and Proposition 12.12

$$\pi^{-1}(J) \cap U = \emptyset \Longleftrightarrow U^{-1}\left(\pi^{-1}(J)\right) \neq U^{-1}R \Longleftrightarrow J \neq U^{-1}R.$$

Since J is a prime ideal of $U^{-1}R$, $J \neq U^{-1}R$, so $\pi^{-1}(J) \cap U = \emptyset$, as desired. We have shown that the image of π^{-1} restricted to $\mathcal{P}_{U^{-1}R}$ lies in $\mathcal{P}_{R\setminus U}$.

To finish we only need to show that $\pi^{-1}(\mathcal{P}_{U^{-1}R}) = \mathcal{P}_{R\setminus U}$. Let $I \in \mathcal{P}_{R\setminus U}$. From Lemma 12.6 we have

$$I = \pi^{-1}(U^{-1}I).$$

As I is a prime ideal in R and $I \cap U = \emptyset$, $U^{-1}I$ is a prime ideal in $U^{-1}R$, so π^{-1} restricted to $\mathcal{P}_{U^{-1}R}$ is surjective. □

Corollary 12.10 *If R is a commutative ring in which every nonzero prime ideal is maximal, then this is also the case for the localization $U^{-1}R$.*

PROOF Let J be a nonzero prime ideal in $U^{-1}R$ which is not maximal. Then there exists a nonzero prime ideal J' in $U^{-1}R$ which properly contains J. From the previous theorem, both $\pi^{-1}(J)$ and $\pi^{-1}(J')$ are nonzero prime ideals and $\pi^{-1}(J)$ is properly contained in $\pi^{-1}(J')$. However, this is a contradiction, because $\pi^{-1}(J)$ must be maximal. Hence J is maximal. □

Exercise 12.10 *If I is a prime ideal in R and $I \cap U \neq \emptyset$, show that $U^{-1}I$ is not a prime ideal in $U^{-1}R$.*

We are now in a position to establish the main theorem of this section.

Theorem 12.9 *If D is a Dedekind domain and U a multiplicative subset of D not containing 0, then $U^{-1}D$ is a Dedekind domain.*

PROOF We noticed in Exercise 12.11 that if the multiplicative set U has no zero divisors, then $U^{-1}R$ is an integral domain. Since D is an integral domain, so is $U^{-1}D$. Next, from Proposition 12.14, $U^{-1}D$ is a noetherian ring. Now, using Proposition 12.18, we see that $U^{-1}D$ is a normal domain. To finish we only need to show that every nonzero prime ideal in $U^{-1}D$ is maximal. However, this follows from Corollary 12.10. □

Suppose now that I is an ideal in D such that $I \neq \{0\}, D$ and $I = P_1^{e_1} \cdots P_r^{e_r}$ is the decomposition of I into prime ideals of D. In the Dedekind domain $D' = U^{-1}D$ the ideal J generated by I has a decomposition into prime ideals of D'. The following proposition gives us the form of this decomposition.

Proposition 12.16 *Let I be an ideal of the Dedekind domain D, such that $I \neq \{0\}, D$, and U a multiplicative subset of D not containing 0. If $I = P_1^{e_1} \cdots P_r^{e_r}$ is the decomposition of I into prime ideals of D and J the ideal in $D' = U^{-1}D$ generated by I, then the decomposition of J into prime ideals has the form*

$$J = \prod_{P_i \cap U = \emptyset} (D'P_i)^{e_i}.$$

PROOF First we have

$$J = D'I = D'\left(\prod_{i=1}^{r} P_i^{e_i}\right) = \prod_{i=1}^{r}(D'P_i)^{e_i}.$$

If $P_i \cap U \neq \emptyset$ then $D'P_i$ contains a unit, so $D'P_i = D'$. Thus

$$J = \prod_{P_i \cap U = \emptyset} (D'P_i)^{e_i}.$$

It remains to show that $D'P_i$ is a prime ideal if $P_i \cap U = \emptyset$. Let $\frac{a}{u}, \frac{b}{v} \in D'$ be such that $\frac{a}{u}\frac{b}{v} \in D'P_i$. Then $\frac{a}{u}\frac{b}{v} = \frac{x}{w}$, with $x \in P_i$ and $w \in U$. So $abw = uvx \in P_i$, because $x \in P_i$. Given that $w \notin P_i$, because $P_i \cap U = \emptyset$, we have $ab \in P_i$, which implies that $a \in P_i$ or $b \in P_i$. Hence $\frac{a}{u} \in D'P_i$ or $\frac{b}{v} \in D'P_i$, which shows that $D'P_i$ is a prime ideal. □

A special case

If a commutative ring has a unique maximal ideal, then we say that it is a *local ring*. In certain cases the localization of a commutative ring is a local ring. We will be particularly interested in the case where the ring is a Dedekind domain. However, we will first present a result giving two characterizations of local rings.

Proposition 12.17 *The following conditions are equivalent for a commutative ring R:*

- **a.** *R is a local ring;*
- **b.** *There is a proper ideal I of R which contains all the nonunits of R;*
- **c.** *The set of nonunits of R is an ideal.*

PROOF **a.** $\Longrightarrow$ **b**. If r is a nonunit, then (r) is a proper ideal in R and so is contained in the unique maximal ideal of R.
b. $\Longrightarrow$ **c**. Let A be the collection of nonunits in R. If $r, r' \in A$ and $x \in R$, then $r + r'$ and xr are in A. If not, then there exists $a \in R$ such that $a(r + r') = 1$, or $b \in R$ such that $b(xr) = 1$. In both cases, $1 \in A \subset I$ and so $I = R$, a contradiction. Hence A is a proper ideal in R.
c. $\Longrightarrow$ **a**. If I is the ideal of nonunits, then I is maximal. If not, then there is an ideal $I' \neq R$ which properly contains I. As I' must contain a unit, $I' = R$. It folllows that I is maximal. If H is a proper ideal in R, then H cannot contain a unit, so $H \subset I$. Therefore I is the unique maximal ideal. □

Exercise 12.11 *Show that the unique maximal ideal of a local ring is composed of its nonunits.*

If P is a prime ideal in the commutative ring R, then $U = R \setminus P$ is a multiplicative subset of R and $0 \notin U$. We write R_P for the localization $(R \setminus P)^{-1}R$. We call R_P the localization of R at P. The expression $X \cap R \setminus P = \emptyset$, for $X \subset R$, is equivalent to $X \subset P$. We also notice that $R \setminus P$ has no zero divisors, so from Exercise 12.11 the mapping $\pi : R \longrightarrow R_P$ is injective.

Theorem 12.10 *If R is a commutative ring and P a prime ideal in R, then the localization R_P is a local ring, with unique maximal ideal*

$$(R \setminus P)^{-1}P = \{\frac{x}{u}, x \in P, u \in R \setminus P\}.$$

PROOF As $P \cap R \setminus P = \emptyset$, from Lemma 12.5, $(R \setminus P)^{-1}P$ is a proper ideal in R_P. Let J be a maximal ideal in R_P. As J is prime, $\pi^{-1}(J)$ is a prime ideal in R, which is disjoint from $R \setminus P$ by Theorem 12.8. As observed above, $\pi^{-1}(J) \cap (R \setminus P) = \emptyset$ is equivalent to $\pi^{-1}(J) \subset P$, since $\pi^{-1}(J) \subset R$. Then, by Proposition 12.12,

$$J = (R \setminus P)^{-1} \left(\pi^{-1}(J)\right) \subset (R \setminus P)^{-1}P.$$

Since J is a maximal ideal in R_P and $(R \setminus P)^{-1}P$ is a proper ideal in R_P, we have $J = (R \setminus P)^{-1}P$. It follows that $(R \setminus P)^{-1}P$ is the unique maximal ideal of R_P. □

In accordance with the discussion after Exercise 12.11, for an ideal I in R, $(R \setminus P)^{-1}I = R_P I$, i.e., $(R \setminus P)^{-1}I$ is composed of finite sums of the form

$$x = \sum_{i=1}^{n} y_i \pi(x_i),$$

where $y_i \in R_P$ and $x_i \in I$. In particular, the unique maximal ideal of R_P can be written $R_P P$.

Now let us now consider the particular case of the localization of a Dedekind domain D at a prime ideal P.

Theorem 12.11 *If D is a Dedekind domain and P a prime ideal in D, then the localization D_P is a PID.*

PROOF From Theorem 12.9, D_P is a Dedekind domain. By Theorem 12.10, D_P is also a local ring and so has a unique ideal. However, a Dedekind domain having only a finite number of prime ideals is a PID (Corollary 12.7), hence the result. □

We may characterize the nonzero fractional ideals of D_P; however, we need to do some preliminary work. We recall that in Proposition 12.11 we showed that if U is a multiplicative subset of the ring R, and I and J ideals, then

$$U^{-1}(IJ) = (U^{-1}I)(U^{-1}J).$$

If R is an integral domain, P a prime ideal of R and $U = R \setminus P$, then we obtain

$$R_P(IJ) = (R_P I)(R_P J). \tag{12.2}$$

We aim to extend this relation to fractional ideals of R. First we extend the definition $R_P I$ to fractional ideals. For a fractional ideal F of R we let $R_P F$ be the subset of the fraction field K of R_P composed of finite sums of the form

$$x = \sum_{j=1}^{n} f_j x_j,$$

where $i_j \in I$, $x_j \in R_P$. (If $f \in F$, then $f = \frac{r}{r'}$, with $r \in R$, $r' \in R^*$; then $fx = \frac{rx}{r'} \in K$ and it follows that $R_P F \subset K$.) In fact, $R_P F$ is a fractional ideal of R_P. If F is the zero ideal, then there is nothing to prove, so let us suppose that this is not the case. Then $F = \alpha I$, where $\alpha \in R^*$ and I an ideal of R (Proposition 12.6). If $f \in F$ and $x \in R_P$, then $fx = \alpha f s x$, where $s \in I$. It follows that $R_P F = \alpha R_P I$. As $R_P I$ is an ideal in R_P, another application of Proposition 12.6 shows that $R_P F$ is a fractional ideal of R_P.

We may now extend Equation (12.2) to fractional ideals.

Proposition 12.18 *If R is an integral domain, P a prime ideal in R and F, G fractional ideals, then*

$$R_P(FG) = (R_P F)(R_P G).$$

PROOF An element of $R_P(FG)$ can be written in the form $x\sum_{i=1}^{n} f_i g_I$, where $f_i \in F$, $g_i \in G$ and $x \in R_P$. Since $x = \frac{r}{u}$, with $r \in R$ and $u \in R \setminus P$, we have

$$x\sum_{i=1}^{n} f_i g_I = \sum_{i=1}^{n}(\frac{r}{1}f_i)(\frac{1}{u}g_i) \in R_P(F)R_P(G),$$

Hence $R_P(FG) \subset (R_P F)(R_P G)$.

Moreover, any element of $(R_P F)(R_P G)$ is a finite sum of terms of the form $(xf)(yg)$, where $x, y \in R_P$ and $f \in F$, $g \in G$. However, $(xf)(yg) = (xy)(fg)$. Given that $xy \in R_P$ and $fg \in FG$, $(xf)(yg) \in R_P(FG)$ and it follows that $(R_P F)(R_P G) \subset R_P(FG)$. □

We are now are in position to establish a result which will prove essential further on. It provides us with a characterization of the nonzero fractional ideals of the localization of a Dedekind domain at a prime ideal.

Theorem 12.12 *If D is a Dedekind domain and P a nonzero prime ideal in D, then every nonzero fractional ideal J of D_P is a power of $D_P P$ and, for any $m \in \mathbf{Z}$, $(D_P P)^m = D_P P^m$. In addition, for any $m \geq 0$, $D_P(P^m) \cap D = P^m$.*

PROOF Theorem 12.9 ensures that D_P is a Dedekind domain and Theorem 12.10 that D_P has a unique prime ideal, namely $D_P P$. Now, using Theorem 12.6, we obtain that every nonzero fractional ideal J of D_P is a power of $D_P P$: $J = (D_P P)^m$, for some $m \in \mathbf{Z}$. If $m = 0$, then $J = D_P$.

Let us now show that $(D_P P)^m = D_P(P^m)$. We will consider three cases, namely, $m = 0$, $m \geq 1$ and $m \leq -1$.

Case 1: $m = 0$. For $m = 0$, this amounts to showing that $D_P = D_P D$. Clearly, $D_P D \subset D_P$. If $\frac{a}{u} \in D_P$, then $\frac{a}{u} = \frac{a}{u}\frac{1}{1} \in D_P D$, so $D_P \subset D_P D$ and we have the desired equality.

Case 2: $m =\geq 1$. For $m \geq 1$ we use an induction argument. For $m = 1$, there is nothing to prove. For $m \geq 2$, it is sufficient to apply Proposition 12.18.

Case 3: $m \leq -1$. From Proposition 12.18 we have

$$D_P = D_P D = D_P(PP^{-1}) = (D_P P)(D_P P^{-1}) \Longrightarrow D_P P^{-1} = (D_P P)^{-1}.$$

If $m \leq -2$, let us set $n = -m$. Then, using Proposition 12.18 again, we have

$$D_P P^m = D_P\left((P^{-1})^{-m}\right) = (D_P P^{-1})^{-m}.$$

However, $D_P P^{-1} = (D_P P)^{-1}$, so

$$(D_P P^{-1})^{-m} = \left((D_P P)^{-1}\right)^{-m} = (D_P P)^m.$$

We now turn to the final part of the theorem. Let $m \geq 1$. It is clear that $P^m \subset D_P P^m \cap D$. Suppose now that $\frac{x}{u} \in D_P P^m \cap D$, with $x \in P^m$ and $u \notin P$. There exists $r \in D$ such that

$\frac{x}{u} = \frac{r}{1}$. This implies that there is a $t \notin P$ such that $t(x - ru) = 0$. Hence we have $tru = tx \in P^m$, with $tu \notin P$. As $tru \in P^m$, P^m contains the product of the principal ideals Dtu and Dr. This means that P^m divides $DtuDr$. As $tu \notin P$, P does not divide Dtu. Since P is a prime ideal, P^m divides Dr, which implies that $r \in P^m$. Thus $\frac{x}{u} = \frac{r}{1}$, with $r \in P^m$. Therefore $D_P P^m \cap D \subset P^m$. This ends the proof. □

Quotient rings of localizations

If I is a proper ideal in R, then we have a canonical homomorphism λ of R onto the quotient ring $\bar{R} = R/I$. A multiplicative subset U of R induces in a natural way a multiplicative subset of $\bar{R} = R/I$, namely $\bar{U} = \lambda(U)$. The following proposition characterizes the localization of $\bar{R}$ with respect to $\bar{U}$.

Proposition 12.19 *Let U be a multiplicative subset of the ring R and $R' = U^{-1}R$. If I is a proper ideal in R such that*

$$ru \in I, r \in R, u \in U \Longrightarrow r \in I,$$

then the image $\bar{U}$ of U under λ is a multiplicative subset of $\bar{R}$ with no zero divisors, and $\bar{U}^{-1}\bar{R}$ is isomorphic to $R'/R'I$.

PROOF First we notice that $I \cap U = \emptyset$: If $a \in I \cap U$, then $a1 \in I$ and so, by hypothesis, $1 \in I$, which is impossible, because I is a proper ideal of R.

To see that $\bar{U}$ is a multiplicative subset of $\bar{R}$, first we notice that $1 \in U$ implies that $\bar{1} \in \bar{U}$. Next, if $\bar{a}, \bar{b} \in \bar{U}$, then $\bar{a} = a + I$, with $a \in U$, and $\bar{b} = b + I$, with $b \in U$, hence $\bar{a}\bar{b} = ab + I \in \bar{U}$, because $ab \in U$.

Finally we show that $\bar{U}$ has no zero divisors. Let $\bar{a} \in \bar{U}$. If $\bar{a}\bar{b} = \bar{0}$, with $\bar{b} \in R/I$, then $ab \in I$. As $a \in U$, by hypothesis $b \in I$, so $\bar{b} = \bar{0}$. Therefore $\bar{U}$ has no zero divisors.

We now define a mapping ψ from $\bar{U}^{-1}\bar{R}$ into $\bar{R}' = R'/R'I$ by

$$\psi(\frac{\bar{r}}{\bar{u}}) = \overline{\frac{r}{u}},$$

where $\overline{\frac{r}{u}}$ is the image of $\frac{r}{u}$ under the canonical homomorphism of R' onto $\bar{R}'$. We need to show that ψ is well-defined, i.e.,

$$\frac{\bar{r}}{\bar{u}} = \frac{\bar{r}_1}{\bar{u}_1} \Longrightarrow \overline{\frac{r}{u}} = \overline{\frac{r_1}{u_1'}}.$$

Indeed, if there exists $\bar{t} \in \bar{U}$ such that

$$\bar{t}(\bar{r}\bar{u}_1 - \bar{r}_1\bar{u}) = \bar{0},$$

then

$$(ru_1 - r_1u)t \in I \Longrightarrow ru_1 - r_1u \in I \Longrightarrow \frac{r}{u} - \frac{r_1}{u_1} = \frac{ru_1 - r_1u}{uu_1} \in R'I,$$

where in the first implication we have used the hypothesis on I. Thus $\overline{\frac{r}{u}} = \overline{\frac{r_1}{u_1'}}$ and the mapping ψ is well-defined.

Clearly, ψ is a ring homomorphism. If $x \in \bar{R}'$, then $x = \frac{r}{u} + R'I$, with $r \in R$, $u \in U$. If we set $y = \frac{\bar{r}}{\bar{u}}$, then $\bar{r} \in \bar{R}$, $\bar{u} \in \bar{U}$ and $\psi(y) = x$. Thus ψ is surjective. If $\overline{\frac{r}{u}} = \bar{0}$, then $\frac{r}{u} \in R'I$. Then $\frac{r}{u} = \frac{r'}{u'}$, with $r' \in I$ and $u' \in U$. Hence there exists $t \in U$ such that $t(ru' - r'u) = 0$ and so $tru' \in I$. As $tu' \in U$, by hypothesis $r \in I$ and it follows that $\frac{\bar{r}}{\bar{u}} = 0$ in $\bar{U}^{-1}\bar{R}$, so ψ is injective. This ends the proof. □

The next result characterizes the residue field of the localization of a commutative ring with respect to a maximal ideal.

Corollary 12.11 *If all the elements of $\bar{U}$ are invertible in $\bar{R}$, then $\bar{R}$ is isomorphic to $R'/R'I$. If P is a maximal ideal in a commutative ring R, then R/P is isomorphic to R_P/R_PP.*

PROOF Suppose that all the elements of $\bar{U}$ are invertible in $\bar{R}$. If $\frac{\bar{r}}{\bar{u}} \in \bar{U}^{-1}\bar{R}$ and we set $\bar{r}_1 = \bar{r}\bar{u}^{-1}$, then $\frac{\bar{r}_1}{1} = \frac{\bar{r}}{\bar{u}}$, so the canonical mapping from $\bar{R}$ into $\bar{U}^{-1}\bar{R}$ is an isomorphism. Thus we have an isomorphism from $\bar{R}$ onto $R'/R'I$.

Let us set $U = R \setminus P$. If $ru \in P$, with $r \in R$ and $u \in U$, then $r \in P$, because P is a prime ideal. Hence we can apply Proposition 12.19 with $I = P$: $\bar{U}^{-1}(R/P)$ is isomorphic to R_P/R_PP. Because R/P is a field, every element of $\bar{U}$ is invertible. It follows that there is an isomorphism from R/P onto R_P/R_PP. □

Localization and integral closure

If U is a multiplicative subset of a ring R, and S a ring containing R, then U is also a multiplicative subset of S. We aim to consider the case where L is some field containing R and S the integral closure of R in L. Thus the set $U^{-1}S$ is defined. However, if $R' = U^{-1}R$ is also contained in L, then integral closure of R' in L also exists.

Proposition 12.20 *Let R be an integral domain and L a field containing R. We suppose that S is the integral closure of R in L and that U is a multiplicative subset of R. Then $S' = U^{-1}S$ is the integral closure of $R' = U^{-1}R$ in L.*

PROOF As $R' \subset K$, the field of fractions of R, and $K \subset L$, the integral closure of R' in L exists.

Let $x = \frac{s}{u} \in S'$. As S is integral over R, there exist $r_0, r_1, \ldots, r_{n-1} \in R$ such that

$$r_0 + r_1 s + \cdots + r_{n-1}s^{n-1} + s^n = 0 \Longrightarrow \frac{1}{u^n}(r_0 + r_1 s + \cdots + r_{n-1}s^{n-1} + s^n) = 0.$$

This can be written

$$\frac{r_0}{u^n} + \frac{r_1}{u^{n-1}}\frac{s}{u} + \cdots + \frac{r_{n-1}}{u}\frac{s^{n-1}}{u^{n-1}} + \frac{s^n}{u^n} = 0$$

which implies that $\frac{s}{u}$ is integral over R'.

Now let $x \in L$ be integral over S'. There exist $\frac{r_0}{u_0}, \frac{r_1}{u_1}, \ldots, \frac{r_{n-1}}{u_{n-1}} \in S'$ such that

$$\frac{r_0}{u_0} + \frac{r_1}{u_1}x + \cdots + \frac{r_{n-1}}{u_{n-1}}x^{n-1} + x^n = 0.$$

Setting $u = u_0 u_1 \cdots u_{n-1}$, we may write

$$u^n\left(\frac{r_0}{u_0} + \frac{r_1}{u_1}x + \cdots + \frac{r_{n-1}}{u_{n-1}}x^{n-1} + x^n\right) = 0.$$

However,

$$\frac{u^n r_i}{u_i}x^i = \frac{u^{n-i}r_i}{u_i}(ux)^i \qquad \textit{with} \qquad \frac{u^{n-i}r_i}{u_i} \in R,$$

so ux is integral over R. As the integral closure of R in L is S, we have $ux \in S$, which implies that $x = \frac{ux}{u} \in U^{-1}S$. □

Remark We may sum up the proposition by saying that localization of the integral closure is the same as the integral closure of the localization, i.e., the operations integral closure and localization commute.

12.7 Integral closures of Dedekind domains

If D is a Dedekind domain, then certain extensions of D are also Dedekind domains. We have seen that this is in general the case with localizations. In this section we aim to consider another class of such extensions. The properties of such extensions enable us to establish certain important results.

Lemma 12.7 *Let $A \subset B \subset C$ be commutative rings. If B is a finitely generated A-module and C a finitely generated B-module, then C is a finitely generated A-module.*

PROOF Let $\{b_1, \ldots, b_m\}$ be a generating set for B over A and $\{c_1, \ldots, c_n\}$ a generating set for C over B. For $x \in C$, there are $\beta_1, \ldots, \beta_n \in B$ such that

$$x = \sum_{i=1}^{n} \beta_i c_i.$$

For any $i = 1, \ldots, n$, there exist $\alpha_{i1}, \ldots, \alpha_{im} \in A$ such that

$$\beta_i = \sum_{j=1}^{m} \alpha_{ij} b_j,$$

hence

$$x = \sum_{i=1}^{n} \left(\sum_{j=1}^{m} \alpha_{ij} b_j \right) c_i = \sum_{i=1}^{n} \sum_{j=1}^{m} \alpha_{ij}(b_j c_i).$$

As $B \subset C$, the elements $b_j c_i$ belong to C and it follows that the $b_j c_i$, for $1 \leq j \leq m$ and $1 \leq i \leq n$, form a generating set for C over A. □

Theorem 12.13 *(transitivity of integrality) Let $A \subset B \subset C$ be commutative rings. If B is integral over A and C integral over B, then C is integral over A.*

PROOF Let $x \in C$. As C is integral over B, there exist $b_0, b_1, \ldots, b_{n-1} \in B$ such that

$$b_0 + b_1 x + \cdots + b_{n-1} x^{n-1} + x^n = 0. \tag{12.3}$$

We set $D = A[b_0, b_1, \ldots, b_{n-1}]$ and $E = D[x]$. From equation (12.3), powers of x higher than $n-1$ can be expressed as a linear sum of powers of x (with coefficients in D) smaller than n. Hence E is a finitely generated D-module. In the same way, as B is integral over A, for each b_i, there is a positive integer m_i such that powers of b_i higher than $m_i - 1$ can be expressed as a linear sum of powers of b_i (with coefficients in A) smaller than m_i. As D is composed of finite sums of of expressions of the form

$$a b_0^{\alpha_0} b_1^{\alpha_1} \cdots b_s^{\alpha_s},$$

with $a \in A$, D is a finitely generated A-module. From Lemma 12.7, E is a finitely generated A-module. Thus x belongs to a subring of C containing A, which is a finitely generated A-module. From Theorem 11.3, x is integral over A. It follows that C is integral over A. □

Corollary 12.12 *Let $S \subset R$ be commutative rings and C the integral closure of S in R. Then C is integrally closed in R.*

The intersection of all subrings of R which contain S and integrally closed in R is the integral closure C of S in R.

PROOF Let $x \in R$ be integral over C. From Theorem 12.13 we deduce that $C[x]$ is integral over S. In particular, x is integral over S, so $x \in C$.

Suppose now that $S \subset T \subset R$ are commutative rings, where T is integrally closed in R. Let $x \in C$. Then x is a zero of a monic polynomial with coefficients in S. As $S \subset T$, x is also a zero of a monic polynomial with coefficients in T. Given that T is integrally closed, $x \in T$. Thus $C \subset T$ and the result now follows. □

We have a second corollary.

Corollary 12.13 *If $K \subset L$ are number fields, then O_L is the integral closure of O_K in L.*

PROOF Let A be the integral closure of O_K in L. Then we have $\mathbf{Z} \subset O_K \subset A$, with O_K integral over $\mathbf{Z}$ and A integral over O_K. From Theorem 12.13, A is integral over $\mathbf{Z}$ and so $A \subset O_L$. On the other hand, of $x \in O_L$, then x is integral over $\mathbf{Z}$. As $\mathbf{Z} \subset O_K$, x is integral over O_K, i.e., $x \in A$. Thus $O_L \subset A$. □

We now aim to consider in particular integral closures of noetherian domains.

Lemma 12.8 *Let E be a separable extension of F, with $[E : F] = m$. If $\{b_1 \dots, b_m\}$ is a basis of E over F, then there is a basis $\{c_1, \dots, c_m\}$ such that $T_{E/F}(b_i c_j) = \delta_{ij}$, where δ_{ij} is the Kronecker symbol.*

PROOF The trace $T_{E/F} : E \longrightarrow F$ is linear, so $T_{E/F} \in Hom(E, F)$, the dual space of the F-vector space E. We define $\tau : E \longrightarrow Hom(E, F)$ by

$$\tau(b)(x) = B(b, x),$$

where B is the bilinear form defined by the trace. The mapping τ is clearly linear; it is also injective, because B is nondegenerate. As E and $Hom(E, F)$ hve the same dimension, τ is an isomorphism. Let $\{\phi_1, \dots, \phi_m\}$ be the dual basis of $\{b_1 \dots, b_m\}$, so that $\phi_i(b_j) = \delta_{ij}$. As τ is an isomorphism, there exist $c_1, \dots, c_m \in E$ such that $\tau(c_i) = \phi_i$, for $i = 1, \dots, m$, therefore

$$\tau(c_i)(x) = \phi_i(x) \Longrightarrow \tau(c_i)(b_j) = \delta_{ij} \Longrightarrow T_{E/F}(c_i b_j) = \delta_{ij},$$

which is what we set out to prove. □

We now consider integral closures of noetherian domains.

Theorem 12.14 *Let D be a noetherian integrally closed domain, with field of fractions F. If E is a finite separable extension of F and B the integral closure of D in E, then B is a noetherian ring.*

PROOF From Theorem 11.5, B is a submodule of a finitely generated D-module, which we note M. As D is noetherian and M finitely generated, M is noetherian. However, a submodule of a noetherian module is noetherian, and so B is a noetherian D-module.

Let I be an ideal in B. Then I is a submodule of the D-module B. As B is a noetherian, I is finitely generated D-module: there exist $x_1, \dots, x_n \in I$ such that

$$I = Dx_1 + \cdots + Dx_n.$$

Given that $D \subset B$, we may also write

$$I = Bx_1 + \cdots + Bx_n$$

and so I is a finitely generated B-module. As every ideal in B is finitely generated, B is noetherian. □

Our next step is to show that every prime ideal in the integral closure B as defined above is maximal. We need some preliminary results.

Lemma 12.9 *Let D be a domain which is integral over the subring R. If J is a nonzero ideal of D, then $J \cap R$ is a nonzero ideal of R.*

PROOF $J \cap R$ is clearly an ideal. Let $x \in J$, $x \neq 0$. There exists a monic polynomial

$$f(X) = a_0 + a_1 X + \cdots + a_{n-1} X^{n-1} + X^n \in R[X]$$

such that $f(x) = 0$. We may take f of minimal degree, which implies that $a_0 \neq 0$. (If $a_0 = 0$, then

$$a_1 + a_2 x + \cdots + a_{n-1} x^{n-2} + x^{n-1} = 0,$$

because $x \neq 0$ and R is a domain and so f is not of minimal degree, a contradiction.) Hence

$$a_0 = -(a_1 + a_2 x + \cdots + a_{n-1} x^{n-2} + x^{n-1}) x \in J \cap R,$$

so $J \cap R \neq \{0\}$. □

Remark It is easy to see that, if J is a prime ideal, then $J \cap R$ is also a prime ideal.

Before considering the case of maximal ideals we prove another lemma.

Lemma 12.10 *Let D be a domain which is integral over the subring R. Then D is a field if and only if R is a field.*

PROOF Suppose that D is a field and let x be a nonzero element of R. The inverse x^{-1} of x is integral over R, hence there exist $a_1, a_1, \ldots, a_{n-1} \in R$ such that

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

Multiplying by x^{n-1} we obtain

$$a_0 x^{n-1} + a_1 x^{n-2} + \cdots + a_{n-1} + x^{-1} = 0,$$

hence $x^{-1} \in R$ and so it follows that R is a field.

Now suppose that R is a field and let x be a nonzero element of D. From Lemma 12.9 there exists $a \in Dx \cap R$, $a \neq 0$. We can write $a = bx$, with $b \in D$. Let a' be the inverse of a in R. Then

$$1 = a'a = a'(bx) = (a'b)x,$$

and so x is invertible in D and thus D is a field. □

Proposition 12.21 *Let D be a domain which is integral over the subring R and J a prime ideal in D. Then J is a maximal ideal in D if and only if $J \cap R$ is a maximal ideal in R.*

PROOF Let J be a prime ideal in D. Then the ring homomorphism

$$\phi : R/(J \cap R) \longrightarrow D/J, x + (J \cap R) \longmapsto x + J$$

is injective, so we may consider $R/(J \cap R)$ to be a subring of D/J. We claim that D/J is integral over $R/(J \cap R)$. To see this let us take $x + J \in D/J$. As D is integral over R, there exists a monic polynomial

$$f(X) = a_0 + a_1 X + \cdots + a_{n-1} X^{n-1} + X^n \in R[X]$$

such that $f(x) = 0$. To simplify the notation we set $I = J \cap R$. We define a monic polynomial $\bar{f} \in R/I[X]$ by

$$\bar{f}(X) = (a_0 + I) + (a_1 + I)X + \ldots + (a_{n-1} + I)X^{n-1} + X^n.$$

Then

$$\bar{f}(x + J) = f(x) + J = J.$$

As J is the zero element of D/J, $x + J$ is integral over R/I. This establishes the claim.

If J is a maximal ideal in D, then D/J is a field. From Lemma 12.10 $R/(J \cap R)$ is a field, therefore $J \cap R$ is a maximal ideal.

Conversely, if $J \cap R$ is a maximal ideal in R, then $R/(J \cap R)$ is a field and so, from Lemma 12.10 again, D/J is a field and thus J is a maximal ideal. □

We may now establish the principal result of this section.

Theorem 12.15 *Let D be a Dedekind domain, with field of fractions F. If E is a finite separable extension of F and B the integral closure of D in E, then B is a Dedekind domain.*

PROOF As B is contained in E, which is a field, B is an integral domain.

Let C be the integral closure of B in its field of fractions. Then C is integral over B and B is integral over D, so C is integral over D (Theorem 12.13). Thus, if $x \in C$, then $x \in B$ and it follows that $C = B$, i.e., B is integrally closed.

To see that B is noetherian, it is sufficient to apply Theorem 12.14.

Finally, we show that every nonzero prime ideal is maximal. Let P be a nonzero prime ideal in B. Then $P = Q \cap D$ is a nonzero prime ideal in D (Lemma 12.9). As D is a Dedekind domain, P is a maximal ideal in D. From Proposition 12.21, Q is a maximal ideal in B. □

Remark From Proposition 11.2 the field of fractions of B is E. If $F \neq E$, then D and B have different fields of fractions and so are distinct. Thus D is strictly included in B. We have shown that a Dedekind domain is strictly included in another Dedekind domain.

Let C be a Dedekind domain and D an integral domain containing C. If P is a nonzero prime ideal in C, then C/P is a field and the mapping

$$\phi : C/P \longrightarrow D/DP,\ a + P \longmapsto a + DP$$

is a well-defined homomorphism. Hence we may consider that D/DP is a C/P-vector space. (The scalar multiplication is defined as follows: $\bar{c}\bar{x} = \phi(\bar{c})\bar{x}$, for $\bar{c} \in C/P$ and $\bar{x} \in D/DP$.) There is a natural question: If K and L are the respective fraction fields of C and D and we know the dimension $[K : L]$, what can we say about the dimension of the C/P-vector space D/DP? We aim to give an answer to this question for a particular integral domain D. We will need the following standard result, for which a proof may be found, for example, in [5].

Theorem 12.16 *If R is a PID and M a free R-module of rank n, then any submodule N of M is free and has rank at most n.*

Theorem 12.17 *Let C be a Dedekind domain, K its field of fractions and L a separable extension of K of degree n. Suppose that D is the integral closure of C in L. If P is a nonzero prime ideal in C, then the dimension of the C/P-vector space D/DP is n.*

PROOF Let $U = C \setminus P$ and $C' = U^{-1}C = C_P$. From Theorem 12.11, C' is a PID. Proposition 12.20 ensures that, as D is the integral closure of C in L, $D' = U^{-1}D$ is the integral closure of C' in L. Since the fraction field of C' is that of C, from Theorem 11.5, D' is contained in a free C'-module M of rank n. As C' is a PID and D' a submodule of M, from Theorem 12.16, D' is a free C'-module of rank at most n. Using Theorem 11.5 again, we see that D' contains a free C'-module of rank n. Thus, using Theorem 12.16 again, we obtain that D' is a free C'-module of rank n.

The extension of P to C' is $C'P$ and its extension to D' is $D'P$. As $D'P = D'(C'P)$, $D'P$ is also the extension of $C'P$ to D', so the mapping

$$\psi : C'/C'P \longrightarrow D'/D'P, c' + C'P \longmapsto c' + D'P$$

is a ring homomorphism. Since $C'P$ is the maximal ideal of the local ring C', the quotient $C'/C'P$ is a field. Thus $D'/D'P$ is a $C'/C'P$-vector space. (The scalar multiplication is defined by $\bar{c}'.\bar{x}' = \psi(\bar{c}')\bar{x}'$, for $\bar{c}' \in C'/C'P$ and $\bar{x}' \in D'/D'P$.) We now consider the dimension of this vector space.

We have seen that D' is a free C'-module of rank n, so D' has a basis $\mathcal{B}' = \{x'_1, \ldots, x'_n\}$. Let us write $\bar{x}'_i$ for the image of x'_i in $D'/D'P$ (under the standard mapping of D' onto $D'/D'P$). We claim that $\bar{\mathcal{B}}' = \{\bar{x}'_1, \ldots, \bar{x}'_n\}$ is a basis of $D'/D'P$. Clearly $\bar{\mathcal{B}}'$ is a generating set of $D'/D'P$, so we only need to consider the independance. Let $\sum_{i=1}^n \bar{c}'_i.\bar{x}'_i = 0$, where $\bar{c}'_i \in C'/C'P$. Then

$$\sum_{i=1}^n c'_i x'_i \in D'P = D'(C'P)$$

and so we may write $\sum_{i=1}^n c'_i x_i = \sum_{j=1}^m \hat{c}'_j y'_j$, with $y'_j \in D'$ and $\hat{c}'_j \in C'P$. Expressing the y'_j in terms of the x'_i, we obtain $\sum_{i=1}^n c'_i x'_i = \sum_{i=1}^n \tilde{c}'_i x'_i$, with $\tilde{c}'_i \in C'P \subset C'$. It follows that $c'_i = \tilde{c}'_i$, for all i, which implies that $c'_i \in C'P$ and so $\bar{c}'_i = 0$, for all i. We have shown that $\bar{\mathcal{B}}'$ is an independant set and so a basis of $D'/D'P$: $D'/D'P$ is a $C'/C'P$-vector space of dimension n.

We now consider the mappings

$$\alpha : C/P \longrightarrow C'/C'P, c + P \longmapsto \frac{c}{1} + C'P \quad \text{and} \quad \beta : D/DP \longrightarrow D'/D'P, d + P \longmapsto \frac{d}{1} + D'P.$$

These mappings α and β are clearly well-defined ring homomorphisms. We aim to use Corollary 12.11 to show that they are in fact isomorphisms. For α there is no difficulty, because P is a prime ideal in a Dedekind domain, hence maximal. We now consider β. Let us set $U = C \setminus P$. Because C/P is a field, for $u \in U$ there exists $v \in U$ and $x \in P$ such that $uv = 1 + x$. As $P \subset DP$, every element of $U + DP$ has an inverse in the same set and it follows that β is an isomorphism.

We now notice that $D'/D'P$ is a C/P-vector space for the scalar multiplication $\bar{c} \cdot \bar{x}' = \alpha(\bar{c})\bar{x}'$, where $\bar{c} \in C/P$ and $\bar{x}' \in D'/D'P$. (We distinguish scalar multiplication and ring multiplication by using a dot in the former case.) It is not difficult to check that $\bar{\mathcal{B}}'$ is a basis of this vector space, so it too has dimension n. We claim that β is an isomorphism of C/P-vector spaces. We only need to verify that the scalar multiplicaion is respected. Let $\bar{c} \in C/P$ and $\bar{x} \in D/DP$. Then

$$\beta(\bar{c} \cdot \bar{x}) = \beta\left(\phi(\bar{c})\bar{x}\right) = \beta\left(\phi(\bar{c})\right)\beta(\bar{x}),$$

with $\beta\left(\phi(\bar{c})\right) = \frac{c}{1} + D'P$. Thus

$$\beta\left(\phi(\bar{c})\right)\beta(\bar{x}) = (\frac{c}{1} + C'P) \cdot \beta(\bar{x}) = \alpha(c+P) \cdot \beta(\bar{x}) = \bar{c} \cdot \beta(\bar{x})$$

and so

$$\beta(\bar{c} \cdot \bar{x}) = \bar{c} \cdot \beta(\bar{x}),$$

as required. Since $D'/D'P$ is a C/P-vector space of dimension n, so is D/DP. This finishes the proof. □

12.8 Norm and trace for ring extensions

We have studied traces and norms in field extensions. We now consider ring extensions. We suppose that $R \subset S$ are commutative rings. In addition we consider that S is a free R-module whose rank n is finite. Let $\mathcal{B} = \{x_1, \ldots, x_n\}$ be a basis of the R-module S and $\theta : S \longrightarrow S$ a linear mapping. We have

$$\theta(x_j) = \sum_{i=1}^{n} a_{ij} x_i,$$

with $a_{ij} \in R$. The matrix $M(\theta) = (a_{ij})$ is called the matrix of θ with respect to the basis $\mathcal{B}$. If $\mathcal{B}' = \{x'_1, \ldots, x'_n\}$ is another basis of the R-module S, then

$$\theta(x'_j) = \sum_{i=1}^{n} a'_{ij} x'_i,$$

with $a'_{ij} \in R$. We note the matrix with respect to this basis $M'(\theta)$. We now look for the relation between the matrices $M(\theta)$ and $M'(\theta)$. If $x_j = \sum_{i=1}^{n} c_{ij} x'_i$, then

$$\theta(x_j) = \sum_{i=1}^{n} a_{ij} x_i = \sum_{i=1}^{n} a_{ij} \left(\sum_{k=1}^{n} c_{ki} x'_k \right) = \sum_{k=1}^{n} \left(\sum_{i=1}^{n} c_{ki} a_{ij} \right) x'_k$$

and, on the other hand

$$\theta(x_j) = \sum_{i=1}^{n} c_{ij} \theta(x'_i) = \sum_{i=1}^{n} c_{ij} \left(\sum_{k=1}^{n} a'_{ki} x'_k \right) = \sum_{k=1}^{n} \left(\sum_{i=1}^{n} a'_{ki} c_{ij} \right) x'_k.$$

Therefore, with $C = (c_{ij})$, we have

$$M'(\theta)C = CM(\theta).$$

As C is the matrix of a change of basis, $C \in Gl_n(R)$, hence we may write

$$M'(\theta) = CM(\theta)C^{-1}. \tag{12.4}$$

Also, as

$$\det(C)\det(C^{-1}) = \det(I_n) = 1,$$

$\det(C)$ is a unit in the ring R.

We now consider the special case where θ is defined by multiplication by a nonzero element of S:

$$\theta(z) = \theta_x(z) = xz.$$

We define the trace, norm and characteristic polynomial of x as we did for field extensions, namely

$$T_{S/R}(x) = Tr(M(\theta_x)) \qquad N_{S/R}(x) = \det M(\theta_x)$$

and

$$\text{char}\ _{S/R}(x) = \det\left(XI - M(\theta_x)\right).$$

(The relation (12.4) ensures that the trace, norm and characteristic polynomial are unaffected by the choice of basis.) In the same way as for field extensions, the trace is linear and the norm multiplicative.

We now turn to rings of fractions. Let U be a multiplicative subset of R. As $R \subset S$, U is also a multiplicative subset S. We set $R' = U^{-1}R$ and $S' = U^{-1}S$. It is not difficult to see that $R' \subset S'$, so S' is an R'-module. Let $\mathcal{B} = \{x_1, \ldots, x_n\}$ be a basis of the R-module S. We claim that $\mathcal{B}' = \{\frac{x_1}{1}, \ldots, \frac{x_n}{1}\}$ is a basis of the R'-module S', hence S' is a free R'-module of rank n. First we show that $\mathcal{B}'$ is a generating set of S'. Let $\frac{a}{u} \in S'$. Then there exist $r_1, \ldots, r_n \in R$ such that

$$\frac{a}{u} = \frac{r_1x_1 + \cdots + r_nx_n}{u} = \frac{r_1}{u}\frac{x_1}{1} + \cdots + \frac{r_n}{u}\frac{x_n}{1},$$

which implies that $\mathcal{B}'$ is a generating set of S'. Now we show that the set $\mathcal{B}'$ is independant. If

$$\frac{r_1}{u_1}\frac{x_1}{1} + \cdots + \frac{r_n}{u_n}\frac{x_n}{1} = 0,$$

with $\frac{r_i}{u_i} \in R'$, then

$$r_1u_1'x_1 + \cdots + r_nu_n'x_n = 0,$$

where $u_i' = \frac{u_1\cdots u_n}{u_i}$. Hence

$$r_1u_1' = \cdots = r_nu_n' = 0 \Longrightarrow r_1 = \cdots = r_n = 0,$$

because $u_i' = 0$, for all i. It follows that $\frac{r_i}{u_i} = 0$, for all i and so $\mathcal{B}'$ is an independant set. We have shown that $\mathcal{B}'$ is a basis of the R'-module S'.

Let γ be the canonical mapping from S into S'. If $x \in S$, then $\gamma(x) \in S'$ and we have linear endomorphisms $\theta_x : S \longrightarrow S$ and $\theta'_{\gamma(x)} : S' \longrightarrow S'$. If the matrix of θ_x in the basis $\mathcal{B}$ is (a_{ij}), then the matrix of $\theta'_{\gamma(x)}$ in the basis $\mathcal{B}'$ is $(\gamma(a_{ij}))$.

$$T_{S'/R'}(\gamma(x)) = \gamma(T_{S/R}(x)) \qquad N_{S'/R'}(\gamma(x)) = \gamma(N_{S/R}(x))$$

and

$$\text{char}\ _{S'/R'}(\gamma(x)) = \gamma^*(\text{char}\ _{S/R}(x)),$$

where γ^* is the mapping from $R[X]$ into $R'[X]$ which applies γ to each coefficient of a polynomial in $R[X]$. Identifying S with its image under γ, we obtain

$$T_{S'/R'}(x) = T_{S/R}(x) \qquad N_{S'/R'}(x) = N_{S/R}(x)$$

and

$$\text{char}\ _{S'/R'}(x) = \text{char}\ _{S/R}(x).$$

Chapter 13

Ramification theory

Let K and L be number fields, with K included in L, and $R = O_K$ and $S = O_L$ the associated number rings. If I is an ideal in R, then we write SI for the ideal generated by I in S: SI is the collection of expressions of the form $\sum_{i=1}^n x_i y_i$, with $x_i \in S$ and $y_i \in I$. If I is a principal ideal (a), then $SI = Sa$, i.e., the prime ideal generated by a in S. We will be particularly interested in the case where I is a prime ideal and the relation of such an ideal with prime ideals in S. For example, $I = \mathbf{Z}2$ is a prime ideal in $\mathbf{Z}$, but $J = \mathbf{Z}[\sqrt{2}]2$ is not a prime ideal in $\mathbf{Z}[\sqrt{2}]$, since $(2+3\sqrt{2})^2 \in J$, but $2+3\sqrt{2} \notin J$. The way a prime ideal "lifted" to a larger ring is decomposed is a central topic of algebraic number theory.

Remark The ideal SI is in fact the extension of the ideal I in S with respect to the injection mapping of R into S.

13.1 First notions

Let P be a prime ideal in R; if Q is a prime ideal in S such that $Q \supset SP$, then we say that Q *lies over* P, or P *lies under* Q.

Remark If $K = \mathbf{Q}$, then $R = \mathbf{Z}$ and a prime ideal $P \neq \{0\}$ is of the form $(p) = \mathbf{Z}p$, where p is a prime number, so $SP = Sp$.

Proposition 13.1 *Let Q be a proper ideal of S and P a nonzero prime ideal of R. Then $Q \supset SP$ if and only if $P = Q \cap R$.*

PROOF If $Q \supset SP$, then $Q \supset P$, because $1 \in S$. This implies that $Q \cap R \supset P \cap R = P$. As P is a maximal ideal, because P is prime and nonzero, and $Q \cap R \neq R$, we have $Q \cap R = P$.

On the other hand, if $Q \cap R = P$, then $Q \supset P$, which implies that $Q = SQ \supset SP$. □

Proposition 13.2 *If I is a proper ideal in R, then SI is a proper ideal in S.*

PROOF If $SI = S$, then there exist $n \in \mathbf{N}^*$, $s_1, \ldots, s_n \in S$ and $x_1, \ldots, x_n \in I$ such that

$$1 = \sum_{i=1}^n s_i x_i.$$

Let $S' = R[s_1, \ldots, s_n]$ be the subring of S generated by R and the elements $s_1, \ldots, s_n$. The ring S' is a finitely generated R-module, since the s_i are algebraic integers. In addition, as $1 \in S'I$,

$S' \subset S'I$. We now take a set of generators $g_1, \dots g_n$ of the R-module S'. Because $S' \subset S'I$, we may write

$$g_i = \sum_{j=1}^{k_i} x_{ij} s_{ij} = \sum_{j=1}^{k_i} x_{ij} \left(\sum_{u=1}^{n} r_u^{ij} g_u \right) = \sum_{u=1}^{n} \left(\sum_{j=1}^{k_i} x_{ij} r_u^{ij} \right) g_u,$$

where $x_{ij} \in I$, $s_{ij} \in S'$ and $r_u^{ij} \in R$. As $\sum_{j=1}^{k_i} x_{ij} r_u^{ij} \in I$, we have

$$g_i = \sum_{u=1}^{n} x_u g_u,$$

with $x_u \in I$. Hence there is a matrix $A \in \mathcal{M}_n(I)$ such that

$$g = Ag,$$

where

$$g = \begin{pmatrix} g_1 \\ \vdots \\ g_n \end{pmatrix}.$$

Therefore, $(I_n - A)g = 0$. Multiplying on the left by the adjoint matrix of $I_n - A$, we obtain $\det(I_n - A)I_n g = 0$. Consequently $\det(I_n - A)s' = 0$, for any $s' \in S'$, which implies that $\det(I_n - A) = 0$. If we develop the determinant, then we obtain an expression which is 1 plus a sum of products of elements of I, i.e., of the form $1 + x$, with $x \in I$. From this we have $1 = -x \in I$, which contradicts the fact that I is a proper ideal of R. We have shown that SI is properly contained in S. □

Exercise 13.1 *In the proof of the theorem we used the fact that the s_i are algebraic integers. Why is this important?*

Corollary 13.1 *Let P be prime ideal in R. Then $SP \cap R = P$.*

PROOF If $P = \{0\}$, then the result is clear, so let us suppose that this is not the case. As P is a prime ideal of R, P is a proper ideal of R, therefore SP is a proper ideal of S. From Proposition 13.1, with $Q = SP$, we have $SP \cap R = P$. □

Remarks

- **a.** Corollary 13.1 is in fact a particular case of Theorem 12.7.
- **b.** If $K = \mathbf{Q}$ and $P = \mathbf{Z}p$, where p is prime number, then we obtain

$$O_L p \cap \mathbf{Z} = \mathbf{Z}p.$$

It is natural to ask whether there exists a prime ideal lying over a given prime ideal.

Theorem 13.1 *Every nonzero prime ideal Q of S lies over a unique nonzero prime ideal P of R.*
Every prime ideal P of R lies under at least one prime ideal Q of S. If $P \neq \{0\}$, then there is a finite number of prime ideals Q lying over P.

PROOF Let Q be a nonzero prime ideal of S. Clearly $P = Q \cap R$ is a prime ideal of R. Since $Q \neq \{0\}$, there is a nonzero integer $x \in Q$ (Proposition 11.13). As $x \in R$, $x \in Q \cap R$, so $P \neq \{0\}$. If Q lies over the nonzero prime ideal P', then, from Proposition 13.1, $P' = Q \cap R$, so Q lies over a unique prime ideal.

Suppose now that P is a prime ideal of R. If $P = \{0\}$, then P lies under $\{0\} \subset S$. Now let us suppose that $P \neq \{0\}$. We claim that a prime ideal Q of S contains SP if and only if Q appears in the decomposition of SP into prime ideals: From Corollary 12.2, $Q \supset SP$ if and only if $Q|SP$; as $SP \neq \{0\}$ nor S, from Theorem 12.3, SP has a unique decomposition into nonzero prime ideals, so Q divides SP if and only if Q is one of the prime ideals in the decomposition of SP. It follows that P lies under a prime ideal of S, namely any prime ideal in the decomposition of SP. These are the only ideals which can lie over P, so the number of prime ideals lying over P is finite. □

Exercise 13.2 *Use Theorem 13.1 to find a proof that a prime ideal P in a number ring O_K contains exactly one prime number p. (This result has already been seen in Proposition 13.6.)*

If P is a nonzero prime ideal of R, Q a nonzero prime ideal of S dividing SP and e the highest power of Q in the decomposition of SP into prime ideals, then we call e the *ramification index of Q over P*. We note the ramification index $e(Q|P)$. In the case where $R = \mathbf{Z}$ and $P = \mathbf{Z}p$, then we write $e(Q|p)$.

Suppose again that P is a nonzero prime ideal of R and Q a nonzero prime ideal of S dividing SP. As P and Q are maximal ideals, R/P and S/Q are fields, which, from Proposition 11.12, are finite. The mapping

$$\phi : R \longrightarrow S/Q, x \longmapsto x + Q$$

is a well-defined ring homomorphism, with kernel $Q \cap R = P$, so we may consider R/P as a subfield of S/Q. We set $f(Q|P) = [S/Q : R/P]$, which is called the *inertial degree of Q over P*. In the case where $R = \mathbf{Z}$ and $P = \mathbf{Z}p$ we write $f(Q|p)$.

We often say that the ramification index and the inertial degree are multiplicative due to the properties given in the following proposition.

Proposition 13.3 *Suppose that P, Q and U are nonzero prime ideals in the number rings $R \subset S \subset T$ such that U lies over Q and Q lies over P. Then U lies over P and*

$$e(U|P) = e(U|Q)e(Q|P) \qquad \text{and} \qquad f(U|P) = f(U|Q)f(Q|P).$$

PROOF Q lies over P means that we have

$$SP = Q^{e(Q|P)} Q_2^{e_2} \cdots Q_s^{e_s},$$

where $e_i = e(Q_i|P)$. Since $TS = T$ and $T^n = T$, for all $n \in \mathbf{N}^*$, when we multiply the previous expression by T we obtain

$$TP = (TQ)^{e(Q|P)} (TQ_2)^{e_2} \cdots (TQ_s)^{e_s}.$$

Now, U lies over Q, so we can write

$$TQ = U^{e(U|Q)} U_2^{a_2} \cdots U_t^{a_t},$$

where $a_i = e(U_i|Q)$. Hence,

$$TP = U^{e(U|Q)e(Q|P)} U_2^{a_2 e(Q|P)} \cdots U_t^{a_t e(Q|P)} (TQ_2)^{e_2} \cdots (TQ_s)^{e_s}.$$

Moreover, U does not divide TQ_i, for $i = 2, \ldots, s$. Indeed, if $U|TQ_i$, then $U|TQ$ and $U|TQ_i$, which implies that

$$U \supset T(Q + Q_i) = T\text{hcf}(Q, Q_i) = TS = T,$$

which is not possible. Therefore U lies over P and

$$e(U|P) = e(U|Q)e(Q|P).$$

We now consider the inertial degree. S/Q is a field extension of R/P and T/U is a field extension of S/Q, so we have

$$f(U/P) = [T/U : R/P] = [T/U : S/Q][S/Q : R/P] = f(U|Q)f(Q|P),$$

as claimed. □

13.2 Norm of an ideal

In this section we introduce the norm of an ideal in a number ring, which will play an important role in the following. We have seen above that $|O_K/I|$ is finite when I is a nonzero ideal (Proposition 11.12). We define the norm of I by

$$\|I\| = |O_K/I|.$$

The norm has an important multiplication property, namely, if I and J are nonzero ideals, then

$$\|IJ\| = \|I\|\|J\|.$$

We will first prove this in the case where the ideals are coprime and then later in the general case.

Proposition 13.4 *If I and J are nonzero coprime ideals in a number ring O_K, then*

$$\|IJ\| = \|I\|\|J\|.$$

PROOF From the Chinese remainder theorem (Appendix F) we have

$$O_K/(I \cap J) = O_K/I \times O_K/J.$$

However, from Proposition 12.4, $I \cap J = IJ$, hence the result. □

We now generalize Proposition 13.4.

Theorem 13.2 *If I and Q are nonzero ideals in a number ring O_K, then*

$$\|IQ\| = \|I\|\|Q\|.$$

PROOF From Theorem 12.5, there is an ideal J in O_K, coprime with Q, such that IJ is principal. Let $IJ = (x)$. Then

$$(x) + IQ = I(J + Q) = I(O_K) = I. \tag{13.1}$$

We now define a mapping ϕ from O_K into I/IQ by

$$\phi(a) = ax + IQ.$$

The mapping ϕ is an O_K-module homomorphism, which, from equation 13.1, is surjective. Also,

$$\operatorname{Ker}\phi = \{a \in O_K : ax \in IQ\}.$$

We claim that $\operatorname{Ker}\phi = Q$. First,

$$\begin{aligned} ax \in IQ &\iff (a)(x) \subset IQ \\ &\iff (a)IJ \subset IQ \\ &\iff (a)J \subset Q, \end{aligned}$$

thus, for all $a \in \operatorname{Ker}\phi$,

$$(a) = (a)O_K = (a)(J+Q) = (a)J + (a)Q \subset Q + Q = Q.$$

This implies that $\operatorname{Ker}\phi \subset Q$. In addition, if $a \in Q$, then $ax \in IQ$, since $x \in I$, and so $Q \subset \operatorname{Ker}\phi$ and we have $\operatorname{Ker}\phi = Q$.

As ϕ is surjective, from the third isomorphism theorem for groups, we have

$$O_K/Q \simeq I/IQ \Longrightarrow \|Q\| = |I/IQ|$$

and

$$\|IQ\| = |O_K/IQ| = |O_K/I||I/IQ| = \|I\|\|Q\|.$$

This ends the proof. □

If K is a number field, with $[K:\mathbf{Q}] = n$ and I a nonzero ideal in O_K, then I is a free abelian group of rank n (Corollary 11.5). From a basis of I we may obtain an expression for the norm of I.

Theorem 13.3 *If $\mathcal{B} = \{b_1, \dots, b_n\}$ is a basis of I, then*

$$\|I\| = \left| \frac{disc_{K/\mathbf{Q}}(\mathcal{B})}{disc(O_K)} \right|^{\frac{1}{2}}.$$

PROOF From Theorem E.4, there exists a basis $\mathcal{E} = \{e_1, \dots, e_n\}$ of O_K and numbers $d_1, \dots, d_n \in \mathbf{N}^*$ such that $\mathcal{D} = \{d_1e_1, \dots, d_ne_n\}$ is a basis of I. We define a mapping ϕ of O_K onto $\mathbf{Z}_{d_1} \times \cdots \times \mathbf{Z}_{d_n}$ in the following way:

$$\text{if } x = x_1e_1 + \cdots + x_ne_n, \text{ then } \phi(x) = (x_1 + d_1\mathbf{Z}, \dots, x_n + d_n\mathbf{Z}).$$

The mapping ϕ is a ring homomorphism and $\operatorname{Ker}\phi = I$, hence

$$O_K/I \simeq \mathbf{Z}_{d_1} \times \cdots \times \mathbf{Z}_{d_n} \Longrightarrow |O_K/I| = d_1 \cdots d_n.$$

If we set $C = \operatorname{diag}(d_1, \dots, d_n)$, then C is the matrix transforming the basis $\mathcal{E}$ into the basis $\mathcal{D}$ and

$$|O_K/I| = \det C.$$

If $\mathcal{B} = \{b_1, \dots, b_1\}$ is any basis of I, then the b_i are linear combinations of the elements of $\mathcal{D}$ with integer coefficients. The matrix M transforming the basis $\mathcal{B}$ into the basis $\mathcal{D}$ thus has integer coefficients. This is also the case of the matrix N transforming the basis $\mathcal{D}$ into the basis $\mathcal{B}$. It follows that $\det M = \pm 1$ (and also that $\det N = \pm 1$). It follows that the matrix C'

expressing the basis $\mathcal{B}$ in terms of the elements of the basis $\mathcal{E}$ is such that $\det C' = \pm \det C$ and so

$$|O_K/I| = |\det C'| = d_1 \cdots d_n.$$

However, from Proposition 10.6,

$$\mathrm{disc}_{K/\mathbf{Q}}(\mathcal{B}) = |\det C'|^2 \mathrm{disc}_{K/\mathbf{Q}}(\mathcal{E}) = \|I\|^2 \mathrm{disc}(O_K),$$

from which we deduce

$$\|I\| = \left| \frac{\mathrm{disc}_{K/\mathbf{Q}}(\mathcal{B})}{\mathrm{disc}(O_K)} \right|^{\frac{1}{2}}.$$

This finishes the proof. □

If an ideal I of O_K is principal and $I = (a)$, then we consider two norms, namely the norm of the generator a and the norm of the ideal. In fact, we have

Theorem 13.4 *If $a \in O_K \setminus \{0\}$, then*

$$|N_{K/\mathbf{Q}}(a)| = \|(a)\|.$$

PROOF Let $\mathcal{E} = \{e_1, \ldots, e_n\}$ be a basis of O_K. Then $\mathcal{B} = \{ae_1, \ldots, ae_n\}$ is a basis of (a). Now

$$\begin{aligned}
\mathrm{disc}_{K/\mathbf{Q}}(\mathcal{B}) &= \big(\det(\sigma_i(ae_j))\big)^2 \\
&= \big(\det(\sigma_i(a)\sigma_i(e_j))\big)^2 \\
&= \big(\sigma_1(a)\cdots\sigma_n(a)\det(\sigma_i(e_j))\big)^2 \\
&= (\sigma_1(a)\cdots\sigma_n(a))^2(\mathrm{disc}(O_K)^2.
\end{aligned}$$

By Theorem 13.3, we have

$$\begin{aligned}
\|(a)\| &= \left| \frac{\mathrm{disc}_{K/\mathbf{Q}}(\mathcal{B})}{\mathrm{disc}(O_K)} \right|^{\frac{1}{2}} \\
&= |\sigma_1(a)\cdots\sigma_n(a)| \;=\; |N_{K/\mathbf{Q}}(a)|,
\end{aligned}$$

as required. □

We will now investigate further the properties of the norm.

Proposition 13.5 *Let K be a number field, O_K its associated number ring and I a nonzero ideal in O_K.*

- **a.** *If $\|I\|$ is prime, then I is a prime ideal.*
- **b.** $\|I\| \in I$.

PROOF **a.** If $I = P_1 \cdots P_s$, where the P_i are prime ideals, then

$$\|I\| = \|P_1\| \cdots \|P_s\|.$$

As $\|I\|$ is prime, only one P_i, say P_1, has a norm different from 1. This means that $P_2 = \cdots = P_s = O_K$ and so $I = P_1$.

b. If $A = \{\alpha_1, \ldots, \alpha_{\|I\|}\}$ is a complete set of residues modulo I; we claim that the set $B = \{1 + \alpha_1, \ldots, 1 + \alpha_{\|I\|}\}$ is also a complete set of residues modulo I. If $x \in O_K$, then $x - 1 = \alpha_j + y$, for some $1 \leq j \leq \|I\|$ and $y \in I$. From this we obtain $x = \alpha_j + 1 + y$, so the set $\bar{B} = \{(1 + \alpha_1) + I, \ldots, (1 + \alpha_{\|I\|}) + I\}$ covers O_K. In addition, if $(1 + \alpha_i) - (1 + \alpha_j) \in I$, then $\alpha_i - \alpha_j \in I$, which is impossible if $i \neq j$. This proves the claim. Then

$$\alpha_1 + \cdots + \alpha_{\|I\|} = (1 + \alpha_1) + \cdots + (1 + \alpha_{\|I\|}) \pmod{I},$$

which implies that $\|I\|1 \equiv 0 \pmod{I}$, and it follows that $\|I\| \in I$. □

Before going further we introduce a preliminary result.

Lemma 13.1 *A nonzero integer belongs to at most a finite number of ideals in O_K.*

PROOF Let a be a positive integer and suppose that I is an ideal containing a. We now let $\mathcal{B} = \{w_1, \ldots, w_n\}$ be an integral basis of O_K. If $\alpha \in O_K$, then there exist $c_1, \ldots, c_n \in \mathbf{Z}$ such that

$$\alpha = c_1 w_1 + \cdots + c_n w_n.$$

For each c_i we may write $c_i = aq_i + r_i$, where $q_i, r_i \in \mathbf{Z}$ and $0 \leq r_i < a$. Then

$$\alpha = (aq_1 + r_1)w_1 + \cdots + (aq_n + r_n)w_n = a(q_1 w_1 + \cdots + q_n w_n) + (r_1 w_1 + \cdots + r_n w_n) = a\gamma + \beta.$$

Clearly $\gamma \in O_K$ and $\beta \in B$, where B is a finite subset of O_K. The ideal I is finitely generated, because O_K is noetherian, so there exist $\alpha_1, \ldots, \alpha_s \in O_K$, such that

$$I = (\alpha_1, \ldots, \alpha_s).$$

As $a \in I$, we may also write

$$I = (\alpha_1, \ldots, \alpha_s, a)$$

and then

$$I = (a\gamma_1 + \beta_1, \ldots, a\gamma_s + \beta_s, a),$$

where $\gamma_1, \ldots, \gamma_s \in O_K$ and $\beta_1, \ldots \beta_s \in B$. It is not difficult to derive the expression

$$I = (\beta_1, \ldots, \beta_s, a).$$

As there is a finite number of ideals of this form, the result follows for the case $a > 0$.

If $a < 0$ and a belongs to an infinite number of ideals, then so does $-a$, which contradicts what we have just proved. This finishes the proof. □

We may now prove an interesting result concerning the number of ideals having a given norm.

Theorem 13.5 *There is only a finite number of ideals in O_K of a given norm.*

PROOF Suppose that there is an infinite number of ideals having the same norm α. From Proposition 13.5, α belongs to an infinite number of ideals, which contradicts Lemma 13.1. Therefore there can be only a finite number of ideals with a given norm. □

We now consider the special case where I is a prime ideal.

Proposition 13.6 *If P is a nonzero prime ideal in O_K, then P contains exactly one prime number p and $\|P\| = p^m$, for some natural number $m \leq n = [K : \mathbf{Q}]$.*

PROOF If P is a prime ideal, then P is maximal and so O_K/P is a finite field. It follows that $\|P\| = p^m$, for some prime number p and positive integer m. The characteristic of the field O_K/P is p, which implies that the number $p \in P$ and so the principal ideal $(p) = O_K p$ is contained in P. If $q \neq p$ and $q \in P$, then $(q) = O_K q$ is also contained in P. However, $(p) + (q) = O_K$, so $O_K \subset P$, which is impossible; hence there is a unique prime number p in P.

As (p) is a subset of P, P divides (p), hence $\|P\|$ divides $\|(p)\|$. From Theorem 13.4, $\|(p)\| = N_{K/\mathbf{Q}}(p) = p^n$, therefore $\|P\| = p^m$, with $m \leq n$. □

13.3 Principal theorem of ramification

Our goal in this section is to prove an important result connecting ramification indices and inertial degrees. We will refer to this as the principal theorem of ramification. We begin with a special case of this result and then generalize it.

Proposition 13.7 *Let p be a prime number and L an extension of $K = \mathbf{Q}$, with number field S. If $n = [L : \mathbf{Q}]$ and*

$$Sp = Q_1^{e(Q_1|p)} \cdots Q_s^{e(Q_s|p)}$$

is the decomposition of Sp into nonzero prime ideals, then

$$n = \sum_{i=1}^{s} f(Q_i|p)e(Q_i|p).$$

PROOF To simplify the notation, let us write e_i for $e(Q_i|p)$ and f_i for $f(Q_i|p)$. From Theorem 13.2 we have

$$\|Sp\| = \|Q_1\|^{e_1} \cdots \|Q_s\|^{e_s}.$$

Also,

$$f_i = [S/Q_i : \mathbf{Z}/p\mathbf{Z}] \Longrightarrow \|Q_i\| = p^{f_i},$$

therefore

$$\|Sp\| = p^{f_1 e_1} \cdots p^{f_1 e_1}.$$

However, from Theorem 13.4 and Section 10.1

$$\|Sp\| = |N_{L/\mathbf{Q}}(p)| = p^n,$$

so we have

$$n = \sum_{i=1}^{s} f(Q_i|p)e(Q_i|p),$$

as announced. □

We aim now to generalize this proposition to the case where K is not necessarily $\mathbf{Q}$. We will begin with a preliminary result.

Lemma 13.2 *Let I, J be nonzero ideals in a Dedekind domain D, with $J \subset I \neq D$, and K the field of fractions of D. Then there exists $\gamma \in K$ such that $\gamma J \subset D$ and $\gamma J \not\subset I$.*

PROOF From Theorem 12.2 we know that there is a nonzero ideal C in D such that JC is principal: $JC = (a)$. Then $JC \not\subset aI$, because

$$JC \subset aI \Longrightarrow \frac{1}{a}JC \subset I \Longrightarrow 1 \in I \Longrightarrow I = D,$$

a contradiction. We now take $b \in C$ such that $bJ \not\subset aI$ and set $\gamma = \frac{b}{a}$. Then

$$\gamma J = \frac{b}{a}J \subset \frac{1}{a}JC = \frac{1}{a}(a) = D.$$

If $\gamma J \subset I$, then $bJ \subset aI$, a contradiction, so $\gamma J \not\subset I$. □

We now establish another preliminary result. This is a little longer to prove.

Proposition 13.8 *Let $K \subset L$ be number fields, with corresponding number rings $R \subset S$, and I a nonzero ideal in R. Then*

$$\|SI\| = \|I\|^n,$$

where $n = [L : K]$.

PROOF It is sufficient to prove the result for a prime ideal: If this is the case and $I = P_1 \cdots P_r$ is the decomposition of the ideal I into prime ideals, then

$$\begin{aligned} \|SI\| &= \|P_1 \cdots P_r S\| \\ &= \|P_1 S \cdots P_r S\| \\ &= \|P_1 S\| \cdots \|P_r S\| \\ &= \|P_1\|^n \cdots \|P_r\|^n \\ &= \|P_1 \cdots P_r\|^n \ = \ \|I\|^n. \end{aligned}$$

So let us now establish the result for a nonzero prime ideal P.

To begin with, we notice that S/SP is a vector space over the field R/P. (The scalar multiplication is defined by

$$(x + P)(y + PS) = xy + SP.$$

There is no difficulty in seeing that this scalar multiplication is well-defined.) We claim that the dimension of the vector space we have defined is n. First we show that the dimension is at most n. Let $a_1, \ldots, a_{n+1} \in S$ and consider the corresponding cosets of S/SP. The a_i are linearly dependant over K, because they are elements of L and $n = [L : K]$. As K is the field of fractions of R, the a_i are linearly dependant over R. Hence we have

$$\beta_1 a_1 + \cdots + \beta_{n+1} a_{n+1} = 0,$$

with $\beta_i \in R$ and at least one β_i nonzero. We need to show that we can find $\beta'_1, \ldots, \beta'_{n+1} \in R$ such that

$$\beta'_1 a_1 + \cdots + \beta'_{n+1} a_{n+1} = 0,$$

and at least one $\beta'_i \notin P$. If one of the $\beta_i \notin P$, then we have nothing to do, so let us suppose that all the β_i belong to P. If J is the ideal generated by the β_i, then $J \subset P \neq R$. Applying Lemma 13.2 we obtain an element $\gamma \in K$ such that $\gamma J \subset R$ and $\gamma J \not\subset P$. If we replace β_i by $\beta'_i = \gamma\beta_i$, then the set of β'_i so obtained has the properties we were looking for. Thus we have shown that S/SP is at most n-dimensional over R/P.

Now we establish the equality. As $P \cap \mathbf{Z}$ is a nonzero ideal of $\mathbf{Z}$, there is a prime number $p \in \mathbf{Z}$ such that $P \cap \mathbf{Z} = \mathbf{Z}p$. We consider the prime ideals $P_1, \ldots, P_r$ of R lying over $\mathbf{Z}p$. From Proposition 13.1 P is one of the ideals P_i. From what we have just seen S/SP_i is a vector space over R/P_i of dimension $n_i \leq n$. Also, from Proposition 13.7 we have

$$m = \sum_{i=1}^{r} f(P_i|p)e(P_i|p) = \sum_{i=1}^{r} f_i e_i,$$

where $m = [K : \mathbf{Q}]$. Then

$$Rp = \prod_{i=1}^{r} P_i^{e_i} \Longrightarrow Sp = RSp = \left(\prod_{i=1}^{r} P_i^{e_i}\right) S = \prod_{i=1}^{r} (P_i S)^{e_i},$$

therefore

$$\|Sp\| = \prod_{i=1}^{r} \|SP_i\|^{e_i} = \prod_{i=1}^{r} \|P_i\|^{n_i e_i} = \prod_{i=1}^{r} (p^{f_i})^{n_i e_i}.$$

(The second equality follows from the fact that S/SP_i is a vector space over R/P_i of dimension $n_i \leq n$.)

On the other hand, we have

$$\|Sp\| = |N_{L/\mathbf{Q}}(p)| = p^{nm},$$

because

$$[L : \mathbf{Q}] = [L : K][K : \mathbf{Q}] = nm.$$

If there exists $n_i < n$, then

$$\sum_{i=1}^{r} f_i n_i e_i < n \left(\sum_{i=1}^{r} f_i e_i\right) = nm,$$

a contradiction. Hence $n_i = n$, for all P_i, in particular, for P. We have shown that the dimension of S/SP over R/P is n. If V is a vector space of dimension u over a finite field of s elements, then V has s^u elements. As S/SP has $\|SP\|$ elements and the dimension of S/SP over R/P is n, S/SP has $\|P\|^n$ elements, i.e., $\|SP\| = \|P\|^n$. This finishes the proof. □

We now prove the main theorem of this section, which we refer to as the *principal theorem of ramification.*

Theorem 13.6 *Let $K \subset L$ be number fields, with $[L : K] = n$, and R, S the corresponding number rings. We suppose that $Q_1, \ldots, Q_s$ are the nonzero prime ideals in S lying over the prime ideal P of R and we denote by $e_1, \ldots, e_s$ and $f_1, \ldots, f_s$ the corresponding ramification indices and inertial degrees. Then*

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

PROOF We have

$$SP = \prod_{i=1}^{s} Q_i^{e_i} \Longrightarrow \|SP\| = \prod_{i=1}^{s} \|Q_i\|^{e_i} = \prod_{i=1}^{s} \|P\|^{f_i e_i}.$$

Also,

$$\|SP\| = \|P\|^n,$$

therefore

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

This ends the proof. □

Example If L is a quadratique extension of $\mathbf{Q}$, with number field S, and p is a prime number, then there are three possible decompositions of pS into prime ideals:

$$Sp = \begin{cases} Q^2, & f(Q|p) = 1, \\ Q, & f(Q|p) = 2, \\ Q_1 Q_2, & f(Q_1|p) = f(Q_2|p) = 1. \end{cases}$$

13.4 Normal extensions

Let us now suppose that K and L are number fields, with L a normal extension of K. As char $\mathbf{Q} = 0$, L is separable over $\mathbf{Q}$. Using Proposition 3.5 we obtain that L is separable over K. Hence L is a Galois extension of K. As usual we set $R = O_K$ and $S = O_L$. If $x \in S$, then there exists a monic polynomial $f \in \mathbf{Z}[X]$ such that $f(x) = 0$. However, $\mathbf{Z} \subset R \subset K$, so the coefficients of f are fixed by any automorphism $\sigma \in Gal(L/K)$, which implies that $\sigma(x)$ is an algebraic number. Thus $\sigma(x) \in O_L = S$ and so $\sigma(S) \subset S$. In the same way, $\sigma^{-1}(S) \subset S$, which implies that $S \subset \sigma(S)$, hence $\sigma(S) = S$.

We now consider ideals in S. Let Q be an ideal in S. If $x, y \in Q$, $a \in S$ and $\sigma \in Gal(L/K)$, then

$$\sigma(x) - \sigma(y) = \sigma(x - y) \in \sigma(Q)$$

and

$$a\sigma(x) = \sigma(a')\sigma(x) = \sigma(a'x) \in \sigma(Q),$$

where $a' = \sigma^{-1}(a) \in S$. Therefore $\sigma(Q)$ is an ideal of S.

Suppose now that Q is a prime ideal in S. If $x, y \in S$ and $xy \in \sigma(Q)$, then

$$\begin{aligned} \sigma^{-1}(xy) \in Q &\implies \sigma^{-1}(x)\sigma^{-1}(y) \in Q \\ &\implies \sigma^{-1}(x) \in Q \text{ or } \sigma^{-1}(y) \in Q \\ &\implies x \in \sigma(Q) \text{ or } y \in \sigma(Q). \end{aligned}$$

As $\sigma(Q) \neq S$, $\sigma(Q)$ is a prime ideal.

If Q is a prime ideal in S lying over the prime ideal P in R, then

$$Q \supset SP \Longrightarrow \sigma(Q) \supset \sigma(SP) = \sigma(S)\sigma(P) = S\sigma(P).$$

Since $P \subset R \subset K$, $\sigma(P) = P$, so $\sigma(Q)$ lies over P. Thus we obtain an action ϕ of the group $Gal(L/K)$ on the set $\mathcal{Q}$ of nonzero prime ideals Q lying over the prime ideal P:

$$\phi : Gal(L/K) \times \mathcal{Q} : (\sigma, Q) \longmapsto \sigma(Q).$$

In fact, due to the normality of the extension L/K, this action is transitive:

Theorem 13.7 *If Q and Q' are nonzero prime ideals in S lying over the prime ideal P in R, then there exists $\sigma \in Gal(L/K)$ such that $\sigma(Q) = Q'$.*

PROOF If this is not the case, then $\sigma(Q) \neq Q'$, for all $\sigma \in G = Gal(L/K)$. Let us suppose that $\sigma_1(Q), \ldots, \sigma_s(Q)$ are the distinct images of Q under $G = Gal(L/K)$. (We may assume that $\sigma_1 = \mathrm{id}_L$, so $Q = \sigma_1(Q)$.) The prime ideals $Q', \sigma_1(Q), \ldots, \sigma_s(Q)$ are coprime in pairs. By the Chinese remainder theorem (Theorem F.1), there is a solution $a \in S$ of the system of congruences

$$\begin{array}{rcl} x & \equiv & 0 \pmod{Q'} \\ x & \equiv & 1 \pmod{\sigma_1(Q)} \\ \vdots & \vdots & \vdots \\ x & \equiv & 1 \pmod{\sigma_s(Q)}. \end{array}$$

Let us now consider $N_{L/K}(a)$. Corollary 10.3 ensures that

$$N_{L/K}(a) = \prod_{\sigma \in G} \sigma^{-1}(a).$$

Since $\mathrm{id}_L \in G$ and $\sigma^{-1}(a) \in S$, we have

$$N_{L/K}(a) \in K \cap Q' = Q' \cap R.$$

As Q' lies over P, $N_{L/K}(a) \in P$.

On the other hand, $\sigma^{-1}(a) \notin Q$, for every $\sigma \in G$. Given that Q is a prime ideal, $N_{L/K}(a) \notin Q$, which is a contradiction, because $P \subset SP \subset Q$ □

Corollary 13.2 *Let K and L be number fields with corresponding number rings R and S. If L is a normal extension of K, P a nonzero prime ideal in R and Q, Q' nonzero prime ideals in S lying over P, then*

$$e(Q|P) = e(Q'|P) \qquad \text{and} \qquad f(Q|P) = f(Q'|P).$$

PROOF We may write

$$SP = Q^{e_1} Q'^{e_2} Q_3^{e_3} \cdots Q_s^{e_s},$$

where $e_1 = e(Q|P)$, $e_2 = e(Q'|P)$, $Q_3, \ldots, Q_s$ are the other prime ideals lying over P and $e_i = e(Q_i|p)$, for $i = 3, \ldots, s$. There exists $\sigma \in Gal(L/K)$ such that $\sigma(Q) = Q'$. We have

$$SP = \sigma(PS) = \sigma(Q)^{e_1} \sigma(Q')^{e_2} \sigma(Q_3)^{e_3} \cdots \sigma(Q_s)^{e_s} = Q'^{e_1} \sigma(Q')^{e_2} \sigma(Q_3)^{e_3} \cdots \sigma(Q_s)^{e_s}.$$

However, we also have

$$SP = Q^{e_1} Q'^{e_2} Q_3^{e_3} \cdots Q^{e_s}$$

As Q is the only prime ideal whose image under σ is Q' and the decomposition of SP into prime ideals is unique, we must have

$$Q'^{e_2} = Q'^{e_1} \Longrightarrow e_2 = e_1.$$

Now we show that $f(Q|P) = f(Q'|P)$. There exists $\sigma \in Gal(L/K)$ such that $\sigma(Q) = Q'$. The mapping σ restricted to S is a ring automorphism. We set $\phi = \pi \circ \sigma_{|S}$, where π is the projection of S onto S/Q'. Then

$$\operatorname{Ker} \phi = \{x \in S : \sigma(x) \in Q'\} = Q.$$

Hence

$$S/Q \simeq S/Q'.$$

and

$$[S/Q' : R/P] = [S/Q' : S/Q][S/Q : R/P] = [S/Q : R/P],$$

i.e.,

$$f(Q'|P) = f(Q|P),$$

as announced. $\square$

Remark From Corollary 13.2 , if L is a normal extension of K and P is a nonzero prime ideal in R, then

$$SP = (Q_1 \dots Q_s)^e,$$

where e is the common ramification index of the prime ideals in S lying over P.

Example The cyclotomic field $\mathbf{Q}(\mu_n)$ is a normal extension of $\mathbf{Q}$, because $\mathbf{Q}(\mu_n)$ is the splitting field of the minimal polynomial $m(\mu_n, \mathbf{Q})$. If p is a prime number and $Q_1, \dots, Q_s$ are the prime ideals in $S = O_{\mathbf{Q}(\mu_n)}$ which lie over p, then $Sp = (Q_1, \cdots Q_s)^e$, where e is the common ramification index of the ideals Q_i.

13.5 Ramified prime ideals

Let $R \subset S$ be number rings, with respective number fields K and L. We say that a prime ideal P in R is *ramified* in S, if $e(Q|P) > 1$ for some prime ideal Q in S lying over P. This amounts to saying that SP is not squarefree. If p is a prime number, then we say that p is ramified in S, if $e(Q|p) > 1$, for some prime ideal Q lying over (p). A prime ideal (resp. prime number) is unramified in S, if it is not ramified in S. It may occur that $e(Q|P) = n$ (resp. $e(Q|p) = n$), where $[L : K] = n$; in this case we say that P (resp. p) is *totally ramified* in S.

We recall that all integral bases of a number ring R have the same discriminant, which we note $\mathrm{disc}(R)$. We have seen that $\mathrm{disc}(R) \in \mathbf{Z}$. The discriminant of a number ring R helps us to determine whether a prime number p is ramified in R.

Theorem 13.8 *Let L be an extension of $\mathbf{Q}$ of degree n. If $S = O_L$ and $p \in \mathbf{Z}$ a prime ramified in S, then $p|disc(S)$.*

PROOF Let Q be a prime ideal in S lying over p such that $e(Q|p) > 1$. Then

$$Sp = QI,$$

where I is an ideal of S divisible by all prime ideals lying over p. We note $\sigma_1, \dots, \sigma_n$ the $\mathbf{Q}$-monomorphisms of L into an algebraic closure C of $\mathbf{Q}$. (We may take the set of algebraic numbers $A(\mathbf{C}/\mathbf{Q})$ for C.) From Section 5.1 we know that there is a finite extension N of L which is normal over $\mathbf{Q}$. Now, using Theorem 3.2, we extend each σ_i to a monomorphism $\bar{\sigma}_i$ from N into C. As N is a normal extension of $\mathbf{Q}$, from Proposition 5.2 we have $\bar{\sigma}_i(N) = N$ and so $\bar{\sigma}_i$ is an automorphism of N.

Let $\alpha_1, \dots, \alpha_n$ be an integral basis of S and take $\alpha \in I \setminus Sp$; α belongs to every prime ideal of S lying over p. We may write

$$\alpha = m_1\alpha_1 + \cdots + m_n\alpha_n,$$

with $m_i \in \mathbf{Z}$. If $p|m_i$, for all i, then $\alpha \in pS$, a contradiction, so there exists an m_i such that $p \not| m_i$. Without loss of generality, let us suppose that $i = 1$; then $p \not| m_1$. We set

$$d = \mathrm{disc}(S) = \mathrm{disc}_{L/\mathbf{Q}}(\alpha_1, \dots, \alpha_n).$$

Then, using Exercise 10.2 we see that

$$\mathrm{disc}_{L/\mathbf{Q}}(\alpha, \alpha_2, \ldots, \alpha_n) = m_1^2 d.$$

As $p \not| m_1$, to show that $p|d$ it is sufficient to prove that $p|\mathrm{disc}(\alpha, \alpha_2, \ldots, \alpha_n)$. This we will now do.

As α belongs to every prime ideal in S lying over p, α must lie in every prime ideal in $T = O_N$ lying over p: If $\tilde{Q}$ is such a prime ideal, then $\tilde{Q} \supset Tp$ and so $p \in \tilde{Q}$; if we set $Q = \tilde{Q} \cap S$, then Q is a prime ideal in S lying over p, so $\alpha \in Q \subset \tilde{Q}$. We now fix a prime ideal $\tilde{Q}$ in T lying over p; we claim $\bar{\sigma}(\alpha) \in \tilde{Q}$ for every $\mathbf{Q}$-automorphism $\bar{\sigma}$ of N. We notice first that $\bar{\sigma}^{-1}(\tilde{Q})$ is a prime ideal in T lying over p, hence $\alpha \in \bar{\sigma}^{-1}(\tilde{Q})$. It follows that $\bar{\sigma}_i(\alpha) \in \tilde{Q}$, for $i = 1, \ldots, n$. Since C is an algebraic closure of L, from the definition of the discriminant we see that $\mathrm{disc}_{L/\mathbf{Q}}(\alpha, \alpha_2, \ldots, \alpha_n) \in \tilde{Q}$. However, the discriminant is an integer, so $\mathrm{disc}_{L/\mathbf{Q}}(\alpha, \alpha_2, \ldots, \alpha_n) \in \tilde{Q} \cap \mathbf{Z} = \mathbf{Z}p$. Therefore $p|\mathrm{disc}_{L/\mathbf{Q}}(\alpha, \alpha_2, \ldots, \alpha_n)$. □

Exercise 13.3 *Consider the quadratic number field $K = \mathbf{Q}(\sqrt{d})$, where d is squarefree. Show that if an odd prime number p is ramified in the number ring O_K, then p divides d.*

Corollary 13.3 *Only finitely many primes in $\mathbf{Z}$ are ramified in a given number ring S.*

PROOF The discriminant of S has only a finite number of prime divisors. □

We may extend this result.

Corollary 13.4 *Let R and S be number rings, with $R \subset S$. Then only a finite number of prime ideals in R are ramified in S.*

PROOF Let P be a prime ideal in R which is ramified in S. Then there exists a prime ideal Q in S which lies over P and is such that $e(Q|P) > 1$. However, the prime ideal P lies over a unique prime number $p \in \mathbf{Z}$ (Theorem 13.1). From Proposition 13.3, we have

$$e(Q|p) = e(Q|P)e(P|p) > 1.$$

Corollary 13.3 states that there is only a finite number of such primes p. Now, each such prime lies under a finite number of prime ideals in R (Theorem 13.1) and the result follows. □

13.6 Decomposition and inertia groups

Let K and L be number fields, with L normal over K. As L is a Galois extension of K, we have $n = [L : K] = |Gal(L/K)|$. Let R and S be the number rings of K and L respectively, i.e., $R = O_K$ and $S = O_L$, and P a prime ideal in R. All the prime ideals Q lying over P have the same ramification index e and inertia degree f. If there are r such prime ideals, then $n = ref$. For each prime ideal Q lying over P we define two subgroups of $G = Gal(L/K)$:

- the decomposition group
  $D = D(Q|P) = \{\sigma \in G : \sigma(Q) = Q\}$
- the inertia group
  $E = E(Q|P) = \{\sigma \in G : \sigma(\alpha) \equiv \alpha (\mathrm{mod}\ Q),\ \forall \alpha \in S\}$

It is clear that D and E are subgroups of G. Also, E is a subgroup of D: for all $\sigma \in E$, we have

$$\sigma(\alpha) \equiv \alpha (\bmod Q),\ \forall \alpha \in S \Longrightarrow \sigma(\alpha) \equiv \alpha (\bmod Q),\ \forall \alpha \in Q \Longrightarrow \sigma(Q) \subset Q.$$

As E is a subgroup of G, $\sigma^{-1} \in E$, so we also have

$$\sigma^{-1}(Q) \subset Q \Longrightarrow Q \subset \sigma(Q).$$

Therefore

$$\sigma(Q) = Q.$$

The members σ of D induce elements $\bar{\sigma}$ of the Galois group $\bar{G} = Gal(S/Q/R/P)$ in a natural way. If we restrict $\sigma \in G$ to S, then we obtain an automorphism $\sigma_{|S}$ of S. We now set $\phi = \pi \circ \sigma_{|S}$, where π is the projection of S onto S/Q. As

$$\operatorname{Ker} \phi = \{\alpha \in S : \sigma(\alpha) \in Q\} = Q,$$

the mapping

$$\bar{\sigma} : S/Q \longrightarrow S/Q, \alpha + Q \longmapsto \sigma(\alpha) + Q$$

is an automorphism. In addition, $\bar{\sigma}$ fixes R/P, so $\bar{\sigma} \in \bar{G} = Gal(S/Q, R/P)$.

It is not difficult to see that the mapping

$$\psi : D \longrightarrow \bar{G}, \sigma \longmapsto \bar{\sigma}$$

is a group homomorphism, whose kernel is E. It follows that E is a normal subgroup of D and D/E is isomorphic to a subgroup of $\bar{G}$. However, from Proposition 13.10 proved below, $[L^E : L^D] = f = [S/Q, R/P]$ and $[S/Q, R/P] = |\bar{G}|$, because S/Q is a Galois extension of R/P, being a finite extension of a finite field, hence $[L^E : L^D] = |\bar{G}|$. In addition, $[L^E : L^D] = |D/E|$, so $|D/E| = |\bar{G}|$ and it follows that the groups D/E and $\bar{G}$ are isomorphic. From Theorem 7.9 the group $\bar{G}$ is cyclic (and generated by the Frobenius automorphism $Fr : \bar{x} \longmapsto \bar{x}^q$, where $q = |R/P|$), which implies that D/E is also cyclic.

Exercise 13.4 *If $P \subset R$ is a prime ideal, then there is a finite number of ideals $Q_1, \ldots, Q_r \subset S$ lying over P. Corresponding to each Q_i is a decomposition group D_i and an inertia group E_i. Show that the decomposition (resp. inertia) groups are conjugate in the Galois group $Gal(L/K)$, if L is a normal extension of K. Deduce that, if the Galois group is abelian, then there is only one decomposition (resp. inertia) group.*

We now consider the fixed fields L^D and L^E, called respectively the *decomposition field* and *inertia field*. We have the relations

$$K \subset L^D \subset L^E \subset L$$

and

$$R = O_K \subset S^D \subset S^E \subset S,$$

where $S^D = O_{L^D}$ and $S^E = O_{L^E}$. We also introduce two other prime ideals, namely Q^D and Q^E, where Q^D (resp. Q^E) is the unique prime ideal in S^D (resp. S^E) lying under Q. Then

$$P \subset Q^D \subset Q^E \subset Q.$$

We aim now to consider the relation between the fields K, L, L^D and L^E, in particular, to determine $[L^D : K]$, $[L^E : L^D]$ and $[L : L^D]$.

Proposition 13.9 *We have*

$$[L^D : K] = r.$$

PROOF We define a mapping ϕ from the set of left cosets of D into the set of prime ideals over P in S by

$$\phi(\sigma D) = \sigma(Q).$$

We have

$$\sigma(Q) = \tau(Q) \Longleftrightarrow \tau^{-1}\sigma(Q) = Q \Longleftrightarrow \tau^{-1}\sigma \in D \Longleftrightarrow \sigma D = \tau D,$$

therefore ϕ is well-defined and injective. From Theorem 13.7 ϕ is also surjective, so ϕ is a bijection. There are r prime ideals lying over P, so $[G : D] = r$. However, from Theorem 6.6 $[L^D : K] = [G : D]$, hence $[L^D : K] = r$. □

Using the multiplicativity of the degree, we obtain

Corollary 13.5 *The degree*

$$[L : L^D] = ef.$$

Our next task is to show that $[L^E : L^D] = f$. To do so we need some preliminary results.

Lemma 13.3 *We have*

$$f(Q|Q^E) = 1.$$

PROOF Since S/Q is a Galois extension of the finite field S^E/Q^E, it is sufficient to prove that the Galois group $\bar{G} = Gal(S/Q/S^E/Q^E)$ is reduced to the identity. We take $\theta \in S/Q$ and consider the polynomial

$$f(X) = (-\theta + X)^m \ \in \ S/Q\,[X],$$

where $m = |E|$. We claim that the coefficients of f belong to the subring of S/Q

$$S_1 = \{a + Q : a \in S^E\}.$$

To see this, first we notice that there exists $\alpha \in S$ such that $\theta = \alpha + Q$. We set

$$g(X) = \prod_{\sigma \in E} (-\sigma(\alpha) + X) \ \in \ L[X].$$

In fact, $g \in S^E[X]$: The coefficients of g are fixed by any element $\sigma \in E$, so they belong to L^E; in addition, as $\alpha \in S$, $\sigma(\alpha) \in S$, for all $\sigma \in E$, hence the coefficients of g belong to S; it follows that the coefficients of g belong to $L^E \cap S = S^E$. If we now consider the coefficients of g modulo Q, then we obtain a polynomial $\bar{g}$ with coefficients in S_1. However, this polynomial is precisely f, hence the coefficients of f belong to S_1, as claimed.

Now we consider the ring homomorphism

$$\psi : S^E \longrightarrow S_1, x \longmapsto x + Q.$$

The kernel of this mapping is $S^E \cap Q = Q^E$, hence $S^E/Q^E \simeq S^E/Q$. Therefore we may consider that the coeffiients of f belong to S^E/Q. If $\sigma \in \bar{G}$, then σ fixes the coefficients of f, so $\sigma(\theta)$ is a root of f. As f has the unique root θ, we must have $\sigma(\theta) = \theta$. We have shown that the only element in $\bar{G}$ is the identity, as required. □

The prime ideal Q lies over Q^D. This is the unique prime ideal in S with this property: Theorem 6.7 ensures that L is a finite Galois extension of L^D. If Q' lies over Q^D, then there exists $\sigma \in Gal(L/L^D)$, such that $\sigma(Q) \subset Q'$ (Theorem 13.7). However, Theorem 6.7 also ensures that $Gal(L/L^D) = D$, so $Q = \sigma(Q) \subset Q'$, which implies that $Q = Q'$. We will use this observation to obtain our second preliminary result.

Lemma 13.4 *We have*
$$e(Q^D|P) = f(Q^D|P) = 1.$$

PROOF First we notice that
$$ef = [L : L^D] = e(Q|Q^D)f(Q|Q^D),$$
because Q is the unique ideal in S lying over Q^D. Also,
$$e = e(Q|P) = e(Q|Q^D)e(Q^D|P) \Longrightarrow e(Q|Q^D) \leq e.$$
In the same way,
$$f(Q|Q^D) \leq f.$$
Hence
$$e(Q|Q^D) = e \qquad \text{and} \qquad f(Q|Q^D) = f$$
and it follows that
$$e(Q^D|P) = f(Q^D|P) = 1,$$
as claimed. □

The third preliminary result is the following:

Corollary 13.6 *For Q^E and Q^D we have*
$$f(Q^E|Q^D) = f.$$

PROOF Using the multiplicativity of the inertial degree, we obtain
$$f(Q|P) = f(Q|Q^E)f(Q^E|Q^D)f(Q^D|P) \Longrightarrow f = 1f(Q^E|Q^D)1 = f(Q^E|Q^D).$$
The result now follows from Lemma 13.3 and Lemma 13.4. □

Now we are in a position to consider $[L^E : L^D]$

Proposition 13.10 *We have*
$$[L^E : L^D] = f.$$

PROOF As Q^E lies over Q^D, from Theorem 13.6 we have
$$[L^E : L^D] \geq e(Q^E|Q^D)f(Q^E|Q^D).$$
and then, using Corollary 13.6, we obtain
$$[L^E : L^D] \geq f.$$
We have seen that L is a Galois extension of L^D, with $D = Gal(L/L^D)$, and that E is a normal subgroup of D, with D/E embedded in $\bar{G} = Gal(S/Q, R/P)$. Then Theorem 6.4 ensures that $E = Gal(L/L^E)$; in addition, from Theorem 6.6 we obtain that L^E is a Galois extension of L^D and D/E is isomorphic to $Gal(L^E/L^D)$. From this we deduce
$$[L^E : L^D] = |Gal(L^E/L^D)| = |D/E| \leq |\bar{G}|.$$
Moreover, $|\bar{G}| = f$, because S/Q is a finite extension of the finite field R/P and thus a Galois extension. This finishes the proof. □

We can now easily obtain $[L : L^E]$. In fact,

Proposition 13.11

$$[L : L^E] = e.$$

PROOF We have

$$ef = [L : L^D] = [L : L^E][L^E : L^D] = [L : L^E]f$$

and the result follows. □

13.7 Optimal properties of L^D and L^E

Let K and L be number fields with L normal over K. The prime ideal Q lies over Q^D. This is the unique such prime ideal in S with this property: If Q' is such a prime ideal, then there exists $\sigma \in Gal(L^D)$ such that $\sigma(Q) = Q'$. However, we have seen that $Gal(L/L^D) = D$, so $Q' = Q$. This suggests the following question: If K' is a field intermediate between K and L, is there a prime ideal $Q' \subset R' = O_{K'}$ such that Q is the unique prime ideal of S lying over Q'? We claim that any such field must contain L^D, or, in other words, L^D is the smallest intermediate field with this property.

Theorem 13.9 *Let L be a normal extension of K. If K' is a field intermediate between K and L and there is a prime ideal $Q' \subset R'$ such that Q is the unique prime ideal of S lying over Q', then $L^D \subset K'$.*

PROOF If K' is an intermediate field between K and L, then there is a subgroup H of $Gal(L/K)$ such that $K' = L^H$. Suppose that Q is the unique prime ideal lying over Q'. Every element $\sigma \in H$ sends Q to a prime ideal lying over Q'. As there is only one such prime ideal, $H \subset D$, which implies that $L^D \subset L^H = K'$. □

We are going to consider another property of L^D, but, before doing so, we must do some preliminary work. We suppose that K' is an intermediate field between K and L. From Proposition 5.3, L is a normal (hence Galois) extension of K'. We now set $R' = O_{K'}$ and $Q' = Q \cap R'$. Then Q' is the unique prime ideal in R' lying under Q. Also, Q' lies over P. We aim to replace K by K'. We set

$$D' = D(Q|Q') \qquad \text{and} \qquad E' = E(Q|Q').$$

There is a subgroup H of the Galois group $Gal(L/K)$ such that $K' = L^H$. We have

$$D' = \{\sigma \in Gal(L/L^H) : \sigma(Q) = Q\} = \{\sigma \in H : \sigma(Q) = Q\} = D \cap H$$

and

$$\begin{aligned} E' &= \{\sigma \in Gal(L/L^H) : \sigma(\alpha) = \alpha (\text{mod } Q),\ \forall \alpha \in S\} \\ &= \{\sigma \in H : \sigma(\alpha) = \alpha (\text{mod } Q),\ \forall \alpha \in S\} \\ &= E \cap H. \end{aligned}$$

Now, from Theorem 6.9, $L^{D'} = L^D K'$ and $L^{E'} = L^E K'$.

We now consider the property of L^D referred to above. We restate Lemma 13.4 as a proposition:

Proposition 13.12

$$e(Q^D|P) = f(Q^D|P) = 1.$$

This proposition suggests the following question: If K' is a field intermediate between K and L and there is a prime ideal $Q' \subset R' = O_{K'}$ such that

$$e(Q'|P) = f(Q'|P) = 1,$$

what can we say about the relation between K' and L^D? We claim that L^D must contain such a field, or, in other words, L^D is the largest intermediate field with this property.

Theorem 13.10 *Let K and L be number fields with L normal over K. If K' is a field intermediate between K and L such that the prime ideal Q' in $R' = O_{K'}$ lying under Q has the property*

$$e(Q'|P) = f(Q'|P) = 1,$$

then $K' \subset L^D$.

PROOF Since Q lies over Q' and Q' over P, we notice that

$$e = e(Q|Q')e(Q'|P) = e(Q|Q') \qquad \text{and} \qquad f = f(Q|Q')f(Q'|P) = f(Q|Q').$$

Therefore, since L is a normal extension of K' (Proposition 5.3), from Corollary 13.5,

$$[L : L^{D'}] = e(Q|Q')f(Q|Q') = ef = [L : L^D].$$

However, $L^D \subset L^{D'}$, which implies that $L^D = L^{D'} = L^D K'$ and so $K' \subset L^D$. This ends the proof. □

We now turn to a property of L^E.

Proposition 13.13 *We have*

$$e(Q^E|P) = 1.$$

PROOF We notice that

$$e(Q|P) = e(Q^E|Q^D)e(Q^D|P) = e(Q^E|Q^D),$$

from Proposition 13.12. It remains to show that $e(Q^E|Q^D) = 1$. This can be derived from Corollary 13.6 and Proposition 13.10. We have

$$f = [L^E : L^D] = e(Q^E|Q^D)f(Q^E|Q^D) = e(Q^E|Q^D)f$$

hence $e(Q^E|Q^D) = 1$. □

This property suggests the following question: If K' is a field intermediate between K and L and there a prime ideal $Q' \subset R' = O_{K'}$ such that

$$e(Q'|P) = 1,$$

what can we say about the relation between K' and L^E? We have seen that $K' \subset L^D$. We claim that L^E must contain any intermediate field containing K', or, in other words, L^E is the largest intermediate field with this property.

Theorem 13.11 *Let K and L be number fields with L normal over K. If K' is a field intermediate between K and L and the prime ideal Q' of $R' = O_{K'}$ lying under Q is such that*

$$e(Q'|P) = 1,$$

then $K' \subset L^E$.

PROOF We will use a procedure analogous to that used in the proof of Theorem 13.10. As in the proof of this theorem, we obtain $e(P'|P) = 1$ and $e = e(Q|Q')$, where $P' = Q \cap R'$. However, since L is a normal extension of K' (Proposition 5.3), using Proposition 13.11 we obtain

$$[L : L^{E'}] = e(Q|Q') = e = [L : L^E].$$

Because $L^E \subset L^{E'}$, we have the equality $L^E = L^{E'} = L^E K'$, thus $K' \subset L^E$. This ends the proof. $\square$

Remark It is interesting to compare Theorems 13.10 and 13.11. In the first case we obtain $K' \subset L^D$, which is stronger than $K' \subset L^E$, the result obtained in the second case, because $L^D \subset L^E$.

Non-ramification and complete splitting in composita

Let K, L be number fields, with L an extension (not necessarily normal) of K, and R and S the corresponding number rings. If P is a nonzero prime ideal in R, then we say that P *splits completely in* S, if PS can be written as a product of $n = [K : L]$ distinct prime ideals in S. From Theorem 13.6 we have

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

Clearly, if $e_i = f_i = 1$, for all i, then P splits completely in S.

We can compare this notion with that of non-ramification. If the ideal P splits completely in S, then P is unramified in S. However, the converse is false: We may have

$$SP = Q_1 \cdots Q_s,$$

with $s < n$ and certain $f_i > 1$. Non-ramification is thus weaker than complete splitting. In the following, if F and G are number fields, with $F \subset G$, and Q is an ideal in O_G, then we will write Q_F for $Q \cap O_F$, the unique prime ideal of O_F lying under Q. If Q is a prime ideal, then so is Q_F. (It should be noticed that $Q^D = Q_{L^D}$ and $Q^E = Q_{L^E}$.)

Theorem 13.12 *Let K, L and M be number fields, with L and M extensions of K, and P a nonzero prime ideal in O_K which is unramified (resp. splits completely) in O_L and O_M. Then P is unramified (resp. splits completely) in O_{LM}.*

PROOF We first consider the non-ramification. Suppose that P is a nonzero prime ideal which is unramified in O_L and O_M and Q' a prime ideal in O_{LM} lying over P. We must show that $e(Q'|P) = 1$. As LM is a finite extension of K, there exists a finite normal extension N of K containing LM (see Section 5.1). Let Q be a prime ideal in O_N lying over Q'. Proposition 13.3 ensures that Q also lies over P. We note E the inertia group $E(Q|P)$, i.e.,

$$E(Q|P) = \{\sigma \in Gal(N/K) : \sigma(\alpha) \equiv \alpha (\text{mod } Q),\ \forall \alpha \in O_N\}.$$

As $Q_L \cap O_K = P$ and $Q_M \cap O_K = P$, Q_L and Q_M lie over P. Given that Q_L and P_L are unramified over P, we have

$$e(Q_L|P) = e(Q_M|P) = 1.$$

From Theorem 13.11 N^E contains both L and M and hence LM. As Q is a prime ideal, so is Q_{N^E}. Then, using Proposition 13.14, we have

$$1 = e(Q_{N^E}|P) = e(Q_{N^E}|Q_{LM})e(Q_{LM}|P).$$

This implies that $e(Q_{LM}|P) = 1$, i.e., $e(Q'|P) = 1$.

We now consider the complete splitting. As we have seen, the nonzero prime ideal P in O_K splits completely in O_{LM} if and only if , for every prime ideal Q' in O_{LM} lying over P, we have $e(Q'|P) = f(Q'|P) = 1$. As above we take a prime ideal Q' in O_{LM}, let N be a finite normal extension of K containing LM and Q be a prime ideal in N lying over Q'. Once again, Q also lies over P. We note D the decomposition group $D(Q|P)$, i.e.,

$$D(Q|P) = \{\sigma \in Gal(N/K) : \sigma(Q) = Q\}.$$

We define Q_L and Q_M as above and so Q_L and Q_M lie over P. As P splits completely in O_L and O_M, we have

$$e(Q_L|P) = f(Q_L|P) = 1 \qquad \text{and} \qquad e(Q_M|P) = f(Q_M|P) = 1.$$

From Theorem 13.10, N^D contains both L and M, hence LM. Then, by Proposition 13.12

$$1 = e(Q_{N^D}|P) = e(Q_{N^D}|Q_{LM})e(Q_{LM}|P) \quad \text{and} \quad 1 = f(Q_{N^D}|P) = f(Q_{N^D}|Q_{LM})f(Q_{LM}|P),$$

and so

$$e(Q_{LM}|P) = f(Q_{LM}|P) = 1, \quad \text{i.e.,} \quad e(Q'|P) = f(Q'|P) = 1.$$

This finishes the proof. □

Exercise 13.5 *In the preceeding proof, we take the normal closure N of K over LM. What is the reason for doing so?*

Corollary 13.7 *Let K and L be number fields, with $K \subset L$, and P a nonzero prime ideal in O_K. If P is unramified or splits completely in O_L, then the same is true in a normal closure N of L over K.*

PROOF Let P be a nonzero prime ideal in O_K. We first suppose that P is unramified in O_L. We must show that, if Q is a nonzero prime ideal in O_N lying over P, then $e(Q|P) = 1$. If $\sigma \in Gal(N/K)$, then we have

$$O_L P = Q_1' \cdots Q_s' \Longrightarrow P\sigma(O_L) = \sigma(Q_1') \cdots \sigma(Q_s'),$$

which means that P is unramified in $O_{\sigma(L)}$. However, from Theorem 6.12, we know that

$$N = \prod_{\sigma \in Gal(N/K)} \sigma(L).$$

Applying Theorem 13.12 successively we obtain that P is unramified in O_N.

We use an analogous argument to show that, if P splits completely in L, then P splits completely in O_N. □

A criterion for complete splitting

We begin with a preliminary result.

Proposition 13.14 *Let K, L be number fields, with L a normal extension of K. We suppose that P is a prime ideal in O_K and Q a prime ideal in O_L lying over P. In addition, we assume that the decomposition group $D = D(Q|P)$ is normal in $G = Gal(L/K)$. If r is the number of distinct prime ideals in the splitting of P in O_L, then P splits into r prime ideals in O_{L^D}.*

PROOF Since D is normal in G, the corresponding field L^D is a normal extension of K. From Lemma 13.4 we have

$$e(Q^D|P) = f(Q^D|P) = 1.$$

Thus, using Corollary 13.2, for every prime ideal $\bar{P}$ in O_{L^D} lying over P

$$e(\bar{P}|P) = f(\bar{P}|P) = 1.$$

If $\bar{r}$ is the number of distinct prime ideals $\bar{P}_i$ in the splitting of P in O_{L^D}, then

$$\sum_{i=1}^{\bar{r}} e(\bar{P}_i|P)f(\bar{P}_i|P) = [L^D : K],$$

i.e., $\bar{r} = [L^D : K]$. However, from Proposition 13.9 we know that $[L^D : K] = r$, so $\bar{r} = r$ as claimed. □

Theorem 13.13 *Let Q be any ideal in O_L lying over the prime ideal P of O_K. Let us assume the conditions of Proposition 13.14 and let K' be an intermediate field between K and L. Then P splits completely in $O_{K'}$ if and only if $K' \subset L^{D(Q|P)}$.*

PROOF If P splits completely in $O_{K'}$, then

$$e(Q'|P) = f(Q'|P) = 1, \tag{13.2}$$

where Q' is the unique ideal of $O_{K'}$ lying under Q. (Q' lies over P and the relation (13.2) follows directly from the definition of complete splitting.) By Theorem 13.10 we have $K' \subset L^D$.

Now suppose that $K' \subset L^{D(Q|P)}$. As in the proof of Proposition 13.14, Lemma 13.4 and Corollary 13.2 ensure that P splits completely in $O_{L^{D'}}$. If P' is a prime ideal in $O_{K'}$ lying over P, then P' lies under some prime ideal $\bar{P}$ in O_{L^D} lying over P. We have

$$e(\bar{P}|P) = f(\bar{P}|P) = 1 \Longrightarrow e(P'|P) = f(P'|P) = 1,$$

Hence P splits completely in $O_{K'}$. □

13.8 Existence of ramified prime numbers

In this section our goal is to establish a necessary and sufficient condition for the existence of a ramified prime number in a given number ring. We have already seen that, if p is a prime number which is ramified in a number ring $R = O_K$, then p divides disc(R) (Theorem 13.8). We aim to show that this condition is also sufficient.

Theorem 13.14 *Let K be a number field and $R = O_K$. Then the prime number p is ramified in R if and only if p divides the discriminant of R.*

PROOF We have already shown that if p is ramified in R, then $p|\mathrm{disc}(R)$, so we only need to prove the converse. Let us suppose that $p|\mathrm{disc}(R)$. We fix an integral basis $\alpha_1, \dots, \alpha_n$ of R. Then, from Proposition 10.7,

$$\mathrm{disc}(R) = |T_{K/\mathbf{Q}}(\alpha_i\alpha_j)|,$$

where $|T_{K/\mathbf{Q}}(\alpha_i\alpha_j)|$ is the determinant of the matrix $T = \big(T_{K/\mathbf{Q}}(\alpha_i\alpha_j)\big)$. From the definition of the trace in Section 10.1 the elements $T_{K/\mathbf{Q}}(\alpha_i\alpha_j) \in \mathbf{Q}$. However, $\alpha_i\alpha_j \in O_K$, so $T_{K/\mathbf{Q}}(\alpha_i\alpha_j) \in \mathbf{Z}$ (Exercise 11.1). Working modulo p, i.e., considering these elements lying in $\mathbf{F}_p$ and, knowing that $\mathrm{disc}(R) = 0$ in $\mathbf{F}_p$, we see that the rows of the matrix T are linearly dependant, i.e., there exist $m_1, \ldots, m_n \in \mathbf{F}_p$, not all 0, such that

$$m_1 \left(T_{K/\mathbf{Q}}(\alpha_1\alpha_1) \ldots T_{K/\mathbf{Q}}(\alpha_1\alpha_n)\right) + \cdots + m_n \left(T_{K/\mathbf{Q}}(\alpha_n\alpha_1) \ldots T_{K/\mathbf{Q}}(\alpha_n\alpha_n)\right) = (0, \ldots, 0).$$

We may express this by saying that there exist integers $m_1, \ldots, m_n$, not all divisible by p, such that

$$\sum_{i=1}^{n} T_{K/\mathbf{Q}}(\alpha_i\alpha_j)m_i$$

is divisible by p, for $j = 1, \ldots, n$. If we set $\alpha = \sum_{i=1}^n m_i\alpha_i$, then

$$p | T_{K/\mathbf{Q}}(\alpha\alpha_j),$$

for $j = 1, \ldots, n$, and it follows that $p|T_{K/\mathbf{Q}}(\alpha\beta)$, for any $\beta \in R$, i.e., $T_{K/\mathbf{Q}}(R\alpha) \subset \mathbf{Z}p$. Moreover, $\alpha \in R \backslash pR$, since the integers $m_1, \ldots, m_n$ are not all divisible by p and $(\alpha_1, \ldots, \alpha_n)$ is an integral basis of R.

Let $Q_1, \ldots, Q_s$ be the prime ideals in R involved in the decomposition of the ideal Rp. Propositions 12.2 and 12.3 ensure that $\cap_{i=1}^s Q_i = Q_1 \cdots Q_s$. If p is unramified in R, then $Rp = Q_1 \cdots Q_s$; thus, as $\alpha \notin Rp$, there exists Q_i such that $\alpha \notin Q_i$.

We now consider a normal closure N of K over $\mathbf{Q}$. From Corollary 13.7, p is unramified in $O_N = S$. Let Q' be a nonzero prime ideal in S lying over Q_i. If $\alpha \in Q'$, then $\alpha \in Q' \cap R = Q_i$, a contradiction, thus $\alpha \notin Q'$. We claim that $T_{N/\mathbf{Q}}(S\alpha) \subset \mathbf{Z}p$. To see this, we apply Corollary 10.3:

$$T_{N/\mathbf{Q}}(S\alpha) = T_{K/\mathbf{Q}} \circ T_{N/K}(S\alpha) = T_{K/\mathbf{Q}}\left(T_{N/K}(S)\alpha\right) \subset T_{K/\mathbf{Q}}(R\alpha) \subset \mathbf{Z}p.$$

As Q' lies over Q_i and Q_i lies over p, Q' lies over p. We take the complete set $Q', Q'_2, \ldots, Q'_t$ of nonzero prime ideals in S which lie over p. From the Chinese remainder theorem (Theorem F.1), there is a solution $\beta \in S$ of the system of equivalences

$$\begin{array}{rcl} x & \equiv & 1 \pmod{Q'} \\ x & \equiv & 0 \pmod{Q'_2} \\ \vdots & \vdots & \vdots \\ x & \equiv & 0 \pmod{Q'_t}. \end{array}$$

The element β lies in Q'_i, for $i = 2, \ldots, t$, but not in Q'. We claim that

- $T_{N/\mathbf{Q}}(\alpha\beta\gamma) \in Q'$, for $\gamma \in S$;
- $\sigma(\alpha\beta\gamma) \in Q'$, for $\gamma \in S$ and $\sigma \in G \setminus D$,

where $G = Gal(N/\mathbf{Q})$ and $D = D(Q'|p)$. The first assertion is easy to prove. We only need to observe that $\beta\gamma \in S$ and $T_{N/\mathbf{Q}}(S\alpha) \subset \mathbf{Z}p \subset Q'$. The second assertion requires a little more work. First we notice that $\sigma \in G \setminus D$ implies that $\sigma(Q') \neq Q'$, or equivalently $Q' \neq \sigma^{-1}(Q')$. As $\sigma^{-1}(Q')$ lies over p, $\beta \in \sigma^{-1}(Q')$, which implies that $\sigma(\beta) \in Q'$, which in turn implies that $\sigma(\alpha\beta\gamma) \in Q'$.

We now claim that

$$\sum_{\sigma \in D} \sigma(\alpha\beta\gamma) \in Q'$$

for all $\gamma \in S$. To see this, we first remark that from Corollary 10.3

$$T_{N/\mathbf{Q}}(\alpha\beta\gamma) = \sum_{\sigma \in G} \sigma(\alpha\beta\gamma).$$

Then

$$\sum_{\sigma \in D} \sigma(\alpha\beta\gamma) = T_{N/\mathbf{Q}}(\alpha\beta\gamma) - \sum_{\sigma \in G \setminus D} \sigma(\alpha\beta\gamma),$$

i.e., the difference of two elements in Q'.

We may now finish the proof. The members σ of the subgroup D of G induce automorphisms $\bar{\sigma}$ of S/Q':

$$\bar{\sigma}(x + Q') = \sigma(x) + Q'.$$

Reducing α, β and γ modulo Q', we obtain

$$\sum_{\sigma \in D} \bar{\sigma}(\bar{\alpha}\bar{\beta}\bar{\gamma}) = 0,$$

for all $\gamma \in S$. We have seen above that $\alpha, \beta \notin Q'$, so $\bar{\alpha}\bar{\beta}$ is a nonzero member of the field S/Q'. As γ runs through all the elements of S, $\bar{\gamma}$ runs through all the elements of S/Q'. It follows that

$$\sum_{\sigma \in D} \bar{\sigma}(\bar{x}) = 0,$$

for all $\bar{x} \in S/Q'$. Hence the automorphisms $\bar{\sigma}$, with $\sigma \in D$, are not independant, which contradicts the corollary to Dedekind's lemma (Corollary 8.1). The supposition that p is unramified led us to this contradiction, hence p must be ramified. $\square$

Remark We will show in the next chapter that, if $K \neq \mathbf{Q}$, then $|\mathrm{disc}(R)| > 1$. Thus, in this case there exists a prime number p which divides $\mathrm{disc}(R)$. Consequently, Theorem 13.14 ensures the existence of a ramified prime number. More generally, if $K \subset L$ are number fields, then there exists a prime ideal in O_K which ramifies in O_L. To see this, it suffices to consider any prime ideal in O_K in the decomposition of $O_K p$, where $p | \mathrm{disc}(O_L)$.

13.9 Prime decomposition in cyclotomic number rings

Let p be a prime number, s a positive integer and $\zeta = e^{\frac{2\pi i}{p^s}}$. We will be interested in the decomposition of a prime q in the number ring of the cyclotomic field $K = \mathbf{Q}(\zeta)$. As K is normal over $\mathbf{Q}$ we may write

$$O_K q = (Q_1 \cdots Q_r)^e,$$

where the Q_i are prime ideals in O_K.

We will first consider the case where $q = p$. In the proof of Proposition 11.10 we saw that

$$O_K p = O_K(1-\zeta)^{\phi(p^s)} = (O_K(1-\zeta))^{\phi(p^s)} \tag{13.3}$$

and

$$N_{K/\mathbf{Q}}(1-\zeta) = p.$$

From Theorem 13.4

$$N_{K/\mathbf{Q}}(1-\zeta) = \|O_K(1-\zeta)\|,$$

hence $\|O_K(1-\zeta)\| = p$. However, from Proposition 13.4, the principal ideal $O_K(1-\zeta)$ is a prime ideal, therefore the expression (13.3) is the decomposition of $O_K p$ into prime ideals.

We now turn to the case where $q \neq p$. This is more difficult. From Theorem 11.15 the discriminant of O_K is a power of p. As $q \neq p$, q does not divide the discriminant, so, by Theorem 13.14, q is not ramified in O_K. This implies that the decomposition has the form

$$O_K q = Q_1 \cdots Q_r,$$

where the Q_i are prime ideals in O_K. We now aim to determine the value of r.

We recall that $O_K = \mathbf{Z}[\zeta]$. For $i = 1, \ldots, r$, since $Q_i | O_K q$, we have $Q_i \supset O_K q = \mathbf{Z}[\zeta] q$ and it follows that Q_i lies over $\mathbf{Z}q$. From Corollary 13.2, the inertial degrees $f(Q_i|q)$ all have the same value. If f is the common value of the inertial degrees, then we can write

$$rf = \phi(p^s) = p^{s-1}(p-1), \tag{13.4}$$

where ϕ denotes the Euler totient function. We claim that f is the order of q in the multiplicative group $\mathbf{Z}_{p^s}^{\times}$.

Let Q be one of the Q_i. Then $\mathbf{Z}[\zeta]/Q$ is isomorphic to $\mathbf{F}_{q^f}$, with subfield $\mathbf{F}_q$. (This is obtained from the mapping ϕ defined just before Proposition 13.3.) We may identify the elements of $\mathbf{F}_{q^f}$ with the cosets of Q, which we will write in the usual way, i.e., $\bar{a} = a + Q$. If $a \in \mathbf{Z}$, then $\bar{a} \in \mathbf{F}_q$ and from this it follows that $\mathbf{F}_{q^f} = \mathbf{F}_q(\bar{\zeta})$. This implies that an element of the Galois group $\bar{G} = Gal(\mathbf{F}_{q^f}/\mathbf{F}_q)$ is determined by its value at $\bar{\zeta}$.

Moreover, from Theorem 7.9, $\bar{G}$ is cyclic and generated by the Frobenius automorphism $\mathrm{Fr} : x \longmapsto x^q$. Since $\mathbf{F}_{q^f} = \mathbf{F}_q(\bar{\zeta})$, the Frobenius automorphism, is determined by its value at $\bar{\zeta}$. Let f' be the order of q in in $\mathbf{Z}_{p^s}^{\times}$. Then

$$Fr^{f'}(\bar{\zeta}) = \bar{\zeta}^{q^{f'}} = \overline{\zeta^{q^{f'}}} = \overline{\zeta^{1+kq^s}}, \tag{13.5}$$

for some $k \in \mathbf{N}^*$. Therefore $Fr^{f'}(\bar{\zeta}) = \bar{\zeta}$, which implies that $f|f'$.

We now show that $f'|f$. If $q^f \equiv 1 (\mathrm{mod}\ p^s)$, then $f'|f$, so this is what we will show. We set

$$q^f \equiv a (\mathrm{mod}\ p^s),$$

with $a \in \{1, \ldots, p^s - 1\}$. Suppose that $a > 1$. Then

$$\zeta^{q^f} = \zeta^a \Longrightarrow \bar{\zeta}^{q^f} = \bar{\zeta}^a.$$

However, from equation 13.5),

$$\bar{\zeta}^{q^f} = \bar{\zeta},$$

hence

$$\bar{\zeta}^a = \bar{\zeta} \Longrightarrow \bar{\zeta}^{a-1} = \bar{1} \Longrightarrow 1 - \zeta^{a-1} \in Q.$$

On the other hand we have

$$-1 + X^{p^s} = \prod_{i=0}^{p^s-1} (-\zeta^i + X) \Longrightarrow \prod_{i=1}^{p^s-1} (-\zeta^i + X) = \frac{-1 + X^{p^s}}{-1 + X} = 1 + X + \cdots + X^{p^s-1}.$$

Noting $g(X)$ the last expression on the right-hand side, we obtain

$$\prod_{i=1}^{p^s-1} (-\zeta^i + 1) = g(1) = p^s.$$

Since one of the factors in the expression on the left-hand side of the equation is $1-\zeta^{a-1}$ and all the factors are in O_K, we see that $p^s \in Q$. This means that Q contains both p^s and q, which are coprime. Hence $1 \in Q$, a contradiction. Therefore $a = 1$ and it follows that

$$q^f \equiv 1 (\bmod\ p^s),$$

as required. To conclude, we have shown that f is the order of q in $\mathbf{Z}_{p^s}^\times$, as claimed.

To conclude, from (13.3) we obtain

$$r = \frac{p^{s-1}(p-1)}{f},$$

where f is the order of q in $\mathbf{Z}_{p^s}^\times$.

Remark Further on, in Chapter 18, we will reconsider the question of the decomposition of a prime number in a number ring, but in a more general context.

13.10 Higher ramification groups

Let K and L be number fields, with L a finite normal extension of K. We set $R = O_K$, $S = O_L$ and let $P \subset R$, $Q \subset S$ be prime ideals with Q lying over P. We recall the definition of the inertia group:

$$E = E(Q|P) = \{\sigma \in G : \sigma(\alpha) \equiv \alpha (\bmod\ Q)\ \forall \alpha \in S\},$$

where $G = Gal(L/K)$. We now extend this definition. For $m \in \mathbf{N}$, we set

$$V_m = \{\sigma \in G : \sigma(\alpha) \equiv \alpha (\bmod\ Q^{m+1})\ \forall \alpha \in S\}.$$

Thus $V_0 = E$. The V_m form a descending chain of subgroups of the decomposition group $D = D(Q|P)$ and are called *ramification groups* .

We recall the Krull Intersection Theorem:

Theorem 13.15 *If R is a commutative noetherian domain and I a proper ideal in R, then $\cap_{m=1}^\infty I^m = \{0\}$.*

Proposition 13.15 *The groups V_m are normal subgroups of D and their intersection is the identity.*

PROOF Let $\sigma \in V_m$ and $\tau \in D$. Then, for $\alpha \in S$, we have

$$\sigma\tau(\alpha) = \tau(\alpha) + x$$

with $x \in Q^{m+1}$. This implies that

$$\tau^{-1}\sigma\tau(\alpha) = \alpha + \tau^{-1}(x).$$

Since $\tau^{-1}Q = Q$ and $x \in Q^{m+1}$, $\tau^{-1}(x) \in Q^{m+1}$, thus

$$\tau^{-1}\sigma\tau(\alpha) \equiv \alpha (\bmod\ Q^{m+1}),$$

and it follows that V_m is normal in D.

As S is a noetherian domain, from Theorem 13.15, $\cap_{m=1}^{\infty} Q^m = \{0\}$. If $\sigma \in \cap_{m=0}^{\infty} V_m$ and $\alpha \in S$, then

$$\sigma(\alpha) - \alpha \in \cap_{m=1}^{\infty} Q^m = \{0\} \Longrightarrow \sigma(\alpha) = \alpha.$$

Therefore σ is the identity on S and consequently on L, because L is the field of fractions of S. □

Corollary 13.8 *There exists $n \geq 0$ such that V_m is reduced to the identity for $m \geq n$.*

PROOF As D is finite, so are the subgroups V_m and the chain must be stationary after a certain point, i.e., there exists n such that $V_m = V_n$, for $m \geq n$. If V_m is not reduced to the identity for $m \geq n$, then the intersection of the groups V_m must contain elements other than the identity, which is a contradiction. Therefore, for $m \geq n$, V_m is reduced to the identity. □

We recall that S^E is the number ring of L^E, i.e., $S^E = O_{L^E}$, and that Q^E is the unique prime ideal in S^E lying under Q. We now consider the localizations S_Q and $S^E_{Q^E}$. These rings are both Dedekind domains, being localizations of Dedekind domains (Theorem 12.9). They are also local rings with respective unique maximal ideals $S_Q Q$ and $S^E_{Q^E} Q^E$ (Theorem 12.10). From Theorem 12.11 these localizations are PIDs.

If $\frac{s}{u} \in S^E_{Q^E}$, then $s \in S$, because $S^E \subset S$. In addition, $u \notin Q$ (If $u \in Q$, then $\in S^E \cap Q = Q^E$, a contradiction.) Hence $S^E_{Q^E} \subset S_Q$, and we may consider S_Q to be a $S^E_{Q^E}$-module. Let t be a generator of the principal ideal $S_Q Q$. We may suppose that $t \in S$: if $t' = \frac{t}{u}$ is a generator, then so is t.

Theorem 13.16 *The module S_Q is a free module over $S^E_{Q^E}$, with basis $B = \{1, t, \ldots, t^{e-1}\}$, where $e = [L : L^E]$.*

PROOF Our first step is to show that if a is a nonzero element of L^E, then there exists $s \in \mathbf{Z}$ such that $S_Q a = S_Q Q^{se}$. Let us write L_Q for the fraction field of S_Q and L_{Q^E} for that of $S^E_{Q^E}$. Then $L^E \subset L \subset L_Q$ and so any nonzero element a of L^E generates a nonzero fractional ideal of S_Q, which we may write $S_Q a$. We aim to study the decomposition of $S_Q a$ into prime ideals in S_Q. Since $L^E \subset L_{Q^E}$, a also generates a fractional ideal of $S^E_{Q^E}$, namely $S^E_{Q^E} a$. From Theorem 12.11 there exists $s \in \mathbf{Z}$ such that

$$S^E_{Q^E} a = (S^E_{Q^E} Q^E)^s = S^E_{Q^E} Q^{Es},$$

and so, using the fact that $S^E_{Q^E}$ is contained in S_Q, we obtain

$$S_Q a = S_Q S^E_{Q^E} a = S_Q (S^E_{Q^E} Q^{Es}) = S_Q Q^{Es}.$$

Now, using the inclusion of S in S_Q, we have

$$S_Q Q^{Es} = S_Q S(Q^{Es}) = S_Q (S Q^E)^s.$$

Since Q^E lies over Q^D and Q is the unique prime ideal of S lying over Q^D (see Section 13.7), Q is the unique prime ideal of S lying over Q^E: SQ^E is a power of Q. Taking into account Theorem 13.6, with $K = L^E$, and then Lemma 13.3 and Proposition 13.11, we obtain $SQ^E = Q^e$. Finally, we have shown that, for any nonzero element a in L^E, there exists $s \in \mathbf{Z}$ such that $S_Q a = S_Q Q^{se}$.

Our next step is to show that the elements $1, t, \ldots, t^{e-1}$ form a basis of L over L^E. As $[L : L^E] = e$, it is sufficient to prove that these elements are linearly independant over L^E.

Suppose that $x = \sum_{j=0}^{e-1} a_j t^j$, with $a_j \in L^E$ and some $a_j \neq 0$. If $0 \leq k, l \leq e-1$, with $k \neq l$, and $a_k \neq 0$, $a_l \neq 0$, then we claim that $s_k e + k \neq s_l e + l$, where

$$S_Q a_k = S_Q Q^{es_k} \qquad \text{and} \qquad S_Q a_l = S_Q Q^{es_l}.$$

If not, then

$$0 \neq k - l = e(s_l - s_k),$$

which is impossible, because $|k - l| < e$. We now set

$$m = \min\{es_j + j : a_j \neq 0,\ S_Q a_j = S_Q Q^{es_j}\}.$$

Let i be such that $m = es_i + i$; then, if $0 \leq j < e$ and $a_j \neq 0$, there exists $\alpha_j \in S_Q$ such that $a_j = \alpha_j t^{s_j e}$. Therefore there exists $\beta \in S_Q$ such that

$$x = \sum_{j, a_j \neq 0} \alpha_j t^{s_j e + j} = t^m(\alpha_i + t\beta).$$

If $\alpha_i \in S_Q Q$, then $a_i = t^{s_i e} u t$, with $u \in S_Q$. This implies that

$$(S_Q Q)^{s_i e} = S_Q a_i \subset (S_Q Q)^{s_i e + 1},$$

which is not possible. Hence $\alpha_i \notin S_Q Q$ and it follows that $\alpha_i + t\beta \notin S_Q Q$. Thus $\alpha_i + t\beta \neq 0$ and so $x \neq 0$. We have shown that the set $\{1, t, \ldots, t^{e-1}\}$ is independant.

At this point we should also notice that $S_Q x = S_Q Q^m$. Indeed, as S_Q is a local ring, its maximal ideal $S_Q Q$ is composed of its nonunits. Hence $\alpha_i + t\beta$ is a unit and so

$$S_Q x = S_Q t^m = S_Q Q^m.$$

The final step is to show that B is also a basis of the $S^E_{Q^E}$-module S_Q. Suppose that there exist $b_0, b_1, \ldots, b_{e-1} \in S^E_{Q^E}$ such that $\sum_{j=0}^{e-1} b_j t^j = 0$. As $S^E_{Q^E}$ is included in L^E and we have shown that B is an independant set over L^E, the b_j all have the value 0, so B is an independant set over $S^E_{Q^E}$.

We must now show that B a generating set of the $S^E_{Q^E}$-module S_Q. Let x be a nonzero element of S_Q. As S_Q is included in L, we may write $x = \sum_{j=0}^{e-1} a_j t^j$, where $a_j \in L^E$, for all j, and at least one a_j is nonzero. We claim that each a_j belongs to $S^E_{Q^E}$. Looking at the beginning of the proof, we notice that, if $a_j \neq 0$, then there is an integer s_j such that the fractional ideal $S^E_{Q^E} a_j = (S^E_{Q^E} Q^E)^{s_j}$. This is the decomposition of this fractional ideal into prime ideals of $S^E_{Q^E}$. In addition, we have shown that $S_Q x = (S_Q Q)^m$ is the decomposition into prime ideals of S_Q of the fractional ideal $S_Q x$. As $x \in S_Q$, $S_Q x$ is an integral ideal of S_Q and so $m \geq 0$ (Corollary 12.9). However,

$$m = \min\{es_j + j : a_j \neq 0,\ S_Q a_j = S_Q Q^{es_j}\},$$

so, if $a_j \neq 0$, then $es_j + j \geq 0$, which implies that $s_j \geq -\frac{j}{e} > -1$. Therefore $s_j \geq 0$, because s_j is an integer. It follows that $S^E_{Q^E} a_j$ is an ideal of $S^E_{Q^E}$, because $S^E_{Q^E} a_j = (S^E_{Q^E} Q^E)^{s_j}$, and so $a_j \in S^E_{Q^E}$. We have shown that B is a generating set of S_Q as a $S^E_{Q^E}$-module. This finishes the proof. □

We continue our study of the ramification groups using a generator $t \in S$ of the principal ideal $S_Q Q$. We notice that $t \in S \subset L$, so it makes sense to write $\sigma(t)$ for any automorphism $\sigma \in Gal(L/K)$.

Proposition 13.16 *For $i = 0, 1, 2, \ldots$,*

$$V_i = \{\sigma \in E : \sigma(t) - t \in S_Q Q^{i+1}\}.$$

PROOF If $\sigma \in V_i$, then $\sigma \in E$ and $\sigma(t) - t \in Q^{i+1}$, since $t \in S$. However, $Q^{i+1} \subset S_Q(Q^{i+1})$, thus $\sigma(t) - t \in S_Q Q^{i+1}$.

Now suppose that $\sigma \in E$ and $\sigma(t) - t \in S_Q Q^{i+1}$. If $x \in S$, then we may consider that $x \in S_Q$ and so we can write $x = \sum_{j=0}^{e-1} a_j t^j$, with $a_j \in S_{Q^E}^E$ (Theorem 13.15), hence

$$\sigma(x) - x = \sum_{j=0}^{e-1} a_j \left(\sigma(t)^j - t^j\right),$$

because the a_j are fixed by the automorphisms of E. (Indeed, $a_j \in S_{Q^E}^E$ and $S_{Q^E}^E \subset S^E \subset L^E$.) Also, $\sigma(t) - t | \sigma(t)^j - t^j$ in S, i.e., $\sigma(t)^j - t^j = s_j(\sigma(t) - t)$, for some $s_j \in S$. As both $S_{Q^E}^E$ and S are included in S_Q,

$$\sum_{j=0}^{e-1} a_j \left(\sigma(t)^j - t^j\right) \in S_Q Q^{i+1}$$

Given that $x \in S$, we now have

$$\sigma(x) - x \in S_Q Q^{i+1} \cap S = Q^{i+1},$$

where we have used Theorem 12.12 for the equality. This ends the proof. $\square$

We have seen that the ramification groups V_i form a sequence of normal subgroups of the inertial group E. As $V_{i+1} \subset V_i$, we have a sequence

$$E = V_0 \rhd V_1 \rhd V_2 \rhd \cdots$$

We also know that after a certain point $V_{i+1} = V_i$, so we may consider the sequence to be finite. We are now interested in the factor groups V_i / V_{i+1}.

Theorem 13.17 *There exists a group monomorphism from E/V_1 into $S/Q^\times$. Thus E/V_1 is a cyclic group whose order is coprime to p, where $Q \cap \mathbf{Z} = \mathbf{Z}p$.*

PROOF Let $t \in S$ be a generator of the principal ideal $S_Q Q$, so $t \in S \cap S_Q Q = Q$(Theorem 12.12). If $\sigma \in E$, then $\sigma \in D$, which implies that $\sigma(t) \in Q$, because $t \in Q$. As $Q \subset S_Q Q$, there exists $x_\sigma \in S_Q$ such that

$$\sigma(t) = x_\sigma t.$$

From Exercise 12.8 we may suppose that S_Q as a subset of L, i.e., we consider $x = \frac{r}{u} \in S_Q$ as an element of l. This permits us to induce a mapping σ' on S_Q from $\sigma \in E$ by setting $\sigma'(x) = \frac{\sigma(r)}{\sigma(u)} \in L$. Clearly, $\sigma(r), \sigma(u) \in S$. It is elementary to check that σ' is an automorphism of S_Q. We should also notice that, since $\sigma \in E$, for all $x \in S_Q$,

$$\sigma'(x) \equiv x (\mathrm{mod}\ S_Q Q).$$

Indeed, there exists $q \in Q$ such that $\sigma(r) = r + q$ and so

$$\sigma'(x) = \frac{\sigma(r)}{\sigma(u)} = \frac{r+q}{u+q'} = \frac{r}{u} - \frac{rq' - uq}{u(u+q')} = x + q_1,$$

with $q_1 \in S_Q Q$.

To simplify the notation, from here on we will write σ for σ'. Our next step is to show that $x_\sigma \notin S_Q Q$. As $\sigma^{-1} \in E$, there exists $x_{\sigma^{-1}} \in S_Q$ such that

$$\sigma^{-1}(t) = x_{\sigma^{-1}} t.$$

Then

$$t = \sigma\left(\sigma^{-1}(t)\right) = \sigma(x_{\sigma^{-1}} t) = \sigma(x_{\sigma^{-1}})\sigma(t) = \sigma(x_{\sigma^{-1}}) x_\sigma t.$$

As S_Q is an integral domain, we have

$$1 = \sigma(x_{\sigma^{-1}}) x_\sigma,$$

so x_σ is invertible in S_Q, which implies that $x_\sigma \notin S_Q Q$, because $S_Q Q$ is a proper ideal of S_Q.

From Corollary 12.10, there is an isomorphism ϕ from $S_Q/S_Q Q$ onto S/Q. Noting $\bar{x}_\sigma$ the image $\phi(x_\sigma + S_Q Q)$, we have $\bar{x}_\sigma \neq 0$, because $x_\sigma \notin S_Q Q$. We now define a mapping $\theta : E \longrightarrow S/Q^\times$ by

$$\theta(\sigma) = \bar{x}_\sigma.$$

We consider the properties of θ. First we notice that θ is a group homomorphism: If $\sigma, \tau \in E$, $\sigma(t) = x_\sigma t$ and $\tau(t) = x_\tau t$, then

$$\sigma\tau(t) = \sigma(x_\tau t) = \sigma(x_\tau)\sigma(t) = (x_\tau + vt)x_\sigma t = (x_\tau x_\sigma + v x_\sigma t)t,$$

where $v \in S_Q$, therefore

$$\theta(\sigma\tau) = \overline{x_\tau x_\sigma + v x_\sigma t} = \bar{x}_\tau \bar{x}_\sigma = \theta(x_\tau)\theta(x_\sigma),$$

so θ is a homomorphism. We claim that the kernel of θ is V_1. To establish this we use Proposition 13.16. If $\sigma \in V_1$, then

$$\sigma(t) - t \in S_Q Q^2 \Longrightarrow \sigma(t) = t + vt^2 = (1 + vt)t \Longrightarrow \theta(\sigma) = \overline{1 + vt} = \bar{1},$$

where $v \in S_Q$. Hence $\sigma \in \operatorname{Ker}\theta$. On the other hand, if $\sigma \in \operatorname{Ker}\theta$, then $\theta(\sigma) = \bar{1}$ and we have

$$\bar{x}_\sigma = \bar{1} \Longrightarrow \sigma(t) - t = x_\sigma t - t = (1 + vt)t - t = vt^2,$$

where $v \in S_Q$. It follows that $\sigma \in V_1$. We have shown that $V_1 = \operatorname{Ker}\theta$.

As V_1 is the kernel of θ, the quotient group E/V_1 is isomorphic to a subgroup of $S/Q^\times$, which is the group of nonzero elements of the finite field S/Q. From Corollary 3.3 ,$S/Q^\times$ is cyclic and so E/V_1 is cyclic, being isomorphic to a subgroup of a cyclic group.

There exists a unique prime number p such that $Q \cap \mathbf{Z} = p\mathbf{Z}$. As $p\mathbf{Z} \subset Q$, we have $p \in Q$, so the characteristic of S/Q is p. This implies that the prime field of S/Q is $\mathbf{F}_p$ and it follows that $|S/Q| = p^n$, for some positive integer n. Hence $|S/Q^\times| = p^n - 1$. As $|E/V_1|$ divides $p^n - 1$, $|E/V_1|$ must be coprime to p. □

Remark In the proof of the theorem we chose a particular generator $t \in S$ of $S_Q Q$. In fact, we obtain the same mapping θ if we choose another such generator t'. First we notice that $t' = at$, where $a \in S_Q^\times$. This implies that $a \notin S_Q Q$. Then we have

$$\sigma(t') = x'_\sigma t' = x'_\sigma at.$$

As we saw in the proof of Theorem 13.17, if $x \in S_Q$ and $\sigma \in E$, then $\sigma(x) \equiv x (\mathrm{mod}\ S_Q Q)$, so there exists $q \in S_Q Q$ such that $\sigma(a) = a + q = a + vt$, with $v \in S_Q$. Hence

$$\begin{array}{rcl} x'_\sigma at & = & \sigma(at) = \sigma(a)\sigma(t) = (a+vt)x_\sigma t \\ & \Longrightarrow & x'_\sigma a = (a+vt)x_\sigma \\ & \Longrightarrow & \bar{a}\bar{x}_\sigma = \bar{a}\bar{x}'_\sigma \Longrightarrow \bar{x}'_\sigma = \bar{x}_\sigma, \end{array}$$

because $S_Q/S_Q Q$ is a field and $\bar{a} \neq 0$. Therefore the value of $\theta(\sigma)$ is unaltered by choosing another generator in S of $S_Q Q$.

We now consider the quotient groups V_i/V_{i+1}, with $i \geq 1$.

Theorem 13.18 *There exists a group monomorphism from V_i/V_{i+1} into the additive group of the field S/Q. Hence V_i/V_{i+1} is an abelian p-group, where $Q \cap \mathbf{Z} = \mathbf{Z}p$.*

PROOF As in the proof of Theorem 13.17, we let $t \in S$ be a generator of the principal ideal $S_Q Q$ and so $t \in S \cap S_Q Q$. If $\sigma \in V_i$, then $\sigma(t) = t + x_\sigma t^{i+1}$, where $x_\sigma \in S_Q$ (Proposition 13.16). From Corollary 12.10, there is an isomorphism ϕ from $S_Q/S_Q Q$ onto S/Q. Noting $\bar{x}_\sigma$ the image $\phi(x_\sigma + S_Q Q)$, we obtain a mapping θ_i from V_i into S/Q defined by

$$\theta_i(\sigma) = \bar{x}_\sigma.$$

We claim that θ_i is a homomorphism into the additive group of S/Q. If $\sigma, \tau \in V_i$, then

$$\sigma\tau(t) = \sigma(t + x_\tau t^{i+1}) = \sigma(t) + \sigma(x_\tau)\sigma(t^{i+1}).$$

If $x = \frac{r}{u} \in S_Q$ and $\sigma \in V_i$, then there exist $q, q' \in Q^{i+1}$ such that

$$\sigma(x) = \frac{\sigma(r)}{\sigma(u)} = \frac{r+q}{u+q'} = \frac{r}{u} - \frac{rq' - uq}{u(u+q')} = x + q_1,$$

with $q_1 \in S_Q Q^{i+1}$. Thus

$$\sigma\tau(t) = t + x_\sigma t^{i+1} + (x_\tau + vt^{i+1})(t + x_\sigma t^{i+1})^{i+1}.$$

However,

$$(t + x_\sigma t^{i+1})^{i+1} = t^{i+1} + x_\sigma (i+1) t^{2i+1} + \text{expressions in higher powers of } t,$$

with $2i+1 > i+1$, because $i \geq 1$. Hence

$$\sigma\tau(t) = t + (x_\sigma + x_\tau + v't)t^{i+1},$$

where $v, v' \in S_Q$. It follows that

$$\theta_i(\sigma\tau) = \overline{x_\sigma + x_\tau + v't} = \overline{x_\sigma + x_\tau} = \bar{x}_\sigma + \bar{x}_\tau = \theta_i(\sigma) + \theta_i(\tau).$$

We have shown that θ_i is a homomorphism from V_i into the additive group of S/Q.

Our next task is to consider the kernel of θ_i. If $\sigma \in V_{i+1}$, then, for some $v \in S_Q$,

$$\sigma(t) - t \in S_Q Q^{i+2} \Longrightarrow \sigma(t) = t + vt^{i+2} = t + (vt)t^{i+1}$$

and so

$$\theta_i(\sigma) = \overline{vt} = \bar{0}.$$

So we have $V_{i+1} \subset \operatorname{Ker} \theta_i$. Now suppose that $\theta_i(\sigma) = \bar{0}$. Then $\bar{x}_\sigma = \bar{0}$, which implies that

$$\sigma(t) = t + (vt)t^{i+1} = t + vt^{i+2},$$

with $v \in S_Q$. Therefore $\sigma \in V_{i+1}$ and it follows that $\operatorname{Ker} \theta_i = V_{i+1}$. Therefore the quotient group V_i/V_{i+1} is isomorphic to a subgroup of the additive group of S/Q. We have seen in the proof of Theorem 13.17 that $|S/Q| = p^n$, where $Q \cap \mathbf{Z} = \mathbf{Z}p$ and n is a positive integer, so $|V_i/V_{i+1}| = p^m$, where $m \leq n$. Therefore the order of an element in V_i/V_{i+1} is a power of p. □

Exercise 13.6 *In the proof of the preceding theorem we have used a particuler generator $t \in S$ of the principal ideal $S_Q Q$ to construct the homomorphism θ_i, which in turn gives us a monomorphism $\bar{\theta}_i$ of V_i/V_{i+1} into S/Q. Suppose that we take another generator $t' \in S$ of $S_Q Q$ and so obtain another monomorphism of $\bar{\theta}'_i$ of V_i/V_{i+1} into S/Q. What can we say of the relation between $\bar{\theta}_i$ and $\bar{\theta}'_i$?*

We recall the definition of a solvable group. A normal series of a finite group G, with identity e, is a chain of subgroups

$$G = G_0 \supset G_1 \supset \cdots \supset G_n = \{e\},$$

where the subgroup G_{i+1} is normal in G_i, for all i. If a finite group G has such a series and all the quotient groups G_i/G_{i+1} are abelian, then we say that G is a *solvable group.*

Proposition 13.17 *The inertia and decomposition groups are solvable.*

PROOF The series

$$D \supset E \supset V_1 \supset \cdots \supset V_m = \{\mathrm{id}_D\}$$

is a normal series, because $E, V_1, \ldots, V_m$ are normal in D. In Section 13.6 we saw that D/E is cyclic and from Theorems 13.17 and 13.18 above, for $i \geq 0$, V_i/V_{i+1} is a subgroup of an abelian group, hence abelian. It follows that E and D are solvable groups. □

Here are two further results concerning the first ramification group V_1.

Proposition 13.18 *We have*

- **a.** *The cardinal of V_1 is a power of p, hence V_1 is a p-group: $|V_1| = p^k$, where $k \geq 0$;*
- **b.** *If e is the ramification index $e(Q|P)$, then $e = mp^k$, where $p \not| m$ and $m = |E/V_1|$.*

PROOF **a.** As V_m is reduced to the identity, we may write

$$|V_1| = |V_1/V_m| = |V_1/V_2||V_2/V_3| \cdots |V_{m-1}/V_m|.$$

As all the factors on the right hand side are powers of p, so is $|V_1|$.
b. From Proposition 13.11, $e = [L : L^E]$. In addition, from Theorem 6.6, $[L : L^E] = |E|$, which in turn is equal to $|V_1||E/V_1|$. Using part **a.** we obtain $e = p^k m$, and $p \not| m$, by Theorem 13.17.□

We have seen that V_1 and E are normal subgroups of D. As E is contained in D, V_1 is also normal subgroup of E and so the cosets of V_1 in E form a group, the quotient group E/V_1. We may define an action of D on E/V_1 by conjugation: for $\sigma \in D$ and $\tau V_1 \in E/V_1$, we set

$$\sigma \cdot \tau V_1 = \sigma(\tau V_1)\sigma^{-1} = (\sigma\tau\sigma^{-1})V_1.$$

(It is simple to check that this action is well-defined, i.e., if $\tau' V_1 = \tau V_1$, then $\sigma \cdot \tau' V_1 = \sigma \cdot \tau V_1$.)
From the group action we obtain, for each $\sigma \in D$, a bijection $\hat{\sigma}$ of E/V_1 defined by

$$\hat{\sigma}(\tau V_1) = \sigma \cdot \tau V_1 = \sigma(\tau V_1)\sigma^{-1}.$$

We may also define an action of D on S/Q: for $\sigma \in D$ and $s + Q \in S/Q$, we set

$$\sigma \cdot (s + Q) = \sigma(s) + Q.$$

(There is no difficulty in seeing that this action also is well-defined.)
From this second group action we obtain, for each $\sigma \in D$, a bijection $\tilde{\sigma}$ of S/Q defined as follows:

$$\tilde{\sigma}(s + Q) = \sigma \cdot (s + Q) = \sigma(s) + Q.$$

In Section 13.6 we saw that the the bijections $\tilde{\sigma}$ belong to the Galois group $Gal(S/Q, R/P) = \bar{G}$ and that the corresponding mapping $\psi : \sigma \longmapsto \tilde{\sigma}$ is an epimorphism. Moreover, $\bar{G}$ is a cyclic group generated by the Frobenius automorphism: $Fr : \bar{x} \longmapsto \bar{x}^q$, where $q = |R/P|$. The following result links the bijections $\hat{\sigma}$ and $\tilde{\sigma}$.

Proposition 13.19 *If $\sigma \in D$ is such that $\psi(\sigma) = \tilde{\sigma}$ is the Frobenius automorphism, then*

$$\hat{\sigma}(\tau V_1) = \tau^q V_1,$$

for all cosets $\tau V_1 \in E/V_1$.

PROOF First we fix a generator t of the ideal $S_Q Q$, i.e., $S_Q Q = S_Q t$. As $\hat{\sigma}(\tau V_1) = \sigma\tau\sigma^{-1}$, we have

$$\hat{\sigma}(\tau V_1) = \tau^q V_1 \Longleftrightarrow \sigma\tau^{-1}\sigma^{-1}\tau^q \in V_1 \Longleftrightarrow \sigma\tau^{-1}\sigma^{-1}\tau^q(t) \equiv t \ (\mathrm{mod}\ S_Q Q^2).$$

We now sum up some basic facts which we will need further on in the proof:

- For all $\sigma \in D$, there exists $x_\sigma \in S_Q$ such that $\sigma(t) = x_\sigma t$ and

  $$\sigma(x_{\sigma^{-1}})x_\sigma = 1.$$

  (This result is established in the proof of Theorem 13.17.)

- If $\sigma \in D$ and $x \in S_Q$, then

  $$\sigma(x) \in S_Q.$$

  Indeed, $x = \frac{r}{s} \in S_Q$ can be considered an element of L, thus $\sigma(x) = \frac{\sigma(r)}{\sigma(u)}$, because $\sigma(\frac{r}{u})\sigma(u) = \sigma(\frac{r}{u}u) = \sigma(r)$. If $\sigma(u) \in Q$, then $u = \sigma^{-1}(\sigma(u)) \in \sigma^{-1}(Q) = Q$, because $\sigma^{-1} \in D$, a contradiction. Therefore $\sigma(u) \notin Q$ and so $\frac{\sigma(r)}{\sigma(u)} \in S_Q$.

- If $\tau \in E$ and $x \in S_Q$, then

  $$\tau(x) \equiv x \ (\mathrm{mod}\ S_Q Q).$$

  Since $\tau : L \longrightarrow L$ satisfies the condition $\tau(\alpha) \equiv \alpha \ (\mathrm{mod}\ Q)$, for all $\alpha \in S$, we have $\tau(x) \equiv x \ (\mathrm{mod}\ S_Q Q)$, for all $x \in S_Q$, because

  $$x = \frac{r}{u} \in S_Q \subset L \Longrightarrow \tau(x) = \frac{\tau(r)}{\tau(u)} = \frac{r + q}{u + q'} = \frac{r}{u} - \frac{rq' - uq}{u(u + q')} = x + q_1,$$

  with $q_1 \in S_Q Q$.

With these rules in mind we aim to show that

$$\sigma\tau^{-1}\sigma^{-1}\tau^q(t) \equiv t \pmod{S_Q Q^2}.$$

To begin with, we establish that for $1 \leq i \leq q$ we have

$$\tau^i(t) \equiv x_\tau^i t \pmod{S_Q Q^2}.$$

For $i = 1$, the result is clear, because $\tau(t) = x_\tau t$. Next we consider the case $i = 2$. First,

$$\tau(t) = x_\tau t \Longrightarrow \tau^2(t) = \tau(x_\tau)\tau(t) = \tau(x_\tau)x_\tau t.$$

As $\tau \in E$, there exists $v \in S_Q$ such that $\tau(x_\tau) = x_\tau + vt$, hence

$$\tau^2(t) = (x_\tau + vt)x_\tau t = x_\tau^2 t + vx_\tau t^2 = x_\tau^2 t + v_1 t^2.$$

As $v_1 \in S_Q$, we have

$$\tau^2(t) \equiv x_\tau^2 t \pmod{S_Q Q^2}.$$

Our next step is to consider the case $i = 3$. We have

$$\begin{aligned}
\tau^3(t) &= \tau(\tau^2(t)) = \tau(x_\tau^2 t + v_1 t) \\
&= \tau(x_\tau^2 \tau(t) + \tau(v_1)\tau(t)^2 \\
&= (x_\tau + vt)^2 x_\tau t + \tau(v_1)(x_\tau t)^2 \\
&= x_\tau^3 t + v_2 t^2,
\end{aligned}$$

where $v_2 \in S_Q$. Hence

$$\tau^3(t) \equiv x_\tau^3 t \pmod{S_Q Q^2}.$$

Continuing in the same way we obtain

$$\tau^i(t) \equiv x_\tau^i t \pmod{S_Q Q^2},$$

for $1 \leq i \leq q$ and, in particular for $i = q$. Therefore there exists $w \in S_Q$ such that

$$\tau^q(t) = x_\tau^q t + wt^2.$$

We now consider the expression $\sigma\tau^{-1}\sigma^{-1}\tau^q$. First,

$$\begin{aligned}
\sigma^{-1}(\tau^q(t)) &= \sigma^{-1}(x_\tau^q t + wt^2) \\
&= \sigma^{-1}(x_\tau^q)x_{\sigma^{-1}} t + \sigma^{-1}(w)\sigma^{-1}(t)^2 \\
&= \sigma^{-1}(x_\tau^q)x_{\sigma^{-1}} t + \sigma^{-1}(w)x_{\sigma^{-1}}^2 t^2 \\
&= \sigma^{-1}(x_\tau^q)x_{\sigma^{-1}} t + w_1 t^2,
\end{aligned}$$

where $w_1 \in S_Q$. Thus

$$\sigma^{-1}(\tau^q(t)) \equiv \sigma^{-1}(x_\tau^q)x_{\sigma^{-1}} t \pmod{S_Q Q^2}$$

and so

$$\begin{aligned}
\tau^{-1}\sigma^{-1}\tau^q(t) &\equiv \tau^{-1}(\sigma^{-1}(x_\tau^q)x_{\sigma^{-1}})x_{\tau^{-1}} t \pmod{S_Q Q^2} \\
&\equiv \sigma^{-1}(x_\tau^q)x_{\sigma^{-1}}x_{\tau^{-1}} t \pmod{S_Q Q^2},
\end{aligned}$$

because $\tau^{-1} \in E$ implies that

$$\tau^{-1}(\sigma^{-1}(x_\tau^q)x_{\sigma^{-1}}) \equiv \sigma^{-1}(x_\tau^q)x_{\sigma^{-1}} \pmod{S_Q Q}.$$

Thus

$$\begin{aligned}\sigma\tau^{-1}\sigma^{-1}\tau^q(t) &\equiv x_\tau^q \sigma(x_{\sigma^{-1}})\sigma(x_{\tau^{-1}})x_\sigma t \pmod{S_Q Q^2} \\ &\equiv x_\tau^q \sigma(x_{\tau^{-1}})t \pmod{S_Q Q^2},\end{aligned}$$

because $\sigma(x_{\sigma^{-1}})x_\sigma = 1$.

Our next step is to find useful expressions for x_τ^q and $\sigma(x_{\tau^{-1}})$. Firstly, as $\tau^{-1} \in E$, we have

$$x_\tau \equiv \tau^{-1}(x_\tau) \pmod{S_Q Q} \Longrightarrow x_\tau^q \equiv \tau^{-1}(x_\tau)^q \pmod{S_Q Q}.$$

Secondly, we consider $\sigma(x_{\tau^{-1}})$. Since $\sigma(\alpha) \equiv \alpha^q \pmod{Q}$, for all $\alpha \in S$, because $\tilde{\sigma}$ is the Frobenius automorphim, we have $\sigma(x) \equiv x^q \pmod{S_Q Q}$, for all $x \in S_Q Q$: For $x = \frac{r}{u} \in S_Q \subset L$, we have

$$\sigma(x) = \frac{\sigma(r)}{\sigma(u)} = \frac{r^q + q_1}{u^q + q_2} = \frac{r^q}{u^q} - \frac{r^q q_2 - u^q q_1}{u^q(u^q + q_2)} \equiv \frac{r^q}{u^q} \pmod{S_Q Q}.$$

Hence

$$\sigma(x_{\tau^{-1}}) \equiv x_{\tau^{-1}}^q \pmod{S_Q Q}.$$

Using these two expressions, we have

$$\sigma\tau^{-1}\sigma^{-1}\tau^q(t) \equiv x_\tau^q \sigma(x_{\tau^{-1}})t \equiv \tau^{-1}(x_\tau)^q x_{\tau^{-1}}^q t \pmod{S_Q Q^2}.$$

As $\tau^{-1}(x_\tau)x_{\tau^{-1}} = 1$, we finally obtain

$$\sigma\tau^{-1}\sigma^{-1}\tau^q(t) \equiv t \pmod{S_Q Q^2},$$

and the result follows. □

Corollary 13.9 *If the decomposition group D is abelian, then then $|E/V_1|$ divides $q-1$.*

PROOF If D is abelian, then the action of D on E/V_1 is trivial, i.e., $\sigma \cdot \tau V_1 = \tau V_1$, for all $\sigma \in D$ and cosets $\tau V_1 \in E/V_1$. It follows that $\hat{\sigma}$ is the identity for every $\sigma \in D$. If σ is such that its image under the mapping ψ is the Frobenius automorphism, then from Proposition 13.19 $\hat{\sigma}(\tau V_1) = \tau^q V_1$. Thus we have $\tau V_1 = \tau^q V_1$, or $\tau^{q-1}(\tau V_1) = \tau V_1$. Hence the order of τV_1 divides $q-1$. However, E/V_1 is cyclic, so if τV_1 is a generator of E/V_1, then its order is the cardinal of the group, hence the result. □

Remark In the proof of Theorem 13.17 we showed that $|E/V_1|$ divides $q'-1$, where $q' = |S/Q|$. On the other hand, in Corollary 13.9 we show that $|E/V_1|$ divides $q-1$, where $q = |R/Q|$. As $q-1$ divides $q'-1$, when D is abelian we obtain a stronger result.

Chapter 14

Number fields and lattices

Before reading this chapter we advise the reader unfamiliar with lattices in euclidian space to read our appendix on the subject. There we have brought together the basic notions on the subject and, in particular, we state and prove Minkowski's convex body theorem.

14.1 Number rings as lattices

We consider a number field K, such that $[K : \mathbf{Q}] = n$, with associated number ring R. There are n monomorphisms of K into $\mathbf{C}$ which fix $\mathbf{Q}$. (If K is a normal extension of $\mathbf{Q}$, then the monomorphisms are automorphisms of K and so form the Galois group $Gal(K/\mathbf{Q})$.) Let $\sigma_1, \ldots, \sigma_r$ be the monomorphisms with image in $\mathbf{R}$. The others occur as pairs of complex conjugates, which we write $\tau_1, \bar{\tau}_1, \ldots, \tau_s, \bar{\tau}_s$; clearly, $n = r + 2s$. We obtain a mapping $\phi : K \longrightarrow \mathbf{R}^n$ by setting

$$\phi(\alpha) = (\sigma_1(\alpha), \ldots, \sigma_r(\alpha), \mathrm{Re}\ \tau_1(\alpha), \mathrm{Im}\ \tau_1(\alpha), \ldots, \mathrm{Re}\ \tau_s(\alpha), \mathrm{Im}\ \tau_s(\alpha)),$$

for all $\alpha \in K$. This mapping is a monomorphism from the additive group of K into the additive group of $\mathbf{R}^n$. The image of R, which we note Λ_R, is a subgroup of the additive group of $\mathbf{R}^n$. We claim that Λ_R is a lattice. To see this, let $(\alpha_1, \ldots, \alpha_n)$ be an integral basis of R. Clearly

$$\Lambda_R = \{v \in \mathbf{R}^n : v = \sum_{i=1}^{n} a_i \phi(\alpha_i), a_i \in \mathbf{Z}\}.$$

In order to show that $A = \{\phi(\alpha_1), \ldots, \phi(\alpha_n)\}$ is an independant set in $\mathbf{R}^n$ we consider the determinant D of the matrix having these elements as rows. Applying appropriate column operations we obtain that D is the product of $(-2i)^{-s}$ and the determinant D' of the matrix with rows

$$\sigma_1(\alpha_i) \ldots \sigma_r(\alpha_i)\ \tau_1(\alpha_i)\ \overline{\tau_1(\alpha_i)} \ldots \tau_s(\alpha_i)\ \overline{\tau_s(\alpha_i)}$$

However,

$$D'^2 = \mathrm{disc}(R) \neq 0,$$

since any integral basis of R is a basis of the vector space K over $\mathbf{Q}$ and Proposition 10.8 holds. Thus A is an independant set. It follows that Λ_R is a lattice.

We recall that the determinant of a lattice Λ is the volume of a parallelepiped formed by the vectors of any basis $(u_i)_{i=1}^n$. This volume is the absolute value of the determinant of the matrix

U having these vectors as columns. Hence $\det \Lambda_R = |D|$. Now,

$$D = (-2i)^{-s} D' \Longrightarrow D^2 = (-1)^s 2^{-2s} D'^2,$$

therefore

$$\det \Lambda_R = |D| = 2^{-s}\sqrt{|\mathrm{disc}(R)|}.$$

If I is a nonzero ideal of R, then we claim that $\Lambda_I = \phi(I)$ is a sublattice of Λ_R. To see this, we notice that I is a free abelian group of rank n and hence has a basis $(\beta_1, \ldots, \beta_n)$. The set $B = \{\phi(\beta_1), \ldots, \phi(\beta_n)\}$ generates $\phi(I)$ over $\mathbf{Z}$ and is independant, hence Λ_I is a sublattice of Λ_R. Also, the index of Λ_I in Λ_R is that of I in R, since the mapping

$$\pi : R/I \longrightarrow \Lambda_R/\Lambda_I, r + I \longmapsto \phi(r) + \Lambda_I$$

is a bijection. Therefore, using Theorem G.5, we have

$$\|I\| = |R/I| = \frac{\det \Lambda_I}{\det \Lambda_R} \Longrightarrow \det \Lambda_I = \det \Lambda_R \|I\| = 2^{-s}\sqrt{|\mathrm{disc}(R)|}\|I\|.$$

14.2 Some calculus

In this section we consider a particular subset of $\mathbf{R}^n$, with $n \geq 1$, which we will use further on. We devote a section to the calculation of its volume. We suppose that $n = r + 2s$ and set

$$A = \{x \in \mathbf{R}^n : |x_1| + \cdots + |x_r| + 2\left(\sqrt{x_{r+1}^2 + x_{r+2}^2} + \cdots + \sqrt{x_{n-1}^2 + x_n^2}\right) \leq n\}.$$

Before considering the volume of the set A, we observe certain of its properties. For $x = (x_1, \ldots, x_r, x_{r+1}, \ldots, x_{r+2s}) \in \mathbf{R}^n$, we set

$$S(x) = x_1 \cdots x_r (x_{r+1}^2 + x_{r+2}^2) \cdots (x_{n-1}^2 + x_n^2).$$

Proposition 14.1 *The set A is a convex, compact, centrally symmetric subset of R^n, such that, for all $x \in A$,*

$$|S(x)| \leq 1.$$

PROOF A is clearly convex, compact and centrally symmetric. The arithmetic mean of the numbers

$$|x_1|, \ldots, |x_r|, \sqrt{x_{r+1}^2 + x_{r+2}^2}, \sqrt{x_{r+1}^2 + x_{r+2}^2}, \ldots, \sqrt{x_{n-1}^2 + x_n^2}, \sqrt{x_{n-1}^2 + x_n^2}$$

is at most 1 and their geometric mean, which is $\sqrt[n]{|S(x)|}$ is bounded above by the arithmetic mean, therefore $|S(x)| \leq 1$. □

We now turn to the calculation of the volume of A.

Theorem 14.1 *We have*

$$\mathrm{vol}\, A = \frac{n^n}{n!} 2^r \left(\frac{\pi}{2}\right)^s.$$

PROOF We consider the volume $v_{r,s}(t)$ of the subset of $\mathbf{R}^{r+2s}$

$$A_{r,s}(t)=\{x\in\mathbf{R}^n:|x_1|+\cdots+|x_r|+2\left(\sqrt{x_{r+1}^2+x_{r+2}^2}+\cdots+\sqrt{x_{n-1}^2+x_n^2}\right)\le t\}.$$

As $A_{r,s}(t)=tA_{r,s}(1)$, we have

$$v_{r,s}(t)=t^{r+2s}v_{r,s}(1). \tag{14.1}$$

Given that vol $A=v_{r,s}(r+2s)$, it is sufficient to show that

$$v_{r,s}(1)=\frac{1}{(r+2s)!}2^r\left(\frac{\pi}{2}\right)^s. \tag{14.2}$$

We first consider the case where $r=0$; this implies that $s\ge 1$, because $n\neq 0$. For $s=1$ we have

$$v_{0,s}(1)=\int\int_{x^2+y^2\le\frac14}1\;dxdy=\frac{\pi}{4}.$$

We now suppose that $s>1$ and aim to find a relation between $v_{0,s}(1)$ and $v_{0,s-1}(1)$. To simplify the notation we let f be the characteristic function of $A_{0,s}(1)$. f is a function in the variables $x_1,\ldots,x_{2s}$. Let us set $u=(x_1,\ldots,x_{2s-2}$ and $v=(x_{2s-1},x_{2s})$. If f_v is the function in u obtained by fixing v and we set

$$\phi(v)=\int f_v(u)\;du,$$

then, by Fubini's theorem (see for example [20]), we have

$$\int\phi(v)\;dv=\int\int f(u,v)\;dudv.$$

However, $f_v(u)$ is the characteristic function of the set

$$A_v=\left\{(x_1,\ldots,x_{2s-2})\in\mathbf{R}^{2s-2}:2\left(\sqrt{x_1^2+x_2^2}+\ldots+\sqrt{x_{2s-3}^2+x_{2s-2}^2}\right)\le 1-2\sqrt{x_{2s-1}^2+x_{2s}^2}\right\}.$$

From equation (14.1),

$$\int f_v(u)du=\left(1-2\sqrt{x_{2s-1}^2+x_{2s}^2}\right)^{2s-2}v_{0,s-1}(1)$$

and so, writing $f(u,v)$ for $f_v(u)$,

$$\begin{aligned}\int f(u,v)\;dudv\;=\;v_{0,s}(1)\;&=\;\int\int_{x^2+y^2\le\frac14}v_{0,s-1}(1)\left(1-2\sqrt{x^2+y^2}\right)^{2s-2}\;dxdy\\&=\;v_{0,s-1}(1)\int\int_{x^2+y^2\le\frac14}\left(1-2\sqrt{x^2+y^2}\right)\;dxdy.\end{aligned}$$

Using polar coordinates we obtain

$$\begin{aligned}\int\int_{x^2+y^2\le\frac14}\left(1-2\sqrt{x^2+y^2}\right)^{2s-2}\;dxdy\;&=\;\int_0^{2\pi}\int_0^{\frac12}(1-2\rho)^{2s-2}\rho\;d\rho d\theta\\&=\;2\pi\int_0^{\frac12}(1-2\rho)^{2s-2}\rho\;d\rho\\&=\;\frac{\pi}{2}\int_0^1u^{2s-2}(1-u)\;du\\&=\;\frac{\pi}{2}\left(\frac{1}{2s-1}-\frac{1}{2s}\right)\;=\;\frac{\pi}{2}\frac{1}{2s(2s-1)}\end{aligned}$$

and hence the recurrence relation

$$v_{0,s}(1) = v_{0,s-1}(1)\frac{\pi}{2}\frac{1}{2s(2s-1)}.$$

With an induction argument we find that

$$v_{0,s}(1) = \left(\frac{\pi}{2}\right)^s \frac{1}{(2s)!}.$$

We now consider the case where $r > 0$ and $s \geq 1$. Let g be the characteristic function of $A_{r,s}(1)$. g is a function in the variables $x_1, \ldots, x_{2s}$. Let us set $u = (x_1, \ldots, x_{r-1}, x_{r+1}, \ldots, x_{2s}$ and $v = x_r$. If g_v is the function in u obtained by fixing v and we set

$$\psi(v) = \int g_v(u)\, du,$$

then, by Fubini's theorem, we have

$$\int \psi(v)\, dv = \int\int g(u,v)\, dudv.$$

However, $g_v(u)$ is the characteristic function of the set

$$\begin{aligned} B_v &= \Big\{(x_1, \ldots, x_{r-1}, x_{r+1}, \ldots, x_{2s}) \in \mathbf{R}^{r-1+2s} : |x_1| + \cdots + |x_{r-1}| \\ &+ 2\left(\sqrt{x_{r+1}^2 + x_{r+2}^2} + \ldots + \sqrt{x_{2s-1}^2 + x_{2s}^2}\right) \leq 1 - |x_r|\Big\} \end{aligned}$$

From equation (14.1), we obtain

$$\int g_v(u)\, du = (1 - |x_r|)^{r-1+2s} v_{r-1,s}(1)$$

and so, writing $g(u,v)$ for $g_v(u)$,

$$\begin{aligned} \int g(u,v)\, dudv = v_{r,s}(1) &= \int_{-1}^{1} (1 - |x|)^{r-1+2s} v_{r-1,s}(1)\, dx \\ &= 2v_{r-1,s}(1) \int_0^1 (1-x)^{r-1+2s} dx \\ &= \frac{2}{r+2s} v_{r-1,s}(1). \end{aligned}$$

Using this recurrence relation and the value of $v_{0,s}(1)$, which we have already determined, we obtain the expression for $v_{r,s}(1)$ in equation (14.2), namely

$$v_{r,s}(1) = \frac{1}{(r+2s)!} 2^r \left(\frac{\pi}{2}\right)^s.$$

There is one case we have not considered, namely that where $r > 0$ and $s = 0$. However, this is not difficult. As above, for $r > 1$ we may obtain the recurrence relation

$$v_{r,0}(1) = \frac{2}{r} v_{r-1,0}(1).$$

This, together with the fact that $v_{1,0}(1) = 2$, enables us to establish by induction that

$$v_{r,0}(1) = \frac{2^r}{r!}$$

and hence

$$\text{vol } A = \frac{n^n}{n!} 2^n,$$

as desired. This finishes the proof. □

In the next section we will use the results we have considered here to prove certain important properties of number rings.

14.3 The ideal class group of a number ring

We now return to number rings. As usual, let K be a number field with number ring R. We recall that in the first section of this chapter we defined a monomorphism $\phi : K \longrightarrow \mathbf{R}^n$, where n is the degree of the extension of K over $\mathbf{Q}$, such that the image of R is a lattice Λ_R. We begin with a property of general lattices.

Theorem 14.2 *If A is a compact, convex, centrally symmetric subset of $\mathbf{R}^n$, with* vol $A > 0$*, satisfying the property*

$$a \in A \Longrightarrow |S(a)| \leq 1,$$

then every lattice $\Lambda \subset \mathbf{R}^n$ contains a nonzero point x such that

$$|S(x)| \leq \frac{2^n}{\text{vol } A} \det \Lambda.$$

PROOF We use Minkowski's convex body theorem (Theorem G.4). First we set $B = tA$, where $t > 0$ and

$$t^n = \frac{2^n}{\text{vol } A} \det \Lambda.$$

Then

$$\text{vol } B = t^n \text{vol } A = 2^n \det \Lambda.$$

From Minkowski's theorem, B contains a nonzero lattice point x. As $\frac{x}{t} \in A$, we have

$$|S(x)| = t^n |S(\frac{x}{t})| \leq \frac{2^n}{\text{vol } A} \det \Lambda.$$

This ends the proof. □

Suppose now that we can write $n = r + 2s$ and we take A to be the corresponding set defined in the previous section, then

$$\text{vol } A = \frac{n^n}{n!} 2^r \left(\frac{\pi}{2}\right)^s$$

and so we obtain

Corollary 14.1 *Every lattice $\Lambda \subset \mathbf{R}^n$ contains a nonzero point x such that*

$$|S(x)| \leq \frac{n!}{n^n} \left(\frac{8}{\pi}\right)^s \det \Lambda.$$

Remark We emphasize that the set A and the application S depend on the values of r and s.

We now return to the number field K.

Lemma 14.1 *If $\alpha \in K$, then for $x = \phi(\alpha)$, we have*

$$S(x) = N_{K/\mathbf{Q}}(\alpha).$$

PROOF Since

$$\phi(\alpha) = (\sigma_1(\alpha), \ldots, \sigma_r(\alpha), \mathrm{Re}\ \tau_1(\alpha), \mathrm{Im}\ \tau_1(\alpha), \ldots \mathrm{Re}\ \tau_s(\alpha), \mathrm{Im}\ \tau_s(\alpha)),$$

then, by Proposition 10.2,

$$S(\phi(\alpha)) = \sigma_1(\alpha) \cdots \sigma_r(\alpha)\tau_1(\alpha)\bar{\tau}_1(\alpha) \cdots \tau_s(\alpha)\bar{\tau}_s(\alpha) = N_{K/\mathbf{Q}}(\alpha).$$

This ends the proof. □

Theorem 14.3 *A nonzero ideal I in R, the number ring of K, contains a nonzero element α such that*

$$|N_{K/\mathbf{Q}}(\alpha)| \leq \frac{n!}{n^n}\left(\frac{4}{\pi}\right)^s \sqrt{|disc(R)|}\ \|I\|.$$

PROOF Corresponding to the ideal I is the lattice $\Lambda_I = \phi(I)$. From Lemma 14.1, there exists a nonzero lattice point x such that

$$|S(x)| \leq \frac{n!}{n^n}\left(\frac{8}{\pi}\right)^s \det \Lambda_I.$$

There exists α nonzero in I such that $x = \phi(\alpha)$ and, from Lemma 14.1, $S(x) = N_{K/\mathbf{Q}}(\alpha)$. In addition, in Section 14.1 it is established that $\det \Lambda_I = \frac{1}{2^s}\sqrt{|\mathrm{disc}(R)|}\|I\|$, therefore

$$|N_{K/\mathbf{Q}}(\alpha)| \leq \frac{n!}{n^n}\left(\frac{4}{\pi}\right)^s \sqrt{|\mathrm{disc}(R)|}\ \|I\|,$$

as required. □

From this theorem we may deduce two important results, namely

- the number of ideal classes in a number ring is finite;
- for any number field $K \neq \mathbf{Q}$, there is a prime number p which is ramified in the number ring R of K.

Let us consider the first question. We set $\lambda = \frac{n!}{n^n}\left(\frac{4}{\pi}\right)^s \sqrt{|\mathrm{disc}(R)|}$. (The number λ is called a *Minkowski bound.*)

Proposition 14.2 *Every ideal class of R contains an ideal J such that $\|J\| \leq \lambda$.*

PROOF Let C be an ideal class. As the ideal classes form a group, there exists an ideal class C^{-1}. Let I be an ideal in the class C^{-1}. From Theorem 14.3, there exists a nonzero $\alpha \in I$ such that $|N_{K/\mathbf{Q}}(\alpha)| \leq \lambda\|I\|$. I contains the principal ideal (α), which implies that I divides (α), i.e., there exists an ideal J such that $IJ = (\alpha)$. As (α) is an element of identity class, J lies in the class C. Therefore, using Theorems 13.2 and 13.4, we have

$$|N_{K/\mathbf{Q}}(\alpha)| = \|(\alpha)\| = \|I\|\|J\|,$$

which implies that

$$\|J\| = \frac{|N_{K/\mathbf{Q}}(\alpha)|}{\|I\|} \leq \frac{\|I\|\lambda}{\|I\|} = \lambda,$$

as required. □

We may now handle the first question.

Theorem 14.4 *If R is a number ring, then there is only a finite number of ideal classes in R.*

PROOF We claim that there is only a finite number of nonzero ideals J such that $\|J\| \leq \lambda$. Let J be such an ideal. If the decomposition of J into prime ideals is

$$J = P_1^{n_1} \cdots P_s^{n_s},$$

then, by Theorem 13.2,

$$\|P_1\|^{n_1} \cdots \|P_s\|^{n_s} \leq \lambda.$$

Each prime ideal P_i lies over a unique prime number p_i and $\|P_i\| = p_i^{u_i}$, for some $u_i \in \mathbf{N}*$. Hence

$$\|P_i\|^{n_i} = p_i^{u_i n_i} \leq \lambda \Longrightarrow p_i \leq \lambda.$$

There is only a finite number of prime numbers p such that $p \leq \lambda$, thus in the decomposition of J there can only be prime ideals lying over a finite number of prime numbers. However, from Theorem 13.1, we know that there is only a finite number of prime ideals lying over a given prime number, so in the decomposition of J there can only be members of a certain finite set of prime ideals. If P is one such prime and P^m is in the decomposition of J, then $\|P\|^m \leq \lambda$, so there can only be finite number of powers of P in the decomposition of ideals J. It now follows that there is only a finite number of nonzero ideals J such that $\|J\| \leq \lambda$, as claimed.

As any class contains a nonzero ideal J such that $\|J\| \leq \lambda$, there can only be a finite number of ideal classes. □

Remark To prove Theorem 14.4 we only need to know that there is some constant λ such that every ideal class of R contains an ideal J satisfying the inequality $\|J\| \leq \lambda$. There exists at least one other such constant, namely

$$H_K = \prod_{i=1}^{n} \sum_{j=1}^{n} |\sigma_i(b_j)|,$$

where $\mathcal{B} = \{b_1, \ldots, b_n\}$ is an integral basis of O_K and $\sigma_1, \ldots, \sigma_n$ are the embeddings of K in $\mathbf{C}$ (see [15]). This constant is known as Hurwitz's constant, hence the notation, although it is not certain that Hurwitz was the first to find it. It has the disadvantage of being dependant on the basis chosen and is also in general larger than Minkowski's constant. We will see further on that the bounding constant can be used in determining the class group and it is important that this be as small as possible.

Definition The cardinal of the class group of a number ring O_K is referred to as the *class number of K*. In general we write $h(K)$ (or just h) for the class number.

We now turn to the second question.

Theorem 14.5 *For any number field $K \neq \mathbf{Q}$, there is a prime number p which is ramified in the number ring R of K.*

PROOF From Proposition 14.2 we know that there is a nonzero ideal J such that

$$\|J\| \leq \lambda = \frac{n!}{n^n}\left(\frac{4}{\pi}\right)^s \sqrt{|\mathrm{disc}(R)|} \Longrightarrow \sqrt{|\mathrm{disc}(R)|} \geq \frac{n^n}{n!}\left(\frac{\pi}{4}\right)^{\frac{n-r}{2}},$$

because $n = r + 2s$. As $\frac{\pi}{4} < 1$, we have

$$\sqrt{|\mathrm{disc}(R)|} \geq \frac{n^n}{n!}\left(\frac{\pi}{4}\right)^{\frac{n}{2}}.$$

For $n \geq 1$ the sequence $(\frac{n^n}{2^n n!})$ is increasing, so

$$\sqrt{|\mathrm{disc}(R)|} \geq \frac{1}{2}\pi^{\frac{n}{2}} > 1,$$

when $n \geq 2$; hence some prime number p divides $|\mathrm{disc}(R)|$. From Theorem 13.14, p is ramified in R. □

The Minkowski bound (or equivalent bound) is useful in determining the class number. In particular, if λ is less than 2, then the class number is 1, because every ideal class contains the unique ideal with norm 1, namely R.

For example, consider the quadratic number field $K = \mathbf{Q}(\sqrt{5})$. From Exercise 11.4 we know that $\mathrm{disc}(O_K) = 5$. Also, there are no complex embeddings of K into $\mathbf{C}$. Therefore $\lambda = \frac{2!}{2^2}(\frac{4}{\pi})^0\sqrt{5} = \frac{\sqrt{5}}{2} < 2$ and the class number is 1.

As a second example, we take the quadratic number field $L = \mathbf{Q}(\sqrt{-2})$. From the example before Exercise 11.4, we know that $\mathrm{disc}(O_L) = -8$. As there are two complex embeddings of L into $\mathbf{C}$, we have $\lambda = \frac{2!}{2^2}(\frac{4}{\pi})^1\sqrt{8} = \frac{4}{\pi}\sqrt{2} < 2$, so, as in the first example, the class number is 1.

14.4 Dirichlet's unit theorem

Let K be a number field of degree n over $\mathbf{Q}$. We recall that, if $\alpha \in O_K$ is a unit, then $N_{K/\mathbf{Q}}(\alpha) = \pm 1$ (Proposition 11.3).

We define the monomorphism ϕ as in Section 14.1 and let U_K be the set of units in O_K.

As in Section 14.1, we let r be the number of real and $2s$ the number of complex embeddings of K into $\mathbf{C}$ ($n = r + 2s$). The complex embeddings arise in pairs, namely τ_i and $\bar{\tau}_i$, for $i = 1, \ldots, s$. For $i = 1, \ldots, s$, let us set $\sigma_{r+i} = \tau_i$. We define a new mapping $\lambda : O_K^* \longrightarrow \mathbf{R}^{r+s}$, which we will refer to as the *logarithmic mapping*, by

$$\lambda(\alpha) = (\ln|\sigma_1(\alpha)|, \ldots, \ln|\sigma_r(\alpha)|, 2\ln|\sigma_{r+1}(\alpha)|, \ldots, 2\ln|\sigma_{r+s}(\alpha)|).$$

Proposition 14.3 *Let Y be a bounded subset of $\mathbf{R}^{r+s}$ and $X = \{\alpha \in O_K^* : \lambda(\alpha) \in Y\}$. Then X is a finite set.*

PROOF As Y is bounded, all the coordinates of $\lambda(\alpha)$ are bounded and it follows that the elements $|\sigma_i(\alpha)|$ belong to a bounded interval. Hence the absolute values of the elementary symmetric functions of the $\sigma_i(\alpha)$ lie in some bounded interval. However, the elementary symmetric functions of the $\sigma_i(\alpha)$ are the coefficients of the characteristic polynomial of α (Proposition 10.2), which is a power of the minimal polynomial $m(\alpha, \mathbf{Q})$ (Proposition 10.1). As this polynomial has integer coefficients, there is a real bounded interval containing the coefficients of the characteristic polynomial of α and these are all integers. Therefore there can only be a finite number of characteristic polynomials of elements α belonging to X. Since α is a root of its characteristic polynomial, X is a finite set. □

Corollary 14.2 *The kernel G of λ is a finite group.*

PROOF To see that G is finite, it is sufficient to take $Y = \{0\}$ in Proposition 14.3. We also need to show that G is a group. If $\alpha \in G$, then $|\sigma_i(\alpha)| = 1$, for all i, From Proposition 10.2,

$$|N_{K/\mathbf{Q}}(\alpha)| = \prod_{i=1}^{n} |\sigma_i(\alpha)| = 1,$$

so α is a unit. Therefore G is the kernel of λ restricted to U_K, which is a homomorphism. Hence G is a group. □

We now examine G in more detail.

Proposition 14.4 *The kernel G of λ consists of all the roots of unity of K and is cyclic.*

PROOF As G is a finite subgroup of K^*, by Theorem 3.3, G is cyclic. If n is the order of G and $\alpha \in G$, then $\alpha^n = 1$, hence all elements of G are roots of unity.

Suppose that $\alpha \in K$ and $\alpha^m = 1$, for some $m \in \mathbf{N}^*$. Then $\alpha \in O_K$ and, for every i, with $i = 1, \ldots, r+s$,

$$|\sigma_i(\alpha)|^m = |\sigma_i(\alpha^m)| = |1| = 1.$$

Thus, for all i, $|\sigma_i(\alpha)| = 1$, so $\ln|\sigma_i(\alpha)| = 0$, which implies that $\alpha \in G$. □

We now turn to the analysis of the group of units U_K. We recall that a subgroup H of a topological group G is discrete if the topology induced on H is discrete. For example, $(\mathbf{Z}^n, +)$ is a discrete subgroup of $(\mathbf{R}^n, +)$ with the usual metric topology.

Proposition 14.5 *If K is a number field, then its group of units U_K is finitely generated and there exists $t \leq r+s$ such that U_K is isomorphic to the product $G \times \mathbf{Z}^t$.*

PROOF From Proposition 14.3, every bounded subset of $\mathbf{R}^{r+s}$ contains only a finite number of elements of $\lambda(U_K)$, hence $\lambda(U_K)$ is a discrete subgroup of $\mathbf{R}^{r+s}$. From Theorem G.6, there exists $t \leq r+s$ such that $\lambda(U_K)$ is a lattice in $\mathbf{R}^t$, hence a free abelian group of rank t (Corollary G.1). By the first isomorphism theorem $\lambda(U_K)$ is isomorphic to the quotient group U_K/G, hence U_K/G is a free abelian group of rank t, which we write multiplicatively. If $\mathcal{B} = \{G\alpha_1, \ldots, G\alpha_t\}$ is a basis of U_K/G and $G\alpha$ belongs to U_K/G, then $G\alpha$ is a finite product of powers of the $G\alpha_i$:

$$G\alpha = G\alpha_1^{k_1} \cdots G\alpha_t^{k_t} = G\alpha_1^{k_1} \cdots \alpha_t^{k_t},$$

where the k_i are unique. Thus there exists $\beta \in G$ such that $\alpha = \beta\alpha_1^{k_1} \cdots \alpha_t^{k_t}$. Clearly, β is unique. From Proposition 14.4 , G is cyclic, so U_K is finitely generated. We also notice that the mapping

$$g : U_K \longrightarrow G \times \mathbf{Z}^t, \alpha \longmapsto (\beta, k_1, \ldots, k_t)$$

is a group isomorphism. $\square$

We will now aim to make precise the value of t. If $\alpha \in U_K$ then

$$\pm 1 = N_{K/\mathbf{Q}}(\alpha) = \prod_{i=1}^{n} \sigma_i(\alpha) = \prod_{i=1}^{r} \sigma_i(\alpha) \prod_{j=r+1}^{r+s} \sigma_j(\alpha)\overline{\sigma_j(\alpha)},$$

which implies that

$$0 = \sum_{i=1}^{r} \ln|\sigma_i(\alpha)| + \sum_{j=r+1}^{r+s} 2\ln|\sigma_j(\alpha)|.$$

Thus $\lambda(\alpha)$ belongs to the hyperplane

$$H = \{(x_1, \ldots, x_{r+s}) : \sum_{i=1}^{r+s} x_i = 0\},$$

which has dimension $r+s-1$. Hence $\lambda(U_K)$ may be considered a discrete subgroup of $\mathbf{R}^{r+s-1}$ and it follows that $\lambda(U_K)$ is a lattice in $\mathbf{R}^t$, where $t \leq r+s-1$ (Theorem G.6). Therefore $\lambda(U_K)$ is a free abelian group of rank $t \leq r+s-1$ (Corollary G.1). This improves our estimate of t found in the proof of Proposition 14.5, where we only found that the rank t of $\lambda(U_K)$ was bounded by $r+s$. It follows that U_K is isomorphic to the product $G \times \mathbf{Z}^t$, with $t \leq r+s-1$.

If $r+s=1$, then $t=0$ and U_K is isomorphic to the group G. In fact, in all cases we have equality, i.e., $t = r+s-1$. This is the content of Dirichlet's unit theorem, which we will now prove. The proof is much longer than those of the results we have encountered up to now in this section.

Theorem 14.6 *The group U_K of the number field K is isomorphic to the product $G \times \mathbf{Z}^t$, where G is the finite cyclic group consisting of all the roots of unity in K and $t = r+s-1$.*

PROOF We have already covered the case where $r+s=1$, so we will suppose that $r+s>1$. Let W be the $\mathbf{R}$-span of $\lambda(U_K)$. Above we defined a certain hyperplane H. Since $\lambda(U_K)$ is contained in H, W is a subspace of H. We aim to show that $W = H$. To do so, it is sufficient to prove that $W^\perp \subset H^\perp$, or equivalently that $x \notin H^\perp \Longrightarrow x \notin W^\perp$. We fix $x = (x_1, \ldots, x_{r+s}) \notin H^\perp$ and define a function $f : K^* \longrightarrow \mathbf{R}$ by

$$f(\alpha) = x_1 \ln|\sigma_1(\alpha)| + \cdots + x_r \ln|\sigma_r(\alpha)| + x_{r+1} 2\ln|\sigma_{r+1}(\alpha)| + x_{r+s} 2\ln|\sigma_{r+s}(\alpha)|.$$

To show that $x \notin W^\perp$ we will find $u \in U_K$ such that $f(u) \neq 0$. We will procede by steps.

<u>Step 1: An application of Minkowski's theorem</u>

Let

$$A = \sqrt{|\mathrm{disc}(O_K)|}(\frac{2}{\pi})^s \in \mathbf{R}_+^*.$$

and let us choose $c_1, \ldots, c_{r+s} \in \mathbf{R}_+^*$ such that

$$c_1 \cdots c_r \cdot (c_{r+1} \cdots c_{r+s})^2 = A.$$

We define S to be the subset of $\mathbf{R}^n$ composed of elements $(x_1, \ldots, x_n)$ such that, for $i = 1, \ldots, r$, $|x_i| \leq c_i$, and $x_{r+1}^2 + x_{r+2}^2 \leq c_{r+1}^2$, $x_{r+3}^2 + x_{r+4}^2 \leq c_{r+2}^2$, $\ldots$,$x_{n-1}^2 + x_n^2 \leq c_{r+s}^2$. We may view S as a product of r intervals and s discs. We obtain

$$\text{vol }(S) = \prod_{r=1}^{r}(2c_i) \prod_{i=r+1}^{r+s} (\pi c_i^2) = 2^r \pi^s A.$$

We may associate a lattice Λ_{O_K} $(= \phi(O_K))$ with O_K. From Section 14.1 we have

$$\det \Lambda_{O_K} = 2^{-s} \sqrt{|\text{disc}(O_K)|}$$

and so

$$\begin{aligned} 2^r \pi^s A &= 2^r \pi^s \sqrt{|\text{disc}(O_K)|}(\frac{2}{\pi})^s \\ &= 2^{r+s} \sqrt{|\text{disc}(O_K)|} \\ &= 2^{r+s} 2^s \det \Lambda_{O_K} \\ &= 2^n \det \Lambda_{O_K}, \end{aligned}$$

i.e.,

$$\text{vol }(S) = 2^n \det \Lambda_{O_K}.$$

From Minkowski's theorem (Theorem G.4), S contains a nonzero lattice point, i.e., the set $S \cap \phi(O_K)$ contains a nonzero element. Therefore there exists $\beta \in O_K$ which is nonzero and such that $|\sigma_i(\beta)| \leq c_i$, for $i = 1, \ldots, r+s$.

Step 2: Properties of the point β

First we consider the norm of β. To simplify the notation, for $i = 1, \ldots, s$, we set $\sigma_{r+i} = \tau_i$ and $\sigma_{r+s+i} = \overline{\tau_i}$. Then

$$\begin{aligned} |N_{K/\mathbf{Q}}(\beta)| &= |\prod_{i=1}^{r+2s} \sigma_i(\beta)| \\ &= \prod_{i=1}^{r} |\sigma_i(\beta)| \prod_{i=r+1}^{r+s} |\sigma_i(\beta)|^2 \\ &\leq c_1 \cdots c_r \cdot (c_{r+1} \cdots c_{r+s})^2 = A. \end{aligned}$$

As β is nonzero we also have $|N_{K/\mathbf{Q}}(\beta)| \geq 1$, because the norm of an algebraic integer is an integer. Thus we have $1 \leq |N_{K/\mathbf{Q}}(\beta)| \leq A$.

We now use the norm to estimate the values of the elements $|\sigma_i(\beta)|$. Suppose that for some $i \leq r$ we have $|\sigma_i(\beta)| < \frac{c_i}{A}$. Then

$$1 \leq |N_{K/\mathbf{Q}}(\beta)| < c_1 \cdots \frac{c_i}{A} \cdots c_r \cdot (c_{r+1} \cdots c_{r+s})^2 = \frac{A}{A} = 1,$$

a contradiction, so $|\sigma_i(\beta)| \geq \frac{c_i}{A}$, for $i = 1, \ldots, r$. In the same way, $|\sigma_i(\beta)|^2 \geq \frac{c_i^2}{A}$, for $i = r+1, \ldots, r+s$. Thus we have

$$\frac{c_i}{|\sigma_i(\beta)|} \leq A, \ \ i = 1, \ldots, r \qquad \text{and} \qquad \left(\frac{c_i}{|\sigma_i(\beta)|}\right)^2 \leq A, \ \ i = r+1, \ldots, r+s. \qquad (14.3)$$

From Theorem 13.5, there is only a finite number of ideals in O_K of a given norm, therefore there exists a finite number of nonzero principal ideals $(\gamma_1), \ldots, (\gamma_m)$ of norm at most A. Since $\|(\beta)\| = |N_{K/\mathbf{Q}}(\beta)| \leq A$, we must have $(\beta) = (\gamma_k)$, for some k, so there exists a unit $u \in O_K$ such that $\beta = u\gamma_k$.

Step 3: Showing that $f(u) \neq 0$

For the point $x \notin H^\perp$ we define

$$a = a(c_1, \ldots, c_{r+s}) = x_1 \ln c_1 + \cdots + x_{r+1} 2 \ln c_{r+1} + \cdots .$$

We recall the definition of the function $f : K^* \longrightarrow \mathbf{R}$:

$$f(\alpha) = x_1 \ln |\sigma_1(\alpha)| + \cdots + x_{r+1} 2 \ln |\sigma_{r+1}(\alpha)| + \cdots .$$

Then

$$\begin{aligned}
|f(u) - a| &= |f(\beta) - f(\gamma_k) - a| \\
&\leq |f(\gamma_k)| + |a - f(\beta)| \\
&= |f(\gamma_k)| + |x_1(\ln c_1 - \ln |\sigma_1(\beta)|) + \cdots + 2x_{r+1}(\ln c_{r+1} - \ln |\sigma_{r+1}(\beta)|) + \cdots | \\
&= |f(\gamma_k)| + |x_1 \ln \left(\frac{c_1}{|\sigma_1(\beta)|}\right) + \ldots + x_{r+1} \ln \left(\frac{c_{r+1}}{|\sigma_{r+1}(\beta)|}\right)^2 + \cdots | \\
&\leq |f(\gamma_k)| + \ln A \sum_{i=1}^{r+s} |x_i| \\
&\leq \max |f(\gamma_k)| + \ln A \sum_{i=1}^{r+s} |x_i| = B.
\end{aligned}$$

where we have used the equations (14.3). If we can find a, which depends on the c_i, such that $|a| > B$, then $|f(u) - a| \leq B$ would imply that $|f(u)| > 0$. We will now show that it is possible to find such an element a.

We recall the definition of the hyperplane H:

$$H = \{z = (z_1, \ldots, z_{r+s}) \in \mathbf{R}^{r+s} : \sum_{i=1}^{r+s} z_i = 0\}.$$

Since $H^\perp$ is the vector subspace generated by the vector

$$v = (1, \ldots, 1) \in \mathbf{R}^{r+s},$$

$x \notin H^\perp$ implies that we cannot have $x_1 = \cdots = x_{r+s}$. To simplify the notation, we set $d_i = c_i$, for $i = 1, \ldots, r$ and $d_i = c_i^2$, for $i = r+1, \ldots, r+s$. Then

$$a = x_1 \ln d_1 + \cdots + x_{r+s} \ln d_{r+s}$$

and $\prod_{i=1}^{r+s} d_i = A$. As already stated there exist $x_i \neq x_j$. Without loss of generality, let us suppose that $i = 1$ and $j = 2$. If we set $d_3 = \cdots = d_{r+s} = 1$, then $d_1 d_2 = A$ and

$$\begin{aligned} |a| &= |\sum_{i=1}^{r+s} x_i \ln d_i| = |x_1 \ln d_1 + x_2 \ln d_2| \\ &= |x_1 \ln d_1 + x_2 \ln \frac{A}{d_1}| \\ &= |(x_1 - x_2) \ln d_1 + x_2 \ln A| \longrightarrow \infty, \end{aligned}$$

when $d_1 \longrightarrow \infty$. Hence we can find an element a such that $|a| > B$ and so $W = H$.

In Proposition 14.5 we saw that there are elements $\alpha_1, \ldots, \alpha_t \in U_K$ such that for any element $\alpha \in U_K$ we have $\alpha = \beta \alpha_1^{k_1} \cdots \alpha_t^{k_t}$, where β is a root of unity. Then

$$\lambda(\alpha) = \lambda(\beta \alpha_1^{k_1} \cdots \alpha_t^{k_t}) = k_1 \lambda(\alpha_1) + \cdots + k_t \lambda(\alpha_t).$$

It follows that the set $\mathcal{B} = \{\lambda(\alpha_1), \ldots, \lambda(\alpha_t)\}$ is a generating set of W and hence of H. Given that the dimension of H is $r+s-1$, we have $t \geq r+s-1$. However, we know that $t \leq r+s-1$, so we have $t = r+s-1$. We deduce that $\mathcal{B}$ is a basis of the vector space H. Also, $\lambda(U_K)$ is a free abelian group of rank t and the elements of $\mathcal{B}$ form an independant generating set, so $\mathcal{B}$ is also a basis of the free abelian group $\lambda(U_K)$. $\square$

Dirichlet's unit theorem implies that there are $t = r+s-1$ particular units in O_K such that any unit $\alpha \in O_K$ can be expressed uniquely in the form

$$\alpha = \beta \alpha_1^{k_1} \cdots \alpha_t^{k_t},$$

with β a root of unity and the k_i in $\mathbf{Z}$. The set $\{\alpha_1, \ldots, \alpha_t\}$, which is not unique, is called a *fundamental system of units.*

As an example, let us consider the cyclotomic field $K = \mathbf{Q}(\zeta)$, where $\zeta = e^{\frac{2\pi i}{p}}$, with p an odd prime number. The degree of the extension K over $\mathbf{Q}$ is $p-1$ and so there are $p-1$ embeddings in $\mathbf{C}$. As the applications σ_j, with $\sigma_j(\zeta) = \zeta^j$, for $j = 1, \ldots, p-1$, are distinct embeddings, all the embeddings are complex, i.e., $r = 0, 2s = p-1$, which implies that $t = 0 + \frac{p-1}{2} - 1 = \frac{p-3}{2}$. If $p = 3$, then the only units are the roots of unity. If $p \geq 5$, then there is an infinite number of units.

If $K = \mathbf{Q}(\sqrt{m})$ is an imaginary quadratic field, then there are no real embeddings and so $2s = n = 2 \Longrightarrow s = 1 \Longrightarrow t = 0$, so again the only units are the roots of unity.

Now we consider real quadratic fields, which are more interesting. If $K = \mathbf{Q}(\sqrt{m})$ is a real quadratic field, then there are no imaginary embeddings in $\mathbf{C}$, so $s = 0$ and $r = 2$. Thus $t = 1$ and there is an infinite number of units. There are only two roots of unity, namely ± 1, hence there exists an element $x \in U_K$ such that the elements $u \in U_K$ can be written $u = \pm x^n$, with $n \in \mathbf{Z}$. If u is a unit, then so are $-u$, $\frac{1}{u}$ and $-\frac{1}{u}$. This implies that there are units u with $u > 1$. Let us set U_K^+ for the set of such units. The elements of U_K can be determined from those of U_K^+: $u \in U_K$ if and only if there exists $v \in U_K^+$ such that $u = \pm v$ or $u = \pm \frac{1}{v}$.

Let us look more closely at the set U_K^+. If $v \in U_K^+$, then $v = \pm x^n$, which implies that $v = |x|^n$. Clearly $|x| \in U_K$. If $|x| < 1$, then we may replace x by $\frac{1}{x}$, which ensures that $v = |x|^n$, with $n \in \mathbf{N}^*$. It is clear that $|x|$ is the minimum of U_K^+ and that the elements of U_K^+ are the positive powers of this minimum, which we call the *fundamental unit of* K.

We now consider how we might calculate the fundamental unit. There are different approaches to this question. We will give an elementary method. There are two cases.

Case 1: $m \equiv 2, 3 \pmod 4$ The algebraic integers are of the form $x = a + b\sqrt{m}$, with $a, b \in \mathbf{Z}$ (see the proof of Theorem 11.6). The units are those whose norm is ± 1, i.e., $a^2 - b^2 m = \pm 1$. We seek the smallest such element whose value is greater than 1. Here is a simple method to find it: Compute mb^2 for $b = 1, 2, 3 \ldots$ until either $mb^2 + 1$ or $mb^2 - 1$ is a square a^2, where $a > 0$. Then set $u = a + b\sqrt{m}$. u is the fundamental unit.

Example Let $m = 6$. Then $6 \cdot 1^2 \pm 1$ is not a square. However, $6 \cdot 2^2 = 24$ and $24 + 1 = 5^2$, hence the fundamental unit is $5 + 2\sqrt{6}$.

Case 2: $m \equiv 1 \pmod 4$ The algebraic integers are of the form $x = \frac{1}{2}(a + b\sqrt{m})$, where $a, b \in \mathbf{Z}$ and have the same parity (see the proof of Theorem 11.6). Since the norm of x is $\frac{1}{4}(a^2 - mb^2)$, x is a unit if and only if $a^2 - mb^2 = \pm 4$, with a and b both odd or even. We seek the smallest such element whose value is greater than 1. Here is a simple way to find it: Compute mb^2 for $b = 1, 2, 3 \ldots$ until either $mb^2 + 4$ or $mb^2 - 4$ is a square a^2, where $a > 0$. Then set $u = \frac{1}{2}(a + b\sqrt{m})$. u is the fundamental unit. (As m is odd, the elements a and b found will have the same parity; this may be seen by considering the norm of u.)

Example Let $m = 17$. Then $17 \cdot 1^2 \pm 4$ is not a square. However, $17 \cdot 2^2 = 68$ and $68 - 4 = 64 = 8^2$, hence the fundamental unit is $u = \frac{1}{2}(8 + 2\sqrt{17}) = 4 + \sqrt{17}$.

Exercise 14.1 *Calculate the fundamental unit of* $\mathbf{Q}(\sqrt{m})$ *for* $m = 7$, $m = 11$ *and* $m = 21$.

Exercise 14.2 *Let* $m \equiv 2, 3 \pmod 4$, $K = \mathbf{Q}(\sqrt{m})$ *and* $u = a + b\sqrt{m}$ *be an element of* U_K. *Show that* $\pm a \pm b\sqrt{m}$ *all belong to* U_K. *Establish a similar result for* $m \equiv 1 \pmod 4$ *and* $u = \frac{1}{2}(a + b\sqrt{m})$ *an element of* U_K

Remark We have seen here that all the embeddings of the number field K into $\mathbf{C}$ may be real. In this case we say that K is *totally real.* Then the units in O_K are the roots of unity and so U_K is finite. On the other hand, it may be so that no embedding is real. In this case we say that K is *totally imaginary.*

Exercise 14.3 *Show that a number field* K *which is a normal extension of* $\mathbf{Q}$ *is either real or imaginary.*

14.5 Hermite's theorem

In this section we will see another application of Minkowski's theorem (Theorem G.4). We will show that for any given positive integer there is only a finite number of number fields whose ring of integers has a discriminant equal to the positive integer in question. We will begin with a preliminary result.

Proposition 14.6 *Let* K *be a number field of degree* n *and* r *(resp.* $2s$*) the number of real (resp. complex) embeddings of* K *into* $\mathbf{C}$. *If* I *is a nonzero ideal in* O_K *and* $c_1, \ldots, c_{r+s}$ *positive constants such that*

$$\prod_{i=1}^{r+s} c_i > (\frac{2}{\pi})^s |disc(O_K)|^{\frac{1}{2}} \|I\|,$$

then there exists α nonzero in I, with $|\sigma_i(\alpha)| < c_i$ for $1 \leq i \leq r$, and $|\sigma_{r+j}(\alpha)|^2 < c_{r+j}$, for $1 \leq j \leq s$.

PROOF Consider the region

$$X(c) = \{x = (y, z) \in \mathbf{R}^n \simeq \mathbf{R}^r \times \mathbf{C}^s : |y_i| < c_i, 1 \leq i \leq r; |z_j|^2 < c_{r+j}, 1 \leq j \leq s\}.$$

It is clear that $X(c)$ is convex and centrally symmetric. Also

$$\begin{aligned} \mu(X(c)) &= 2^r \pi^s \prod_{i=1}^{r+s} c_i > 2^r \pi^s (\frac{2}{\pi})^s |\text{disc}(O_K)|^{\frac{1}{2}} \|I\| \\ &= 2^n 2^{-s} |\text{disc}(O_K)|^{\frac{1}{2}} \|I\|, \end{aligned}$$

where μ denotes Lebesgue measure on $\mathbf{R}^n$. In Section 14.1 we saw that

$$\det \Lambda_I = 2^{-s} |\text{disc}(O_K)|^{\frac{1}{2}} \|I\| \Longrightarrow \mu(X(c)) > 2^n \det \Lambda_I.$$

From Minkowski's theorem there exists an $\alpha \in I$ such that $\phi(\alpha) \neq 0$ and $\phi(\alpha) \in \Lambda_I \cap X(c)$. Thus we have $\alpha \neq 0$ and $|\sigma_i(\alpha)| < c_i$ for $1 \leq i \leq r$, and $|\sigma_{r+j}(\alpha)|^2 < c_{r+j}$, for $1 \leq j \leq s$, as required.□

We are now in a position to establish Hermite's theorem.

Theorem 14.7 *For a fixed positive integer d there exist only finitely many number rings O_K such that $disc(O_K) = d$.*

PROOF If K is a number field and $[K : \mathbf{Q}] = n$, then there is an ideal I in O_K such that

$$\|I\| \leq \frac{n!}{n^n} (\frac{4}{\pi})^s |\text{disc}(O_K)|^{\frac{1}{2}} \Longrightarrow \frac{n^n}{n!} (\frac{\pi}{4})^s \leq |\text{disc}(O_K)|^{\frac{1}{2}};$$

because $\|I\| \geq 1$. Hence the degree of the extension is bounded and so it is sufficient to prove that there is only a finite number of number rings with a given discriminant when the degree of the corresponding number field has a certain value. We consider two cases : (1) K has a real embedding in $\mathbf{C}$, (2) all embeddings of K in $\mathbf{C}$ are complex.

<u>Case 1</u> In this case $r > 0$. We choose real numbers c_i, for $1 \leq i \leq r + s$, such that $c_1 > 1$, $c_i < 1$ for $i > 1$ and

$$\prod_{i=1}^{r+s} c_i > (\frac{2}{\pi})^s |\text{disc}(O_K)|^{\frac{1}{2}}.$$

From Proposition 14.6 there exists a nonzero $\alpha \in O_K$ such that $|\sigma_i(\alpha)| < c_i$, for $1 \leq i \leq r$, and $|\sigma_{r+j}(\alpha)|^2 < c_{r+j}$, for $1 \leq j \leq s$. Since

$$1 \leq |N_{K/\mathbf{Q}}(\alpha)| = |\sigma_1(\alpha)| \prod_{i=2}^{r} |\sigma_i(\alpha)| \prod_{j=1}^{s} |\sigma_{r+j}(\alpha)|^2,$$

we have $|\sigma_1(\alpha)| > 1$ and $|\sigma_i(\alpha)| < 1$, for $\sigma_i \neq \sigma_1$. Hence $\sigma_1(\alpha) \neq \sigma_i(\alpha)$, if $i \neq 1$.

<u>Case 2</u> We define a centrally symmetric convex region X of $\mathbf{C}^s$ as follows:

$$X = \{z \in \mathbf{C}^s : |\Re(z_1)| < \frac{1}{2}, |\Im(z_1)| < c_1, |z_j|^2 < c_j = \frac{1}{2}, 2 \leq j \leq s\},$$

where c_1 is some constant such that $\mu(X) > 2^n 2^{-s}|\mathrm{disc}(O_K)|^{\frac{1}{2}} = 2^n \det \Lambda$. From Minkowski's theorem there exists a nonzero $\alpha \in O_K$ such that $\phi(\alpha) \in X \cap \Lambda$, where ϕ is the usual monomorphism of K into $\mathbf{C}$. Therefore we have $|\Re(\sigma_1(\alpha))| < \frac{1}{2}$, $|\Im(\sigma_1(\alpha))| < c_1$ and $|\sigma_j(\alpha)|^2 < \frac{1}{2}$, for $2 \leq j \leq s$. Now

$$1 \leq |N_{K/\mathbf{Q}}(\alpha)| = |\sigma_1(\alpha)|^2 \prod_{j=2}^{s} |\sigma_j(\alpha)|^2 \Longrightarrow |\sigma_1(\alpha)|^2 > 1.$$

Therefore, if $2 \leq j \leq s$, we have $\sigma_i(\alpha) \neq \sigma_1(\alpha)$. (As $|\sigma_1(\alpha)| > 1$ and $|\Re(\sigma_1(\alpha))| < \frac{1}{2}$, we must have $|\Im(\sigma_1(\alpha))| > \frac{\sqrt{3}}{2}$)

In both cases we have $n = [\mathbf{Q}(\alpha) : \mathbf{Q}]$. If this is not the case, then $[K : \mathbf{Q}(\alpha)] = m \geq 2$ and σ_1 restricted to $\mathbf{Q}(\alpha)$ may be extended to K in m distinct ways (Theorem 3.2), which implies that there exists $\sigma_i \neq \sigma_1$ such that $\sigma_i(\alpha) = \sigma_1(\alpha)$, a contradiction. It follows that $[K : \mathbf{Q}(\alpha)] = 1$, i.e., $K = \mathbf{Q}(\alpha)$. If $f = m(\alpha, \mathbf{Q})$, then $\deg f = n$ and $f \in \mathbf{Z}[X]$.

From Proposition 10.2 we have

$$\mathrm{char}_{\ K/\mathbf{Q}}(\alpha) = \prod_{i=1}^{n} (-\sigma_i(\alpha) + X) \in \mathbf{Z}[X],$$

because char $_{K/\mathbf{Q}}(\alpha)$ is a power of f, by Corollary 10.1. Also, as the c_i are bounded, so are the coefficients of char $_{K/\mathbf{Q}}(\alpha)$ and it results that the coefficients of f are all bounded. We now observe that there can only be a finite number of polynomials in $\mathbf{Z}[X]$ with all the coefficients bounded. Let us write $\mathcal{P}(c)$ for the set of such polynomials obtained here. If K is a number field whose ring of integers O_K has discriminant d and $[K : \mathbf{Q}] = n$, then, from what we have seen, there exists α with minimal polynomial f in $\mathcal{P}(c)$ such that $K = \mathbf{Q}(\alpha)$. As a polynomial has a finite number of roots, there can only be a finite number of number fields with $K = \mathbf{Q}(\alpha)$ and α a root of a polynomial in $\mathcal{P}(c)$. This finishes the proof. □

Chapter 15

Differents

In this chapter we introduce the different, which, as the norm, trace and discriminant, plays an important role in algebraic number theory. We will define the different and then consider its properties. As the definition requires quite a lot of preliminary work, we will consecrate a section to it.

15.1 Definition of the different

Let C be a Dedekind domain and K its field of fractions. Suppose that L is an n-dimensional separable extension of K and D the integral closure of C in L. From Theorem 12.15, D is also a Dedekind domain and, from Proposition 11.2, L is the field of fractions of D. We consider the bilinear form B defined on $L \times L$ by $(x, y) \longmapsto T_{L/K}(xy)$. This is nondegenerate, because L is a separable extension of K (see Corollary 10.4). From Lemma 12.8, we know that if $\mathcal{B} = \{x_1, \ldots, x_n\}$ is a basis of L over K, then $\mathcal{B}$ has a dual basis $\mathcal{B}^* = \{x_1^*, \ldots, x_n^*\}$, i.e., $B(x_i, x_j^*) = \delta_{ij}$, where δ_{ij} is the Kronecker symbol.

Proposition 15.1 *Let L be a separable n-dimensional extension of K and B the nondegenerate bilinear form on $L \times L$ defined above. We suppose that $\{x_1, \ldots, x_n\}$ is a basis of L over K and $\{x_1^*, \ldots, x_n^*\}$ its dual basis. Then*

$$disc_{L/K}(x_1, \ldots, x_n) \cdot disc_{L/K}(x_1^*, \ldots, x_n^*) = 1.$$

PROOF Let $\sigma_1, \ldots, \sigma_n$ be the K-monomorphisms of L into an algebraic closure $\mathcal{C}$ of K. We set $X = (\sigma_i(x_j))$ and $X^* = \big(\sigma_i(x_j^*)\big)$. Then

$$X^{*t}x = \big(T_{L/K}(x_i^* x_j)\big)\,,$$

therefore

$$\det X^* \det X = \det I_n = 1.$$

However,

$$\mathrm{disc}_{L/K}(x_1, \ldots, x_n) = (\det X)^2 \qquad \text{and} \qquad \mathrm{disc}_{L/K}(x_1^*, \ldots, x_n^*) = (\det X^*)^2,$$

therefore

$$\mathrm{disc}_{L/K}(x_1, \ldots, x_n) \cdot \mathrm{disc}_{L/K}(x_1^*, \ldots, x_n^*) = 1,$$

as required. $\square$

For a subset M of L, we define

$$M^* = \{x \in L : T_{L/K}(xy) \in C,\ \forall y \in M\}.$$

M^* is called the *complementary subset* of M. In the next proposition we consider some elementary properties of complementary subsets.

Proposition 15.2 *We have*

- **a.** *M^* is a C-module. If $DM \subset M$, then M^* is a D-module.*
- **b.** *$M_1 \subset M_2 \Longrightarrow M_2^* \subset M_1^*$.*
- **c.** *$D \subset D^*$ and $T_{L/K}(D^*) \subset C$.*
- **d.** *If M is a free C-module with basis $\mathcal{B} = \{x_1, \ldots, x_n\}$, then M^* is a free C-module with basis $\{x_1^*, \ldots, x_n^*\}$ and $M^{**} = M$.*

(The basis $\mathcal{B}$ is also a basis of the vector space L over K, so has a dual basis $\mathcal{B}^* = \{x_1^*, \ldots, x_n^*\}$ in L.)

PROOF **a.** Let $x_1, x_2 \in M^*$ and $y \in M$. Then

$$T_{L/K}\left((x_1 + x_2)y\right) = T_{L/K}(x_1 y) + T_{L/K}(x_2 y) \in C,$$

so $x_1 + x_2 \in M^*$. If $a \in C$, $x \in M^*$ and $y \in M$, then

$$T_{L/K}\left((ax)y\right) = aT_{L/K}(xy) \in C,$$

so $ax \in M^*$. We have shown that M^* is C-module.

Suppose now that $DM \subset M$. If $b \in D$, $x \in M^*$ and $y \in M$, then

$$T_{L/K}\left((bx)y\right) = T_{L/K}\left(x(by)\right) \in C,$$

because $by \in M$. Hence $bx \in M^*$ and it follows that M^* is a D-module.

b. The proof of this part is elementary.

c. Let $x \in D$. As x is integral over the integrally closed domain C, from Proposition 11.1 the minimal polynomial $m(x, K)$ has coefficients in C. However, the characteristic polynomial $\text{char}_{\,L/K}(x)$ is a positive power of $m(x, K)$ (Proposition 10.1), therefore the coefficients of $\text{char}_{\,L/K}(x)$ belong to C, in particular $T_{L/K}(x) \in C$. Thus $T_{L/K}(D) \subset C$. If $x, y \in D$, then $xy \in D$ and so $T_{L/K}(xy) \in C$, which implies that $x \in D^*$ and it follows that $D \subset D^*$.

By definition, if $x \in D^*$, then $T_{L/K}(xy) \in C$, for all $y \in D$. As $1 \in D$, $T_{L/K}(x) \in C$ and so $T_{L/K}(D^*) \subset C$.

d. We know that $\mathcal{B}^*$ is a basis of L over K. To show that $\mathcal{B}^*$ is a basis of M^*, we first need to establish the inclusion of $\mathcal{B}^*$ in M^*. If $x_i^* \in \mathcal{B}^*$, then, for $x_j \in \mathcal{B}$, we have

$$T_{L/K}(x_i^* x_j) = \delta_{ij} \in C \Longrightarrow T_{L/K}(x_i^* y) \in C,\ \forall y \in M,$$

because $\{x_1, \ldots, x_n\}$ is a C-basis of M. Thus $x_i^* \in M^*$, for all i.

As $\mathcal{B}^*$ is independant over K, this is also the case over C, which is a subset of K. To show that $\mathcal{B}^*$ is a basis of M^*, we need to show that it is a generating set. As $\mathcal{B}^*$ is a basis of L over K, for $x \in M^*$, we have $x = \sum_{i=1}^n a_i x_i^*$, with $a_i \in K$. It is sufficient to show that the $a_i \in C$. We have

$$a_j = T_{L/K}\left(\left(\sum_{i=1}^n a_i x_i^*\right) x_j\right) \in C \;\; \forall j \Longrightarrow a_j \in C,$$

Thus $\mathcal{B}^*$ is a generating set of M^*.

We now turn to the second part of **d.** M^* is composed of those elements $x \in L$ which can be written in the form $x = \sum_{i=1}^n a_i x_i^*$, with $a_i \in C$, for all i. Replacing M by M^*, we see that M^{**} is composed of those elements $x \in L$ which can be written in the form $x = \sum_{i=1}^n a_i x_i^{**}$, with $a_i \in C$, for all i. As $x_i^{**} = x_i$, for all i, we have

$$M^{**} = M,$$

as claimed. □

We now concentrate our attention on D^*. For the next proposition we will need two standard results on Noetherian rings. Proofs may be found, for example, in [1].

Lemma 15.1

- **a.** *If M is a finitely generated module over a noetherian ring R, then M is noetherian.*
- **b.** *A submodule of a noetherian module is finitely generated.*

Proposition 15.3 *D^* is a fractional ideal of D.*

PROOF As $DD \subset D$, from Proposition 15.2 **a.**, D^* is a D-module (contained in the field of fractions of D). It is sufficient to show that D^* is a finitely generated D-module. (If this is the case, then the product of the denominators of the elements of a generating set provides a denominator of D^*.)

Since the extension L/K is finite and separable, from the primitive element theorem there exists $\alpha \in L$ such that $L = K(\alpha)$. As α is algebraic over K, the fraction field of C, there exists $c \in C \setminus \{0\}$ such that $d = c\alpha$ is is integral over C; then d belongs to D, the integral closure of C in L. Moreover, the set $\mathcal{D} = \{1, d, \ldots, d^{n-1}\}$ is a basis of L over K, since $[L : K] = n$ and $L = K(d)$ ensure that the the degree of the minimal polynomial $m(d, K)$ is n. The free module C-module generated by $\mathcal{D}$ is the module $C[d]$.

As $C[d] \subset D$, we have $D^* \subset C[d]^*$, using Proposition 15.2 **b.** Also, C is a Dedekind domain, hence a noetherian domain, and $C[d]^*$ is finitely generated over C, so $C[d]^*$ is a noetherian C-module (Lemma 15.1 **a.**). Since D^* is a submodule of the C-module $C[d]^*$, D^* is finitely generated over C (Lemma 15.1 **b.**). Given that $C \subset D$, this is also the case over D. □

We are now in a position to define the different. We notice that D^* is nonzero, because $D \subset D^*$, so it has an inverse in the set of fractional ideals of D. The fractional ideal $(D^*)^{-1}$ is called the *different* of D over C and is denoted $\Delta(D|C)$. In the next section, we will see that the different is in fact an integral ideal of D.

Remark Suppose that K and L are number fields, where L is a finite extension of K. If we set $C = O_K$ and $D = O_L$, then C and D are Dedekind domains and D is the integral closure of C in L. In this case we often write $\Delta_{L/K}$ for $\Delta(D|C)$. If $K = \mathbf{Q}$, then, instead of writing $\Delta_{L/\mathbf{Q}}$, we often use the shorter form Δ_L. Δ_L is called the *absolute different of L*.

15.2 Basic properties of the different

As we said at the end of the preceding section, the different is an integral ideal of D. We will now prove this.

Proposition 15.4 *The different of D over C is an integral ideal of D.*

PROOF As $D \subset D^*$, we have $(D^*)^{-1} \subset D^{-1} = D$, so $(D^*)^{-1}$ is an integral ideal of D. □

We may generalize the product of two ideals in the following way. If $R \subset S$ are commutative rings and I (resp. J) is an ideal in R (resp. S), then we may define the product JI to be the collection of all sums of the form $\sum_{i=1}^n x_i y_i$, where $x_i \in I$ and $y_i \in J$. Then clearly JI is an ideal in S. In the case where R and S are integral domains, we may generalize the product of fractional ideals in a similar manner.

We recall that C is a Dedekind domain with field of fractions K, L a finite separable extension of K and D the integral closure of C in L. In addition, let M be finite separable extension of L and E the integral closure of D in M. Then M is also a finite separable extension of K and E the integral closure of C in M. The differents $\Delta(D|C)$, $\Delta(E|C)$ and $\Delta(E|D)$ are all defined and related in the following way:

$$\Delta(E|C) = \Delta(E|D)\Delta(D|C).$$

We say that the different is transitive. To prove this result we need a lemma.

Lemma 15.2 *Let C be a Dedekind domain, with field of fractions K, L a finite separable extension of K and D the integral closure of C in L. Assume that J is a fractional ideal of D. Then $T_{L/K}(J) \subset C$ if and only if $J \subset D^*$.*

PROOF Suppose that $T_{L/K}(J) \subset C$. As J is a D-module, we have $J = DJ$. If $x \in J$ and $d \in D$, then $T_{L/K}(xd) = T_{L/K}(y)$, with $y \in J$. Thus $T_{L/K}(xd) \in C$ and it follows that $J \subset D^*$.

We now consider the converse. Suppose that $J \subset D^*$. If $x \in J$ and $d \in D$, then $T_{L/K}(xd) \in C$. Setting $d = 1$, we obtain $T_{L/K}(x) \in C$ and it follows that $T_{L/K}(J) \subset C$. □

We may now establish the transitivity of the different referred to above.

Theorem 15.1 *We have*

$$\Delta(E|C) = \Delta(E|D)\Delta(D|C).$$

PROOF To simplify matters, we will proceed in steps. However, first of all we recall that

$$\Delta(E|D)^{-1} = \{x \in M : T_{M/L}(xy) \in D, \forall y \in E\}$$

and

$$\Delta(E|C)^{-1} = \{x \in M : T_{M/K}(xy) \in C, \forall y \in E\}.$$

Also, we will write D^* for $\Delta(D|C)^{-1}$.

Step 1 If J_E is a fractional ideal of E contained in $\Delta(E|D)^{-1}$, then

$$T_{M/K}\left(J_E D^*\right) \subset T_{L/K}\left(D^*\right).$$

Indeed, if $d \in D$, $d^* \in D^*$ and $j_E \in J_E$, then

$$T_{L/K}\left(T_{M/L}(j_E d^*)d\right) = T_{L/K}\left(dd^*(T_{M/L}(j_E))\right),$$

because $d^* \in L$. Moreover, $j_E \in \Delta(E|D)^{-1}$ implies that $T_{M/L}(j_E) \in D$. Consequently, $T_{L/K}\left(T_{M/L}(j_E d^*)d\right) \subset C$, since $d^* \in D^*$. This means that

$$T_{M/L}(J_E D^*) \subset D^* \Longrightarrow T_{L/K} \circ T_{M/L}(J_E D^*) \subset T_{L/K}(D^*)$$

and transitivity of the trace ensures that the statement of **Step 1** holds.

Step 2 $J_E \subset \Delta(E/C)^{-1}D^*$.

From Proposition 15.2 **c.** and the first step, we have

$$C \supset T_{L/K}(D^*) \supset T_{M/K}(J_E D^*).$$

Now, using Lemma 15.2, with $L = M$, $D = E$ and $J = J_E D^*$, we obtain

$$J_E D^* \subset \Delta(E|C)^{-1} \Longrightarrow J_E \subset \Delta(E|C)^{-1}\Delta(D|C),$$

because $D^* = \Delta(D/C)^{-1}$.

Step 3 $\Delta(E|C) = \Delta(E|D)\Delta(D|C)$.

Setting $J_E = \Delta(E|D)^{-1}$, we obtain

$$\Delta(E|D)^{-1} \subset \Delta(E|C)^{-1}\Delta(D|C).$$

Since $C \subset D$, we have $\Delta(E|C)^{-1} \subset \Delta(E|D)^{-1}$ and so

$$\Delta(E|D)^{-1} \subset \Delta(E|C)^{-1}\Delta(D|C) \subset \Delta(E|D)^{-1}\Delta(D|C) \subset \Delta(E|D)^{-1},$$

because $\Delta(E|D)^{-1}$ is an E-module and $\Delta(D|C) \subset D$. Therefore

$$\Delta(E|D)^{-1} = \Delta(E|C)^{-1}\Delta(D|C) \Longrightarrow \Delta(E|C) = \Delta(E|D)\Delta(D|C).$$

This ends the proof. □

If we multiply $\Delta(D|C)$ on the left by E, we obtain an ideal of E and an analogous expression to that of Theorem 15.1, but involving a multiplication of ideals in E.

Corollary 15.1 *We have*

$$\Delta(E|C) = \Delta(E|D)\left(E\Delta(D|C)\right).$$

PROOF It is sufficient to show that

$$\Delta(E|D)\left(E\Delta(D|C)\right) = \Delta(E|D)\Delta(D|C).$$

As $\Delta(D|C) \subset E\Delta(D|C)$, we have

$$\Delta(E|D)\Delta(D|C) \subset \Delta(E|D)\left(E\Delta(D|C)\right).$$

Now let $x \in \Delta(E|D)$ and $y \in E\Delta(D|C)$. Then $y = \sum_{i=1}^n a_i b_i$, with $a_i \in E$ and $b_i \in \Delta(D|C)$, so

$$xy = x\sum_{i=1}^n a_i b_i = \sum_{i=1}^n (a_i x) b_i \in \Delta(E|D)\Delta(D\mathbf{C})),$$

because $\Delta(E|D)$ is an ideal in E. It follows that

$$\Delta(E|D)\left(E\Delta(D|C)\right) \subset \Delta(E|D)\Delta(D|C),$$

and hence the required equality. □

15.3 Rings of fractions

We now consider rings of fractions. Let C be a Dedekind domain, with field of fractions K, and L a finite separable extension of K. We suppose that D is the integral closure of C in L and U a multiplicative subset of C. As $C \subset D$, U is also a multiplicative subset of D. We recall that $D' = U^{-1}D$ is the integral closure of $C' = U^{-1}C$ in L. (Proposition 12.20).

If P is a prime ideal of C and $U = C \setminus P$, then we write $\Delta_P(L|K)$ for $\Delta(D'|C')$. The different $\Delta_P(L|K)$ is called the different of $L|K$ over P.

We now consider the special case of number fields. We wish to find a relation between $\Delta_{L/K}$ and $\Delta(D'|C')$.

Theorem 15.2 *Let $K \subset L$ be number fields, where L is a finite extension of K and $C = O_K$, $D = O_L$ the corresponding number rings. If U is a multiplicative subset of C and $C' = U^{-1}C$, $D' = U^{-1}D$, then*

$$D'\Delta_{L/K} = \Delta(D'|C').$$

PROOF If $x \in D'\Delta_{L/K}$, then x is a finite sum of products of the form ab, with $a \in D'$ and $b \in \Delta_{L/K}$. However, $a = \frac{d}{u}$, with $d \in D$ and $u \in U$. As $\Delta_{L/K}$ is an ideal in D, $db \in \Delta_{L/K}$, so $x = \frac{y}{u}$, with $y \in \Delta_{L/K}$ and $u \in U$.

Let $z \in D'^*$; then $T_{L/K}(zD') \subset C'$. As D is a finitely generated $\mathbf{Z}$-module, D is a finitely generated C-module. Let $\{t_1, \ldots, t_m\}$ be a generating set of D. Then $T_{L/K}(zt_i) = \frac{c_i}{u_i}$, with $c_i \in C$ and $u_i \in U$. We set $u_0 = u_1 \cdots u_m \in U$. Then

$$T_{L/K}(zu_0t_i) = u_0 T_{L/K}(zt_i) \in C,$$

for $i = 1, \ldots, m$. Hence

$$T_{L/K}(zu_0D) \subset C \Longrightarrow zu_0 \in D^*.$$

Now, $\Delta(D|C) = D^{*-1}$ and $y \in \Delta(D|C)$, so, by Proposition 12.8, $yzu_0 \in D$. From this we deduce that

$$xz = \frac{yzu_0}{uu_0} \in D'.$$

Thus, for every $z \in D'^*$, $xz \in D'$. Using Proposition 12.8 again, we obtain that x belongs to the inverse of D'^*, i.e., $x \in \Delta(D'|C')$. We have shown that $D'\Delta_{L/K} \subset \Delta(D'|C')$.

We now consider the reverse inclusion. Let $x \in \Delta(D'|C')$. First we recall that D^* is a fractional ideal of D (Proposition 15.3), hence D^* is a finitely generated D-module (Proposition 12.7). Let $\{z_1, \ldots, z_n\}$ be a generating set of the D-module D^*. Then $T_{L/K}(z_iD) \subset C$. If $\frac{y}{u} \in D'$, then

$$T_{L/K}(z_i\frac{y}{u}) = \frac{1}{u}T_{L/K}(z_iy) \in C' \Longrightarrow T_{L/K}(z_iD') \subset C',$$

which implies that $z_i \in D'^*$. Using Proposition 12.8, we obtain $xz_i \in C' \subset D' = U^{-1}D$ and so we may write $xz_i = \frac{d_i}{u_i}$, with $d_i \in D$ and $u_i \in U$. Let $u_0 = u_1 \cdots u_n \in U$. Then $u_0xz_i \in D$, for $i = 1, \cdots, n$, hence $u_0xD^* \subset D$, thus

$$ux\Delta(D|C)^{-1} \subset D \Longrightarrow ux \in D\Delta(D|C) = \Delta(D|C)$$

and so

$$x \in U^{-1}\Delta(D|C) \subset D'\Delta(D|C).$$

Therefore

$$\Delta(D'|C') \subset D'\Delta(D|C).$$

This ends the proof. □

15.4 Preliminary work for Dedekind's different theorem

Let $K \subset L$ be number fields with respective associated number rings C and D. The different $\Delta_{L/K}$ is an ideal in D such that $\Delta_{L/K} \neq \{0\}$. If $\Delta_{L/K} \neq D$, then there exist nonzero prime ideals $Q_1, \ldots, Q_r$ in D and positive integers $n_1, \ldots, n_r$ such that

$$\Delta_{L/K} = Q_1^{n_1} \cdots Q_r^{n_r}.$$

If Q belongs to the set of prime ideals in this decomposition and $Q = Q_i$, then we set $s_Q = s_Q(L/K) = n_i$. For any other prime ideal Q in D, we set $s_Q = 0$. In particular, if $\Delta_{L/K} = D$, then $s_Q = 0$, for all nonzero prime ideals in D. s_Q is called the *exponent at Q of the different* $\Delta_{L/K}$.

If Q is a nonzero prime ideal in D, then $P = C \cap Q$ is a nonzero prime ideal in C (Theorem 13.1). From Proposition 13.1 we have $Q|DP$. If

$$DP = Q_1^{e_1} \cdots Q_t^{e_t},$$

then $Q = Q_i$, for some Q_i in the decomposition of DP. We call e_i the *ramification index* of Q and note it e_Q. (In fact, $e_Q = e(Q|P)$, where $P = C \cap Q$.) Q is said to be ramified if $e_Q \geq 2$. There is an important relation between s_Q and e_Q:

Result For every nonzero prime ideal Q in D, we have $s_Q \geq e_Q - 1$. In addition, $s_Q = e_Q - 1$ if and only if the characteristic of the field D/Q does not divide e_Q.

The proof of this result is rather long and requires some preliminary work. This we will do in this section and in the next we will concentrate our attention on the proof of the result.

Lemma 15.3 *Let $\psi : S \longrightarrow \bar{S}$ be a surjective ring homomorphism. We suppose that R is a subring of S such that S is a free R-module with basis $\mathcal{B} = \{x_1, \ldots, x_n\}$. We note $\bar{R}$ the image of R and $\bar{\mathcal{B}} = \{\bar{x}_1, \ldots, \bar{x}_n\}$ the image of $\mathcal{B}$ and we suppose that $\bar{S}$ is a free $\bar{R}$-module with basis $\bar{\mathcal{B}}$. If $x \in S$, then*

$$\psi\left(N_{S/R}(x)\right) = N_{\bar{S}/\bar{R}}(\bar{x}) \tag{15.1}$$

$$\psi\left(T_{S/R}(x)\right) = T_{\bar{S}/\bar{R}}(\bar{x}) \tag{15.2}$$

$$\psi^*\left(char_{\ S/R}(x)\right) = char_{\ \bar{S}/\bar{R}}(\bar{x}), \tag{15.3}$$

where ψ^* is the mapping from $S[X]$ into $\bar{S}[X]$ which applies ψ to each coefficient of a polynomial of $S[x]$.

PROOF We note θ_x the mapping from S into itself defined by multiplication by x and $M(\theta_x)$ the matrix of θ_x in the basis $\mathcal{B}$. In the same way we note $\theta_{\bar{x}}$ the mapping from $\bar{S}$ into itself defined by multiplication by $\bar{x}$ and $M(\theta_{\bar{x}})$ the matrix of $\theta_{\bar{x}}$ in the basis $\bar{\mathcal{B}}$. If

$$xx_j = \sum_{i=1}^{n} r_{ij} x_i \qquad j = 1, \ldots, n,$$

then

$$\bar{x}\bar{x}_j = \sum_{i=1}^{n} \bar{r}_{ij} \bar{x}_i \qquad j = 1, \ldots, n.$$

Therefore,

$$M(\theta_x) = (r_{ij}) \qquad \text{and} \qquad M(\theta_{\bar{x}}) = (\bar{r}_{ij}).$$

If we apply ψ to the coefficients of the characteristic polynomial char $_{S/R}(x) = \det(XI - M(\theta_x))$, then we obtain $\det(XI - M(\theta_{\bar{x}})) =$ char $_{\bar{S}/\bar{R}}(\bar{x})$, i.e., the third relation. The other two relations follow easily. □

The next preliminary results are more difficult. Let R be a ring and K a subfield of R. Then R is a K-vector space. We suppose that $\dim_K R = n < \infty$. In addition, let $\theta : R \longrightarrow R$ be a K-linear endomorphism and we suppose the existence of K-subspaces R_i of R forming a decreasing sequence

$$R = R_0 \supset R_1 \supset \cdots \supset R_{k-1} \supset R_k = \{0\}$$

such that $\theta(R_i) \subset R_i$, for $i = 1, \ldots, k$. Then θ induces a K-linear endomorphism θ_i on R_{i-1}/R_i defined by

$$\theta_i(x + R_i) = \theta(x) + R_i.$$

(If $x' \in R_i$, then

$$\theta(x + x') + R_i = \theta(x) + \theta(x') + R_i = \theta(x) + R_i,$$

because $\theta(x') \in R_i$, so θ_i is well-defined.)

Lemma 15.4 *For each index $i = 1, \ldots, k$, let $\mathcal{B}_i = \{x_{i1}, \ldots, x_{im_i}\}$ be a set of elements of R_{i-1} such that $\{x_{i1} + R_i, \ldots, x_{im_i} + R_i\}$ is a basis of R_{i-1}/R_i. Then, for $i = 1, \ldots, k$, the set*

$$\tilde{\mathcal{B}}_i = \mathcal{B}_i \cup \cdots \cup \mathcal{B}_k$$

is a basis of R_{i-1}. In particular,

$$\mathcal{B} = \tilde{\mathcal{B}}_1 = \mathcal{B}_1 \cup \cdots \cup \mathcal{B}_k$$

is a basis of R.

PROOF If $x \in R_{i-1}$, then there exist $\lambda_{i1}, \ldots, \lambda_{im_i} \in K$ and $y \in R_i$ such that

$$x = \lambda_{i1}x_{i1} + \cdots + \lambda_{im_i}x_{im_i} + y.$$

As $y \in R_i$, there exist $\lambda_{i+1,1}, \ldots, \lambda_{i+1,m_{i+1}} \in K$ and $z \in R_{i+1}$ such that

$$y = \lambda_{i+1,1}x_{i+1,1} + \cdots + \lambda_{i+1,m_{i+1}}x_{i+1,m_{i+1}} + z.$$

Continuing in the same way, we see that $\tilde{\mathcal{B}}_i$ is a generating set of R_{i-1}, since $R_k = \{0\}$.

Suppose that

$$\lambda_{i1}x_{i1}+\cdots+\lambda_{im_i}x_{im_i}+\lambda_{i+1,1}x_{i+1,1}+\cdots+\lambda_{i+1,m_{i+1}}x_{i+1,m_{i+1}}+\cdots+\lambda_{k1}x_{k1}+\cdots+\lambda_{km_k}x_{km_k} = 0.$$

Then

$$\lambda_{i+1,1}x_{i+1,1} + \cdots + \lambda_{km_k}x_{km_k} \in R_i \Longrightarrow \lambda_{i1}x_{i1} + \cdots + \lambda_{im_i}x_{im_i} \in R_i.$$

As $\{x_{i1} + R_i, \ldots, x_{im_i} + R_i\}$ is a basis of R_{i-1}, we have $\lambda_{i1} = \cdots = \lambda_{im_i} = 0$ and it follows that $\lambda_{i+1,1}x_{i+1,1} + \cdots + \lambda_{km_k}x_{km_k} = 0$. We now repeat the preceding argument to show that $\lambda_{i+1,1} = \cdots = \lambda_{i+1,m_{i+1}} = 0$. Continuing in the same way we find that all the coefficients λ_{ij} have the value 0. Hence $\tilde{\mathcal{B}}_i$ is an independant set and so a basis of R_{i-1}. □

The basis $\mathcal{B}$ enables us to find a factorization of the characteristic polynomial of the K-linear homomorphism θ defined above.

Proposition 15.5 *We have*

$$char_{\,R/K}(\theta) = \prod_{i=1}^{k} char_{\,(R_{i-1}/R_i)/K}(\theta_i).$$

PROOF We consider θ with respect to the basis $\mathcal{B}$. As $\theta(x_{ij}) \in R_{i-1}$, we may express it in terms of the basis $\mathcal{B}_i$:

$$\theta(x_{ij}) = \sum_{l=1}^{m_i} \lambda_{ijl} x_{il} + \sum_{l=1}^{m_{i+1}} \lambda_{i+1,jl} x_{i+1,l} + \cdots + \sum_{l=1}^{m_k} \lambda_{kjl} x_{kl},$$

where the coefficients λ_{abc} belong to K. Then

$$\theta_i(\bar{x}_{ij}) = \sum_{l=1}^{m_i} \lambda_{ijl} \bar{x}_{il}$$

and so

$$M(\theta) = \begin{pmatrix} M(\theta_1) & 0 & \dots & 0 \\ M_{21} & M(\theta_2) & \dots & 0 \\ \vdots & \vdots & \ddots & \\ M_{k1} & M_{k2} & \dots & M(\theta_k) \end{pmatrix},$$

where $M(\theta)$ is the matrix of θ in the basis $\mathcal{B}$ and, for $i = 1, \dots, k$, $M(\theta_i)$ is the matrix of θ_i in the basis $\bar{\mathcal{B}}_i = \{\bar{x}_{i1}, \dots, \bar{x}_{im_i}\}$ of R_{i-1}/R_i; the other blocks M_{ij} are matrices with entries in K. It now follows easily that

$$\mathrm{char}_{\,R/K}(\theta) = \prod_{i=1}^{k} \mathrm{char}_{\,(R_{i-1}/R_i)/K}(\theta_i).$$

This ends the proof. □

Suppose now that we remain in the same context and add the following conditions (C):

- **a.** Each R_i is an ideal in R;
- **b.** For each $i = 1, \dots, k$, there is no ideal I in R such that $R_{i-1} \supsetneqq I \supsetneqq R_i$;
- **c.** If $y \in R_1$ and $z \in R_{i-1}$, then $yz \in R_i$.

Lemma 15.5 *Under the conditions (C), if $y, z \in R$ with $yz \in R_i$ and $y \notin R_i$, then $z \in R_1$.*

PROOF From **a.** and **b.** R_1 is a maximal ideal in R. We claim that R_1 is the unique maximal ideal. Suppose that $t \in R_1$; then $t \in R_{2-1}$, so, from **c.**, $t^2 \in R_2$. Now $t \in R_1$ and $t^2 \in R_{3-1}$, so $t^3 \in R_3$. Continuing in the same way, we find that $t^k \in R_k = \{0\}$, so

$$(1-t)(1+t+\cdots+t^{k-1}) = 1 - t^k = 1,$$

so $1-t$ is invertible. If I is a maximal ideal of R such that I is not included in R_1, then $R = R_1 + I$, because I is a maximal ideal in R, so there exist $t \in R_1$ and $u \in I$ such that $1 = t + u$. However, $u = 1 - t$ is invertible, which is impossible, because I is a proper ideal in R. It follows that any maximal ideal I in R is included in R_1 and so R_1 is the unique maximal ideal of R.

Suppose that $z \in R \setminus R_1$ and z is not invertible. Then z lies in a maximal ideal I. As there is only one such ideal, namely R_1, $z \in R_1$, a contradiction, so z is invertible.

Let $y, z \in R$, with $yz \in R_i$. If $z \notin R_1$, then z is invertible. Since R_i is an ideal, we have $y = z^{-1}yz \in R_i$. □

We are now in a position to establish a key result of this section. We will remain in the same context, with the conditions (C) and suppose that the linear mapping $\theta = \theta_x$ (multiplication by $x \in R$, for some fixed $x \in R$).

Theorem 15.3 *For* $i = 1, \ldots, k$,

$$\mathit{char}_{\,(R_{i-1}/R_i)/K}(\theta_i) = \mathit{char}_{\,(R/R_1)/K}(\theta_1),$$

Hence

$$\mathit{char}_{\,R/K}(x) = \left(\mathit{char}_{\,(R/R_1)/K}(\theta_1)\right)^k.$$

PROOF We claim that, for $i = 1, \ldots, k$, there exists a linear isomorphism $\lambda_i : R_{i-1}/R_i \longrightarrow R/R_1$ such that $\theta_1 \circ \lambda_i = \lambda_i \circ \theta_i$. Let $u \in R_{i-1} \setminus R_i$. Then $R_i \subset R_i + Ru \subset R_{i-1}$. As R_i is an ideal of R (condition (C) **a.**), $R_i + Ru$ is also an ideal of R. In addition, $R_i + Ru = R_{i-1}$ (condition (C) **b.**) If $y + R_i \in R_{i-1}/R_i$, then $y = y_2 + y_1 u$, with $y_2 \in R_i$ and $y_1 \in R$. We set

$$\lambda_i(y + R_i) = y_1 + R_1.$$

Suppose that $y = z_2 + z_1 u$, with $z_2 \in R_i$ and $z_1 \in R$, then

$$0 = (y_2 - z_2) + (y_1 - z_1)u \Longrightarrow (y_1 - z_1)u \in R_i.$$

Given that $u \notin R_i$, from Lemma 15.5 we obtain that $y_1 - z_1 \in R_1$, so $y_1 + R_1 = z_1 + R_1$, i.e., λ_i is well-defined. Clearly λ_i is a surjective R-module homomorphism. Suppose that $\lambda_i(y + R_i) = 0 \in R/R_1$. If $y = y_2 + y_1 u$, then $y_1 \in R_1$ and, from condition (C) **c.**, $y_1 u \in R_i$ and so $y \in R_i$, i.e., $y = 0 \in R_{i-1}/R_i$. It follows that λ_i is injective. We have shown that λ_i is an isomorphism.

It remains to show that $\theta_1 \circ \lambda_i = \lambda_i \circ \theta_i$. Let y be an element of R_{i-1} such that $y = y_2 + y_1 u$, with $y_2 \in R_i$ and $y_1 \in R$. Then $xy = xy_2 + (xy_1)u$, with $xy_2 \in R_i$ and $xy_1 \in R$. We have

$$\theta_1\left(\lambda_i(y + R_i)\right) = \theta_1(y_1 + R_1) = \theta(y_1) + R_1 = xy_1 + R_1,$$

and then

$$xy_1 + R_1 = \lambda_i(xy + R_i) = \lambda_i\left(\theta(y) + R_i\right) = \lambda_i\left(\theta_i(y + R_i)\right).$$

Hence $\theta_1 \circ \lambda_i = \lambda_i \circ \theta_i$, as claimed.

Let $\mathcal{B}_i = \{x_1, \ldots, x_m\}$ be a K-basis of R_{i-1}/R_i and $\mathcal{B}'_i = \{x'_1, \ldots, x'_m\}$, where $x'_k = \lambda_i(x_k)$, for $k = 1, \ldots, m$. Then $\mathcal{B}'_i$ is a K-basis of R/R_1, because λ_i is a linear isomorphism. If $\theta_i(x_j) = \sum_{k=1}^m a^i_{kj} x_k$, then

$$\lambda_i\left(\theta_i(x_j)\right) = \sum_{k=1}^m a^i_{kj} \lambda_i(x_k) = \sum_{k=1}^m a_{ik} x'_k$$

and

$$\theta_1(x'_j) = \theta_1\left(\lambda_i(x_j)\right) = \lambda_i\left(\theta_i(x_j)\right) = \sum_{k=1}^m a^i_{kj} x'_k.$$

Thus the matrix of θ_i with respect to the basis $\mathcal{B}_i$ and the matrix of θ_1 with repect to the basis $\mathcal{B}'_i$ are the same. It follows that

$$\mathrm{char}_{\,(R_{i-1}/R_i)/K}(\theta_i) = \mathrm{char}_{\,(R/R_1)/K}(\theta_1)$$

and, using Proposition 15.5, we obtain

$$\text{char}_{R/K}(\theta) = \left(\text{char}_{(R/R_1)/K}(\theta_1)\right)^k,$$

as required, since $\theta = \theta_x$, the multiplication by x. □

We now turn to Dedekind domains. Let C be a Dedekind domain, with field of fractions K, and L a separable extension of degree n of K. We suppose that D is the integral closure of C in L. (We know from the remark after Theorem 12.15 that D is a Dedekind domain, which is distinct from C, if $n > 1$.) We take a nonzero prime ideal P of C. As DP is an ideal in D and $DP \neq \{0\}, D$, we have a decomposition

$$DP = \prod_{i=1}^{r} Q_i^{e_i},$$

where the Q_i are prime ideals in D and the e_i positive integers. From Theorem 12.16, D/DP is a vector space over the field $C/P = F$ of dimension n. We now define certain canonical mappings:

$$\psi : C \longrightarrow F, \qquad \psi_0 : D \longrightarrow D/DP \qquad \text{and} \qquad \psi_i : D \longrightarrow D/Q_i = L_i,$$

for $i = 1, \ldots, r$. It will be shown during the proof of Theorem 15.4 that L_i is a field extension of F of finite degree. If $i \neq j$, then Q_i and Q_j are coprime and this is also the case for $Q_i^{e_i}$ and $Q_j^{e_j}$. With

$$U = C \setminus P, \qquad C' = U^{-1}C, \qquad D' = U^{-1}D \qquad \text{and} \qquad P' = C'P,$$

we define the following canonical mappings:

$$\tilde{\psi} : C' \longrightarrow C'/P' = F' \qquad \text{and} \qquad \tilde{\psi}_0 : D' \longrightarrow D'/D'P.$$

From Corollary 12.11, there is a ring isomomorphism ϕ from D/DP onto $D'/D'P$, taking $d+DP$ to $\frac{d}{1} + D'P$. The image of F is F'.

From Proposition 12.4, we have

$$\cap_{i=1}^{r} Q_i^{e_i} = \prod_{i=1}^{r} Q_i^{e_i} = DP,$$

so, using Corollary F.1, we obtain

$$D/DP \simeq \prod_{i=1}^{r} D/Q_i^{e_i}.$$

Explicitly the isomorphism is defined by

$$\pi(y + DP) = (y + Q_1^{e_1}, \ldots, y + Q_r^{e_r}).$$

For $i = 1, \ldots, r$, we define

$$\pi_i(y + DP) = y + Q_i^{e_i},$$

i.e., π_i is the projection of D/DP onto $D/Q_i^{e_i}$.

If A and B are rings and $\alpha : A \longrightarrow B$ a ring homomorphism, then we define α^* to be the mapping from $A[X]$ into $B[X]$ which applies α to each coefficient of a polynomial in $A[X]$.

With this preliminary work, we may now state (and prove) the second key result of this section.

Theorem 15.4 *If $x \in D$, then char $_{L/K}(x) \in C[X]$ and*

- **a.** $\psi^*\left(char_{\,L/K}(x)\right) = \prod_{j=1}^{r} char_{\,L_j/F}\left(\psi_j(x)\right)^{e_j}$;
- **b.** $\psi\left(T_{L/K}(x)\right) = \sum_{j=1}^{r} e_j T_{L_j/F}\left(\psi_j(x)\right)$;
- **c.** $\psi\left(N_{L/K}(x)\right) = \prod_{j=1}^{r} N_{L_j/F}\left(\psi_j(x)\right)^{e_j}$.

(It is important to show that char $_{L/K}(x) \in C[X]$, because the mapping ψ is defined on C.)

PROOF The proof of this result is rather long, so we have divided it into parts and paragraphs. Also, to simplify the notation, in general we write x for $\frac{x}{1}$.

Part 1

- As $x \in D$, x is integral over C, therefore the minimal polynomial $m(x, K)$ belongs to $C[X]$ (Proposition 11.1). Given that the characteristic polynomial char $_{L/K}(x)$ is a power of $m(x, K)$ (Proposition 10.1), it belongs to $C[X]$.

- Using the proof of Theorem 12.17, we note certain properties of C' and D', namely C' is a PID, D' is the integral closure of C' in L and D' is a free C'-module of rank n. In addition, $D'/D'P$ is an F'-vector space of rank n: if $\mathcal{B}' = \{x'_1, \dots, x'_n\}$ is a basis of the free C'-module D', then $\bar{\mathcal{B}}' = \{\bar{x}'_1, \dots, \bar{x}'_n\}$ is a basis of the F'-vector space $D'/D'P$, where $\bar{x}'_i$ is the image x'_i under the canonical mapping $\tilde{\psi}_0$ of D' onto $D'/D'P$.

- Now let $V = C' \setminus \{0\}$. The set V is a multiplicative subset of the integral domain C' and $V^{-1}C'$ is the field of fractions of C', which is K. Also, D' is the integral closure of C' in L, so, by Proposition 12.20, $V^{-1}D'$ is the integral closure of $V^{-1}C'$ in L, i.e., the integral closure of K in L. If γ is the canonical monomorphism from D' into $V^{-1}D'$, then from Section 12.8 we have

$$\text{char}_{\,V^{-1}D'/V^{-1}C'}(\gamma(x)) = \gamma^*(\text{char}_{\,D'/C'}(x)).$$

As γ is the canonical inclusion of D' in $V^{-1}D'$, we may identify D' with its image under γ and so we obtain

$$\text{char}_{\,L/K}(x) = \text{char}_{\,V^{-1}D'/V^{-1}C'}(x) = \text{char}_{\,D'/C'}(x).$$

We aim to study char $_{D'/C'}(x)$. At the beginning of the proof we recalled certain properties of C' and D', which permit us to apply Lemma 15.3 with $\tilde{\psi}_0$ in the place of ψ. We obtain

$$\tilde{\psi}_0^*\left(\text{char}_{\,D'/C'}(x)\right) = \text{char}_{\,(D'/D'P)/F'}\left(\tilde{\psi}_0(x)\right),$$

- From Corollary 12.11, there is a ring isomorphism ϕ from D/DP onto $D'/D'P$, taking $d + DP$ to $d + D'P$. The image of F is F'. We now show that

$$\text{char}_{\,(D'/D'P)/F'}\left(\tilde{\psi}_0(x)\right) = \phi^*\left(\text{char}_{\,(D/DP)/F}\left(\psi_0(x)\right)\right).$$

If $\mathcal{B} = \{d_1 + DP, \dots, d_n + DP\}$ is a basis of the F-vector space D/DP, then $\mathcal{B}' = \{d_1 + D'P, \dots, d_n + D'P\}$ is a basis of the F'-vector space $D'/D'P$. Also, if $x \in D$, then $\psi_0(x) = x + DP$ and $\tilde{\psi}_0(x) = x + D'P$. We consider the matrices of $\theta_{\psi_0(x)}$ and $\theta_{\tilde{\psi}_0(x)}$ in the respective bases $\mathcal{B}$ and $\mathcal{B}'$. If

$$\psi_0(x)(d_k + DP) = \sum_{i=1}^{n}(a_{ik} + P)(d_i + DP) = \sum_{i=1}^{n}(a_{ik} + DP)(d_i + DP),$$

then

$$\begin{aligned}
\phi(\psi_0(x))\phi(d_k+DP) &= \sum_{i=1}^{n}\phi(a_{ik}+DP)\phi(d_i+DP)\\
&= \sum_{i=1}^{n}(a_{ik}+D'P)(d_i+D'P)\\
&= \sum_{i=1}^{n}(a_{ik}+C'P)(d_1+D'P).
\end{aligned}$$

However,

$$\phi\left(\psi_0(x)\right)=\psi_0(x)+D'P=\phi\circ\psi(x)=\tilde{\psi}_0(x),$$

hence

$$\tilde{\psi}_0(x)(d_k+D'P)=\sum_{i=1}^{n}(a_{ik}+C'P)(d_i+D'P).$$

If (a_{ik}) is the matrix of $\theta_{\psi_0(x)}$ in the basis $\mathcal{B}$, then the matix of $\theta_{\tilde{\psi}_0(x)}$ in the basis $\mathcal{B}'$ has the form $(\phi(a_{ik}))$. From this we obtain

$$\text{char}_{\,(D'/D'P)/F'}\left(\tilde{\psi}_0(x)\right)=\phi^*\left(\text{char}_{\,(D/DP)/F}\left(\psi_0(x)\right)\right),$$

as required.

- To sum up, we have shown that

$$\tilde{\psi}_0^*\left(\text{char}_{\,D'/C'}(x)\right)=\phi^*\left(\text{char}_{\,(D/DP)/F}\left(\psi_0(x)\right)\right).$$

This finishes the first part of the proof.

<u>Part 2</u>

- Our first step in this part is to show that

$$\text{char}_{\,(D/DP)/F}\left(\psi_0(x)\right)=\text{char}_{\,\prod_{i=1}^{r}(D/Q_i^{e_i})/F}\left(\pi(\psi_0(x))\right).$$

- The ring isomorphism $\pi : D/DP \longrightarrow \prod_{i=1}^{r} D/Q_i^{e_i}$ enables us to define a scalar multiplication on $\prod_{i=1}^{r} D/Q_i^{e_i}$, making it into an F-vector space:

$$(c+P)\cdot\pi(D+DP)=\pi(c+DP)\pi(d+DP)=\pi(c+DP)(d+DP)).$$

Then

$$\pi((c+P)\cdot(D+DP))=\pi(c+DP)(d+DP))=(c+P)\cdot\pi(D+DP),$$

and so π is an F-linear isomorphism.

- With the notation already used, we define $\theta_{\psi_0(x)}$ to be multiplication by $\psi_0(x)$ in D/DP and $\theta_{\pi(\psi_0(x))}$ to be multiplication by $\pi(\psi_0(x))$ in $\prod_{i=1}^{r} D/Q^{e_i}$. We claim that

$$\pi\circ\theta_{\psi_0(x)}\circ\pi^{-1}=\theta_{\pi(\psi_0(x))}. \tag{15.4}$$

Using the fact that π is a ring homomorphism, we have

$$\begin{aligned}
\pi \circ \theta_{\psi_0(x)}(d + DP) &= \pi(\psi_0(x)(d + DP)) \\
&= \pi(\psi_0(x))\pi(d + DP) \\
&= \theta_{\pi(\psi_0(x))} \circ \pi(d + DP),
\end{aligned}$$

hence the claim.

- If $\mathcal{B} = \{x_1, \ldots, x_n\}$ is a basis of D/DP, then $\mathcal{B}' = \{x'_1, \ldots, x'_n\}$ is a basis of $\prod_{i=1}^r D/Q^{e_i}$. For $x'_k \in \mathcal{B}'$ there exist $a_{ik} \in F$, with $i = 1, \ldots, n$, such that

$$\pi(\psi_0(x))x'_k = \sum_{i=1}^n a_{ik}x'_i = \sum_{i=1}^n a_{ik}\pi(x_i) = \pi \sum_{i=1}^n a_{ik}x_i,$$

where we have used the linearity of π. Employing equation (15.4), we obtain

$$\pi(\psi_0(x))x'_k = \theta_{\pi(\psi_0(x))}(x'_k) = \pi \circ \theta_{\psi_0(x)} \circ \pi^{-1}(x'_k) = \pi \circ \theta_{\psi_0(x)}(x_k) = \pi(\psi_0(x)x_k).$$

Therefore

$$\pi(\psi_0(x)x_k) = \pi \sum_{i=1}^n a_{ik}(x_i) \Longrightarrow \psi_0(x)x_k = \sum_{i=1}^n a_{ik}x_i.$$

Thus the matrix of $\theta_{\psi_0(x)}$ in the basis $\mathcal{B}$ is the same as that of $\theta_{\pi(\psi_0(x))}$ in the basis $\mathcal{B}'$. From this we conclude that

$$\text{char}_{\,(D/DP)/F}\,(\psi_0(x)) = \text{char}_{\,\prod_{i=1}^r (D/Q_i^{e_i})/F}\,(\pi(\psi_0(x)))\,,$$

as required.

- We now show that

$$\text{char}_{\,\prod_{i=1}^r (D/Q_i^{e_i})/F}\,(\pi(\psi_0(x))) = \text{char}_{\,\prod_{i=1}^r (D/Q_i^{e_i})/F}\,(\pi(\psi_0(x)))\,.$$

We now use Theorem 15.3. Let

$$R = \prod_{i=1}^r D/Q^{e_i}, R_1 = \prod_{i=2}^r D/Q^{e_i}, R_2 = \prod_{i=3}^r D/Q^{e_i}, \ldots, R_r = \{0\}.$$

Then

$$R \supset R_1 \supset R_2 \supset \cdots \supset R_r = \{0\},$$

and the R_i are F-linear subspaces. Considering the explicit form of the mapping π we deduce that $\theta_{\pi(\psi_0(x))}(R_i) \subset R_i$. In addition, we have $R_{i-1}/R_i \simeq D/Q_i^{e_i}$. The linear endomorphism θ_i induced on R_{i-1}/R_i by $\theta_{\pi(\psi_0(x))}$ is the multiplication by $\pi_i(\psi_0(x))$ in $D/Q_i^{e_i}$. Using Proposition 15.5, we obtain

$$\text{char}_{\,\prod_{i=1}^r (D/Q^{e_i})/F}(\pi(\psi_0(x)) = \prod_{i=1}^r \text{char}_{\,(D/Q_i^{e_i})/F}\,(\pi_i(\psi_0(x)))\,. \tag{15.5}$$

This ends the second part of the proof.

Part 3

- Our aim in this section is to determine the polynomials in the product on the right hand side of equation (15.5), namely, for $i = 1, \dots, r$, to show that

$$\text{char}_{(D/Q_i^{e_i})/F}\,(\pi_i(\psi_0(x))) = \text{char}_{L_i/F}\,(\psi_i(x))\,.$$

We apply Theorem 15.3 for a given j and set $k = e_j$. To apply the theorem, we define

$$R = D/Q_j^k \quad \text{and} \quad R_1 = Q_j/Q_j^k, \dots, R_{k-1} = Q_j^{k-1}/Q_j^k, R_k = Q_j^k/Q_j^k = \{0\}.$$

Then R is a ring. We notice that $P \subset DP \subset Q_j^k$, so the mapping

$$\delta : F \longrightarrow R, c + P \longmapsto c + Q_j^k$$

is a well-defined ring homomorphism. If $\delta(c + P) = 0$, then $c \in C \cap Q_j^k$. However,

$$P \subset C, P \subset Q_j^k \Longrightarrow P \subset C \cap Q_j^k \quad \text{and} \quad C \cap Q_j^k \subset C \cap Q_j = P,$$

so $C \cap Q_j^k = P$ and it follows that δ is a monomorphism. Hence we may define an F-vector space structure on R. In fact, R is finite-dimensional. To see this, we notice that D/DP is an n-dimensional F-vector space and that $Q_j^{e_j}/DP$ is a vector subspace of D/DP. Given that

$$(D/DP)/(Q_j^{e_j}/DP) \simeq D/Q_j^{e_j} = R,$$

R is finite-dimensional. We also need to show that the R_i are vector subspaces of R. For $i = 1, \dots, k-1$, the set R_i is clearly an additive group. If $c \in C$ and $x \in Q_j^i$, then $cx \in Q_j^i$, because $c \in D$ and Q_j^i is an ideal of D. Therefore we may define a scalar product on R_i by $(c+P)(x+Q_j^i) = cx+Q_j^i$. (There is no difficulty in seeing that this scalar product is well-defined.) Hence the R_i are F-vector spaces. Clearly

$$R \supset R_1 \supset \cdots \supset R_{k-1} \supset R_k = \{0\},$$

so the R_i are finite-dimensional subspaces of R.

- In order to apply Theorem 15.3 we need to check that the conditions (C) given before Lemma 15.3 are satisfied:

- **a.** If $x + Q_j^k \in R$ and $y + Q_j^k \in R_i$, then $(x + Q_j^k)(y + Q_j^k) = xy + Q_j^k$, with $xy \in Q_k^i$, because $y \in Q_k^i$, so the R_i are ideals of R.
- **b.** Suppose that there is an ideal I of R such that $R_{i-1} \supset I \supset R_i$. Let $\lambda : D \longrightarrow D/Q_j^k$ be the standard homomorphism. If $J = \lambda^{-1}(I)$, then J is an ideal and $Q_j^{i-1} \supset J \supset Q_j^i$. As $Q_j^{i-1} \supset J$, there is an ideal A such that $J = Q_j^{i-1}A$. If $A = D$, then $J = Q_j^{i-1}$. If this is not the case, then, as $J \supset Q_j^i$, $A = Q_j$ and so $J = Q_j^i$. It follows that $R_{i-1} = I$ or $I = R_i$.
- **c.** If $\bar{y} = y + Q_j^k \in R_1$ and $\bar{z} = z + Q_j^k \in R_{i-1}$; then $\bar{y}\bar{z} = yz + Q_j^k$, with $yz \in Q_j^i$, so $\bar{y}\bar{z} \in R_i$.

Therefore the conditions (C) are satisfied.

- We now apply Theorem 15.3. Let $x \in D$ and $\bar{x} = x + Q_j^k \in R$ and consider the mapping $\theta = \theta_{\bar{x}}$ defined by multiplication by $\bar{x}$: for all $\bar{y} \in R$,

$$\theta(\bar{y}) = \bar{x}\bar{y} = xy + Q_j^k.$$

Since R_j is an ideal of R, $\theta(R_j) \subset R_j$. From Theorem 15.3 we have

$$\text{char}_{\,(D/Q_j^k)/F}\,(\pi_j((\psi_0(x))) = \text{char}_{\,R/F}\,(\pi_j((\psi_0(x))) = \left(\text{char}_{\,(R/R_1)/F}(\theta_1)\right)^k$$

and for θ_1 we have

$$\theta_1(\bar{y} + R_1) = \bar{x}\bar{y} + R_1.$$

- Next we notice that

$$R/R_1 = (D/Q_j^k)/(Q_j/Q_j^k) \simeq D/Q_j = L_j.$$

(As R_1 is a finite-dimensional subspace of R, R/R_1 is finite-dimensional and hence this is the case for L_j.) The isomorphism of F-vector spaces from R/R_1 onto L_j, which we note α, has the explicit form:

$$\alpha(\bar{y} + R_1) = y + Q_j = \psi_j(y).$$

If $x \in D$, then the element $\psi_j(x)$ belongs to L_j and, in conformity with the notation already used, we define the mapping $\theta_{\psi_j(x)}$ to be multiplication by the element $\psi_j(x)$. Then, for all $y \in D$,

$$\theta_{\psi_j(x)}\,(\alpha(\bar{y} + R_1)) = (x + Q_j)(y + Q_j) = xy + Q_j$$

and

$$\alpha\,(\theta_1(\bar{y} + R_1)) = \alpha(\bar{x}\bar{y} + R_1) = xy + Q_j,$$

thus

$$\theta_{\psi_j(x)} \circ \alpha = \alpha \circ \theta_1.$$

We may now write

$$\begin{aligned}
\text{char}_{\,(R/R_1)/F}(\theta_1) &= \text{char}_{\,(R/R_1)/F}\left(\alpha^{-1} \circ \theta_{\psi_j(x)} \circ \alpha\right) \\
&= \text{char}_{\,\alpha(R/R_1)/F}\left(\theta_{\psi_j(x)}\right) \\
&= \text{char}_{\,L_j/F}\,(\psi_j(x))\,.
\end{aligned}$$

Therefore we have obtained

$$\text{char}_{\,(D/Q_j^k)/F}\,(\pi_j((\psi_0(x))) = \text{char}_{\,L_j/F}\,(\psi_j(x))^k$$

and it follows that

$$\prod_{i=1}^{r} \text{char}_{\,(D/Q_i^{e_i})/F}\,(\pi_i(\psi_0(x))) = \prod_{i=1}^{r} \text{char}_{\,L_i/F}\,(\psi_i(x))^{e_i}\,.$$

Part 4

We have now shown that

$$\text{char}_{\,(D/DP)/F}\,(\psi_0(x)) = \prod_{i=1}^{r} \text{char}_{\,L_i/F}\,(\psi_i(x))^{e_i}\,.$$

and so

$$\tilde{\psi}_0^*\left(\text{char }_{D'/C'}(x)\right) = \phi^*\left(\prod_{i=1}^r \text{char }_{L_i/F}\left(\psi_i(x)\right)^{e_i}\right).$$

However,

$$\tilde{\psi}_0^*\left(\text{char }_{D'/C'}(x)\right) = \phi^* \circ \psi^*\left(\text{char }_{L/K}(x)\right)$$

and it follows that

$$\psi^*\left(\text{char }_{L/K}(x)\right) = \prod_{i=1}^r \text{char }_{L_i/F}\left(\psi_i(x)\right)^{e_i},$$

which is the first equality in the statement of the theorem.

Part 5

Let us set $n = \deg \text{char }_{L/K}(x)$ and $n_j = \deg \text{char }_{L_j/F}\left(\psi_j(x)\right)$, for $j = 1, \ldots, r$. The constant term of $\psi^*(\text{char }_{L/K}(x))$ is the product of the constant terms of the polynomials $\text{char }_{L/F}\left(\psi_j(x)\right)$, each taken respectively to the power e_j. However, the constant term of $\psi(\text{char }_{L/K}(x))$ is $(-1)^n\psi\left(N_{L/K}(x)\right)$ and the constant term of the product of the polynomials $\text{char }_{L_j/F}\left(\psi_j(x)\right)$, each taken respectively to the power e_j, is

$$(-1)^{\sum_{j=1}^r n_j e_j} \prod_{j=1}^r N_{L_j/F}\left(\psi_j(x)\right)^{e_j}.$$

As $n = \sum_{j=1}^r n_j e_j$, we obtain the third equality, namely

$$\psi\left(N_{L/K}(x)\right) = \prod_{j=1}^r \left(N_{L_j/F}\left(\psi_j(x)\right)\right)^{e_j}.$$

For the second equality we consider the coefficients of X^{n-1} in the two sides of the first equality. The coefficient of X^{n-1} on the lefthand side is $-\psi\left(T_{L/K}(x)\right)$. The coefficient of X^{n-1} on the righthand side is the sum of coefficients of the X^{n_j-1}, each multiplied respectively by e_j. As the coefficient of X^{n_j-1} is $-T_{L_j/F}\left(\psi_j(x)\right)$, we have the second equality, i.e.,

$$\psi\left(T_{L/K}(x)\right) = \sum_{j=1}^r e_j T_{L_j/F}\left(\psi_j(x)\right).$$

This ends the proof. □

The theorem we have just proved has an interesting corollary.

Corollary 15.2 *Let C be a Dedekind domain with fraction field K, L a finite separable extension of K and D the integral closure of C in L. If P is a prime ideal of C and $DP = \prod_{i=1}^r Q_i^{e_i}$, then*

$$[L : K] = \sum_{i=1}^r e_i f_i,$$

where $f_i = [D/Q_i : C/P]$.

PROOF It is sufficient to consider the degrees of the characteristic polynomials in the statement of Theorem 15.4 **a.** □

Remark The corollary which we have just proved is in fact a generalization of Theorem 13.6.

We will need another result, based on the Chinese remainder theorem.

Proposition 15.6 *Let D be a Dedekind domain and $P_1, \dots, P_s$ distinct nonzero prime ideals in D. Suppose that $x_1, \dots, x_s \in D$ and $e_1, \dots, e_s \in \mathbf{N}$. Then there exists $x \in D$ such that*

$$x - x_i \in P_i^{e_i} \quad \textit{and} \quad x - x_i \notin P_i^{e_i+1},$$

for $i = 1, \dots, s$.

PROOF For each i, $P_i^{e_i+1}$ is strictly included in $P_i^{e_i}$, so there exists $a_i \in P_i^{e_i} \setminus P_i^{e_i+1}$. If $i \neq j$, then P_i^{i+1} and P_j^{j+1} are coprime. From the Chinese remainder theorem (Theorem F.1) there exists $x \in D$ such that

$$\begin{array}{ccl} x & \equiv & (x_1 + a_1) \ (\mathrm{mod}\ P_1^{e_1+1}) \\ \vdots & \vdots & \vdots \quad\quad \vdots \\ x & \equiv & (x_s + a_s) \ (\mathrm{mod}\ P_s^{e_s+1}). \end{array}$$

Then, for all i,

$$x - (x_i + a_i) \in P_i^{e_i+1} \Longrightarrow x - x_i \in P_i^{e_i}.$$

If $x - x_i \in P_i^{e_i+1}$, then

$$(x - x_i) - a_i + a_i \in P_i^{e_i+1} \Longrightarrow a_i \in P_i^{e_i+1},$$

a contradiction. This proves the result. □

15.5 Proof of Dedekind's different theorem

Having done the preliminary work, we may prove the inequality referred to in the last section. For the notation, it is sufficient to look at the beginning of the previous section. We only recall that $K \subset L$ are number fields with associated number rings C and D. We set $n = [L : K]$.

Theorem 15.5 *For every nonzero prime ideal Q in D, we have $s_Q \geq e_Q - 1$. In addition, $s_Q = e_Q - 1$ if and only if the characteristic of the field D/Q does not divide e_Q.*

PROOF As the proof is long, we will break it up into three parts, namely

- **a.** Proof of the inequality;
- **b.** The case where the characteristic of D/Q divides e_Q;
- **c.** The case where the characteristic of D/Q does not divide e_Q.

a. Proof of the inequality Let Q be a nonzero prime ideal in D and set $P = Q \cap C$. We now set $U = C \setminus P$, $C' = U^{-1}C$ and $D' = U^{-1}D$. In the decompositions of $\Delta_{L/K}$ and DP appear a finite set of nonzero prime ideals $Q_1, \ldots, Q_m$. We have

$$\Delta_{L/K} = \prod_{i=1}^{m} Q_i^{s_i} \qquad \text{and} \qquad DP = \prod_{i=1}^{m} Q_i^{e_i}.$$

(Certain s_i or e_i may be equal to 0.) From Proposition 12.16,

$$D'P = \prod_{i=1}^{m} D'Q_i^{e_i}$$

and, having number fields, from Theorem 15.2,

$$\Delta(D'|C') = D'\Delta_{L/K} = \prod_{i=1}^{m} D'Q_i^{s_i}.$$

Hence the complementary module D'^* has the form $\prod_{i=1}^{m} D'Q_i^{-s_i}$. Then the inequalities

$$s_i \geq e_i - 1 \qquad i = 1, \ldots, m$$

hold if and only if $\prod_{i=1}^{m} D'Q_i^{1-e_i} \subset D'^*$. We aim to show that this is the case.

Let $x \in \prod_{i=1}^{m} D'Q_i^{1-e_i}$. From Theorem 12.11 we know that $P' = C'P$ is a principal ideal, so there exists $t \in C'$ such that $P' = C't$. We may suppose that $t \in C$. However,

$$\prod_{i=1}^{m} D'Q_i^{e_i} = D'P = D'C'P = D'P' = D'C't = D't,$$

so $xt \in \prod_{i=1}^{m} D'Q_i$. We claim that $T_{L/K}(xt) \in P'$. (As $xt \in D'$, we may consider that $xt \in L$, so $T_{L/K}(xt)$ is defined.) We notice first that D' is a free C'-module of rank n. This has already been shown in the proof of Theorem 12.17 in a more general framework. We have also seen, in the proof of Theorem 15.4, that if $V = C' \setminus \{0\}$, then V is a multiplicative subset of C', $V^{-1}C' = K$, $V^{-1}D' = L$ and, for $x \in D'$, we have

$$\text{char}_{\,L/K}(x) = \text{char}_{\,V^{-1}D'/V^{-1}C'}(x) = \text{char}_{\,D'/C'}(x).$$

It follows that

$$T_{L/K}(xt) = T_{D'/C'}(xt),$$

because $xt \in D'$.

We now consider $T_{D'/C'}(xt)$. In the proof of Theorem 12.17 we saw that, if $\mathcal{B}' = \{x'_1, \ldots, x'_n\}$ is a basis of the free C'-module D', then $\bar{\mathcal{B}}' = \{\bar{x}'_1, \ldots, \bar{x}'_n\}$ is a basis of the $C'/C'P$-vector space $D'/D'P$, where $\bar{x}'_i$ is the image of x'_i under the standard mapping of D' onto $D'/D'P$. We can thus apply Lemma 15.3, with ψ this standard mapping, to obtain

$$\overline{T_{D'/C'}(xt)} = T_{(D'/(D'P))/(C'/P')}(\overline{xt}).$$

We claim that $\overline{xt}$ is a nilpotent element of the ring $D'/D'P$. Let $r = e_1 + \cdots + e_m$. Then

$$xt \in \prod_{i=1}^{m} D'Q_i \Longrightarrow xt = y_1 \cdots y_m \qquad y_i \in D'Q_i,$$

where $y_i = d_i q_i$, with $d_i \in D'$ and $q_i \in Q_i$. Hence

$$(xt)^r = y^{e_1} y^{r-e_1} \cdots y_m^{e_m} y^{r-e_m} = d_1^{e_1} q_1^{e_1} \cdots d_m^{e_m} q_m^{e_m} d,$$

where $d \in D'$. As $\prod_{i=1}^m D'Q_i^{e_i}$ is an ideal, $(xt)^r \in \prod_{i=1}^m D'Q_i^{e_i} = D'P$, which implies that $\overline{xt}$ is a nilpotent element of the ring $D'/D'P$, as claimed. From the fact that $\overline{xt}$ is a nilpotent element of the ring $D'/D'P$ we obtain that char $_{(D'/(D'P))/(C'/P')}(\overline{xt}) = X^n$, which implies that $T_{(D'/(D'P))/(C'/P')}(\overline{xt}) = 0$; this in turn implies that $\overline{T_{D'/C'}(xt)} = 0$, which means that $T_{D'/C'}(xt) \in D'P$. However, $T_{D'/C'}(xt) \in C'$, so

$$T_{L/K}(xt) = T_{D'/C'}(xt) \ \in \ C'P = P'.$$

Now,

$$tT_{L/K}(x) = T_{L/K}(xt) \in P' = C't \Longrightarrow T_{L/K}(x) \in C'.$$

If $y \in D'$, then $xy \in \prod_{i=1}^m D'Q_i^{1-e_i}$, so, replacing x by xy, we obtain $T_{L/K}(xy) \in C'$. Therefore $x \in D'^*$, which finishes the proof of the first part of the theorem.

b. The case where the characteristic of D/Q divides e_Q Suppose that Q is a prime ideal in D such that the characteristic of the field D/Q divides the ramification index e_Q. If $P = C \cap Q$, then P is a nonzero prime ideal. Supposing that $DP = Q_1^{e_1} \cdots Q_m^{e_m}$ is the decomposition of DP into prime ideals, then $Q = Q_i$, for some i. Without loss of generality, let us suppose that $Q = Q_1$. We set

$$J = D'Q_1^{-e_1} \prod_{i=2}^m D'Q_i^{-s_i}.$$

If $J \subset D'^* = \prod_{i=1}^m D'Q_i^{-s_i}$, then

$$D'Q_1^{-s_1} | D'Q_1^{-e_1} \Longrightarrow D'Q_1^{-s_1} \supset D'Q_1^{-e_1} \Longrightarrow D'Q_1^{s_1} \subset D'Q_1^{e_1},$$

which implies that $s_1 \geq e_1$. We aim to show that $J \subset D'^*$. Let $x \in J$. We notice that

$$J \subset \prod_{i=2}^m D'Q_i^{-s_i} \Longrightarrow x \in \prod_{i=2}^m D'Q_i^{-s_i}.$$

Since $1 - e_i \geq -s_i$, for $i = 2, \ldots, m$, $\prod_{i=2}^m Q_i^{1-e_i} \supset \prod_{i=2}^m Q_i^{-s_i}$, so $x \in \prod_{i=2}^m Q_i^{1-e_i}$, and, from part **a.**, we may write $xt \in \prod_{i=2}^m D'Q_i$. Then $xt \in D'$ and $T_{L/K}(xt) = T_{D'/C'}(xt) \in C'$. We now use Theorem 15.4, with $\psi : C' \longrightarrow C'/P'$ and $\psi_i : D' \longrightarrow D'/D'Q_i$, for $i = 1, \ldots, m$, the standard mappings. Then, setting $L_i' = D'/D'Q_i$ and $F' = C'/P'$, we have

$$\psi\left(T_{L/K}(xt)\right) = \sum_{i=1}^m e_i T_{L_i'/F'}\left(\psi_i(xt)\right) = e_i T_{L_1'/F'}\left(\psi_1(xt)\right),$$

because $xt \in \prod_{i=2}^m D'Q_i = \cap_{i=2}^m D'Q_i$.

In addition, $\psi_1(xt)$ is in $D'/D'Q_1$, which is isomorphic to D/Q_1, by Corollary 12.11, and so has a characteristic which is a divisor of e_1. Given that the trace $T_{L_1'/F'}\left(\psi_1(xt)\right)$ belongs to $D'/D'Q_1$, we have $\psi\left(T_{L/K}(xt)\right) = 0$. This implies that $T_{L/K}(xt) \in P'$, hence

$$tT_{L/K}(x) = T_{L/K}(xt) \in P' = C't \Longrightarrow T_{L/K}(x) \in C'.$$

If $y \in D'$, then $xy \in J$, because J is a D'-module. It follows that $T_{L/K}(xy) \in C'$, which shows that $x \in D'^*$, as required. We have shown that

$$s_1 \geq e_1 \Longrightarrow s_1 \neq e_1 - 1.$$

This finishes the proof of part **b.**

<u>**c. The case where the characteristic of D/Q does not divide e_Q**</u> We will use the notation defined in **a.** and **b.** For example, we set $P = C \cap Q$ and suppose that $DP = Q_1^{e_1} \cdots Q_m^{e_m}$, with $Q = Q_1$. Let $x \in D'$ be such that $\psi_1(x) \in D'/D'Q_1$ has nonzero trace, i.e., $T_{L_1'/F'}(\psi_1(x)) \neq 0$. (For example, we could take $x = 1$.) From Proposition 15.6 there exists $y \in D'$ such that $y - x \in D'Q_1$ and $y \in D'Q_i^{e_i}$, for $i = 2, \ldots, m$. On the one hand, $\psi_1(y) = \psi_1(x) \neq 0$, and so $\psi_1(y)$ has nonzero trace; on the other hand, for $i = 2, \ldots, m$ such that $e_i \neq 0$, $y \in D'Q_i$, hence $\psi_i(y) = 0$. Applying Theorem 15.4 we obtain

$$\psi\left(T_{L/K}(y)\right) = \sum_{i=1}^m e_i T_{L_i'/F'}\left(\psi_i(y)\right) = e_1 T_{L_1'/F'}\left(\psi_1(y)\right) \neq 0,$$

because the characteristic of $D'/D'Q_1$ (equal to that of D/Q_1) does not divide e_1. Therefore

$$T_{L/K}(y) = T_{D'/C'}(y) \notin P' = C't \Longrightarrow T_{L/K}(\frac{y}{t}) \notin C'.$$

Now,

$$D't = \prod_{i=1}^m D'Q_i^{e_i} \Longrightarrow D'Q_1^{-e_1} = (D't)^{-1} \prod_{i=2}^m D'Q_i^{e_i}.$$

Also, $\frac{1}{t} \in (D't)^{-1}$, because $(D't)^{-1} = D'\frac{1}{t}$, and, for $i = 2, \ldots, m$,

$$y \in D'Q_i^{e_i} \Longrightarrow y \in \cap_{i=2}^m D'Q_i^{e_i} = \prod_{i=2}^m D'Q_i^{e_i},$$

because the ideals $D'Q_i^{e_i}$ are pairwise coprime. Therefore

$$\frac{y}{t} \in (D't)^{-1} \prod_{i=2}^m D'Q_i^{e_i} = D'Q_1^{-e_1}.$$

Given that $\frac{y}{t} \notin D'^*$, it must be so that $D'Q_1^{-e_1}$ is not included in D'^*.

Suppose now that $s_1 \geq e_1$. Then $D'Q_1^{e_1} \prod_{i=2}^m D'Q_i^{s_i}$ divides $\prod_{i=1}^m D'Q_i^{s_i}$, which implies that $D'Q_1^{e_1}$ divides $\prod_{i=1}^m D'Q_i^{s_i}$, i.e.,

$$D'Q_1^{e_1} \supset \prod_{i=1}^m D'Q_i^{s_i} \Longrightarrow D'Q_1^{-e_1} \subset D'^*,$$

a contradiction. Therefore

$$e_1 > s_1 \geq e_1 - 1 \Longrightarrow s_1 = e_1 - 1,$$

as required. □

The theorem which we have just proved has an important consequence.

Corollary 15.3 *A nonzero prime ideal Q in D is ramified in L/K if and only if Q divides the different $\Delta_{L/K}$. Hence D has only a finite number of ramified prime ideals.*

PROOF If Q is ramified in L/K, then $e_Q \geq 2$, which implies that $s_Q \geq 1$ and so Q divides the different $\Delta_{L/K}$. On the other hand, if Q is not ramified in L/K, then $e_Q = 1$, which implies that $s_Q = 0$, so Q does not divide the different $\Delta_{L/K}$. □

15.6 Total ramification

We recall the definition of a totally ramified prime ideal or prime number. Let $K \subset L$ be number fields such that L/K is Galois and $[L : K] = n < \infty$. We set $R = O_K$ and $S = O_L$ and suppose that P is a nonzero prime ideal in R. If there is a prime ideal Q in S such that $SP = Q^n$, then we say that P is totally ramified in S. If $K = \mathbf{Q}$ and $p \in \mathbf{Z}$ is a prime number, then we say that p is totally ramified in S if the ideal (p) is totally ramified in S.

Example $1 + i$ is irreducible in $\mathbf{Z}[i]$, so prime. Hence $(1 + i)$ is a prime ideal in $\mathbf{Z}[i]$. As $\mathbf{Z}[i]2 = (1 + i)^2$, the prime number 2 is totally ramified in $\mathbf{Z}[i]$.

We will presently return to the context of number fields; however, before doing so, we will establish some results in the more general context of Dedekind domains.

Proposition 15.7 *Let C be a Dedekind domain, K its field of fractions, L a finite Galois extension of K and D the integral closure of C in L. We suppose that P is a prime ideal in C and assume that there is a unique ideal Q such that $C \cap Q = P$. Finally we let $U = C \setminus P$ and set $D' = U^{-1}D$. Then $D_Q = D'$.*

PROOF Let $x \in D'$. As $Q \cap C = P$, if $x \notin P$, then $x \notin Q$, so $U \subset D \setminus Q$. This implies that $D' \subset D_Q$. We now must show that $D_Q \subset D'$. If every element of D_Q is integral over C', then D_Q is contained in the integral closure of C' in L, which is D'. We aim to show that this is the case. If $x \in D_Q$, then $x = \frac{d}{v}$, where $d \in D$ and $v \in D \setminus Q$. As d is integral over C, d is also integral over C_P, so it is sufficient to show that $\frac{1}{v}$ is integral over C_P. Let

$$m(v, K) = a_0 + a_1X + \cdots + a_{n-1}X^{n-1} + X^m \in C[X]$$

be the minimal polynomial of v over K. (From Theorem 11.1, m belongs to $C[X]$, because v is integral over C.) Since L/K is a Galois extension and Q is the only ideal of D such that $C \cap Q = P$, we have $\sigma(Q) = Q$, for all $\sigma \in Gal(L/K)$. This implies that no conjugate of v lies in Q and hence the product of the conjugates of v is not in Q. Hence $a_0 \in C \setminus P$ and so $\frac{1}{v} \in C_P$. However, $\frac{1}{v}$ is a root of the polynomial

$$f(X) = \frac{1}{a_0} + \frac{a_{n-1}}{a_0}X + \cdots + \frac{a_1}{a_0}X^{n-1} + X^n \in C_P[X],$$

hence $\frac{1}{v}$ is integral over C_P. □

The next result is technical.

Proposition 15.8 *Let C be a Dedekind domain, K its field of fractions, L a finite Galois extension of K and D the integral closure of C in L. We also suppose that $L = K(t)$, where $t \in D$ and we set $f = m(t, K)$ and $n = \deg f$. Then*

- **a.** $T_{L/K}\left(\frac{t^i}{f'(t)}\right) = 0$, *for* $i = 0, 1, \cdots, n-2$, *and* $T_{L/K}\left(\frac{t^{n-1}}{f'(t)}\right) = 1$;
- **b.** $C[t]^* = \frac{1}{f'(t)} C[t]$.

PROOF **a.** As L is a Galois extension of K, we may write

$$f(X) = \prod_{k=1}^{n} (-t_k + X),$$

with $t = t_1$ and $t_1, t_2, \ldots, t_n$ distinct elements of L. (As L/K is separable, the roots of f are simple; these roots lie in L because L/K is normal.)

We now consider the rational fraction $\frac{1}{f}$. To begin with, the partial fraction decomposition theorem (Theorem A.9) in $L[X]$ ensures that there exist $a_1, \ldots, a_n \in L$ such that

$$\frac{1}{f(X)} = \frac{1}{\prod_{k=1}^{n}(-t_k + X)} = \sum_{k=1}^{n} \frac{a_k}{-t_k + X},$$

where $a_k \in L$. Multiplying by $f(X)$ we obtain

$$1 = \sum_{k=1}^{n} \frac{f(X) a_k}{-t_k + X} = \sum_{k=1}^{n} a_k \left(\prod_{i \neq k} (-t_i + X) \right).$$

Setting $X = t_j$, we find

$$1 = \sum_{k=1}^{n} a_k \left(\prod_{i \neq k} (-t_i + t_j) \right) = a_j \prod_{i \neq j} (-t_i + t_j),$$

and so

$$a_j = \frac{1}{\prod_{i \neq j}(-t_i + t_j)} = \frac{1}{f'(t_j)}.$$

From this we obtain the expression

$$\frac{1}{f(X)} = \sum_{k=1}^{n} \frac{1}{f'(t_k)(-t_k + X)}.$$

To continue we consider the rational fraction $\frac{1}{f(X)}$ in the ring of formal Laurent series $L((\frac{1}{X}))$, composed of series of the form $\sum_{-\infty}^{m} a_i X^i$, with $a_i \in L$ and $m \in \mathbf{Z}$. It is easy to check that, for $k = 1, \ldots, n$,

$$(-t_k + X)^{-1} = X^{-1} + t_k X^{-2} + t_k^2 X^{-3} + \cdots,$$

hence

$$\frac{1}{f(X)} = \sum_{k=1}^{n} \frac{1}{f'(t_k)} (X^{-1} + t_k X^{-2} + t_k^2 X^{-3} + \cdots).$$

However, $\frac{1}{f(X)}$ is also equal to $\frac{1}{\prod_{k=1}^{n}(-t_k + X)}$ and so

$$
\begin{aligned}
\frac{1}{f(X)} &= (X^{-1}+t_1X^{-2}+t_1^2X^{-3}+\cdots)\cdots(X^{-1}+t_nX^{-2}+t_n^2X^{-3}+\cdots) \\
&= X^{-n}(1+t_1X^{-1}+t_1^2X^{-2}+\cdots)\cdots(1+t_nX^{-1}+t_n^2X^{-2}+\cdots) \\
&= X^{-n}+b_1X^{-(n+1)}+b_2X^{-(n+2)}+\cdots
\end{aligned}
$$

Comparing the two formal Laurent series for $\frac{1}{f(X)}$ we find

$$\sum_{k=1}^{n}\frac{t_k^i}{f'(t_k)}=0,$$

for $i=0,1,\cdots,n-2$, and

$$\frac{t_k^{n-1}}{f'(t_k)}=1.$$

Now, using Corollary 10.3 and the fact that $f'\in K[X]$, we obtain

$$
\begin{aligned}
T_{L/K}\left(\frac{t^i}{f'(t)}\right) &= \sum_{\sigma\in Gal(L/K)}\sigma\left(\frac{t^i}{f'(t)}\right) \\
&= \sum_{\sigma\in Gal(L/K)}\frac{\sigma(t)^i}{f'(\sigma(t)} \\
&= \sum_{k=1}^{n}\frac{t_k^i}{f'(t_k)},
\end{aligned}
$$

since the sets $\{t_1,\ldots,t_n\}$ and $\{\sigma(t),\sigma\in Gal(L/K)\}$ are both composed of the conjugates of t (Proposition 6.2). This establishes part **a.** of the proposition.

b. We first show that $\frac{1}{f'(t)}C[t]\subset C[t]^*$. As t is a root of a monic polynomial in $C[X]$ of degree n, there exist $a_0,\ldots,a_{n-1}\in C$ such that

$$t^n=a_0+a_1t+\cdots+a_{n-1}t^{n-1}.$$

Thus, for all $s\geq n$, there exist $c_0,\ldots,c_{n-1}\in C$ such that

$$t^s=c_0+c_1t+\cdots+c_{n-1}t^{n-1}.$$

This implies that the set $\mathcal{B}=\{1,t,\ldots,t^{n-1}\}$ (resp. $\mathcal{B}'=\{\frac{1}{f'(t)},\frac{t}{f'(t)},\ldots,\frac{t^{n-1}}{f'(t)}\}$) generates the C-module $C[t]$ (resp. C-module $\frac{1}{f'(t)}C[t]$). As $\mathcal{B}$ and $\mathcal{B}'$ are clearly independant sets, they are bases of the respective C-modules $C[t]$ and $\frac{1}{f'(t)}C[t]$.

For $0\leq i\leq n-1$ and $0\leq j\leq n-1$, there exist $d_0,\ldots,d_{n-1}\in C$ such that

$$t^{i+j}=d_0d_1t+\cdots+d_{n-1}t^{n-1}.$$

(For $i+j\geq n$, this is clear; for $i+j<n$, it is sufficient to take $d_{i+j}=1$ and $d_k=0$, for $k\neq i+j$.) Thus

$$T_{L/K}\left(\frac{t^{i+j}}{f'(t)}\right)=d_0T_{L/K}\left(\frac{1}{f'(t)}\right)+d_1T_{L/K}\left(\frac{t}{f'(t)}\right)+\cdots+d_{n-1}T_{L/K}\left(\frac{t^{n-1}}{f'(t)}\right)=d_{n-1},$$

from part **a.** Hence $T_{L/K}\left(\frac{t^{i+j}}{f'(t)}\right) \in C$.

However,

$$C[t]^* = \{x \in L : T_{L/K}(xz) \in C, \forall z \in C[t]\}$$

and an element of $\frac{1}{f'(t)}C[t]$ (resp. $C[t]$) has the form $\sum_{i=1}^{n-1} a_i \frac{t^i}{f'(t)}$ (resp. $\sum_{j=1}^{n-1} b_j t^j$). Hence, for $x \in \frac{1}{f'(t)}C[t]$ and $z \in C[t]$, we have

$$T_{L/K}(xz) = T_{L/K}\left(\sum_{i=1}^{n-1} a_i \frac{t^i}{f'(t)} \sum_{j=1}^{n-1} b_j t^j\right) = \sum_{0 \le i,j \le n-1} a_i b_j \left(\frac{t^{i+j}}{f'(t)}\right) \in C$$

and so $\frac{1}{f'(t)}C[t] \subset C[t]^*$.

We now consider the reverse inclusion $C[t]^* \subset \frac{1}{f'(t)}C[t]$. An element y of $C[t]^*$ is in $L = K(t)$. Thus there exist $k_0, \dots, k_{n-1} \in K$ such that

$$y = \frac{k_0}{f'(t)} + \frac{k_1 t}{f'(t)} + \cdots + \frac{k_{n-1}t^{n-1}}{f'(t)}.$$

(Clearly $y = \sum_{i=0}^{n-1} k_i' t^i$, with $k_i' \in K$; setting $k_i = k_i' f'(t)$, we obtain the required expression for y.) Moreover,

$$T_{K/L}(y) = k_0 T_{L/K}\left(\frac{1}{f'(t)}\right) + k_1\left(\frac{t}{f'(t)}\right) + \cdots + k_{n-1}\left(\frac{t^{n-1}}{f'(t)}\right) = k_{n-1},$$

from part **a.** As $y \in C[t]^*$, $T_{K/L}(y) = T_{K/L}(y1) \in C$, i.e., $k_{n-1} \in C$. Now,

$$\begin{aligned} T_{L/K}(yt) &= k_0 T_{L/K}\left(\frac{t}{f'(t)}\right) + k_1 T_{L/K}\left(\frac{t^2}{f'(t)}\right) + \cdots + k_{n-2} T_{L/K}\left(\frac{t^{n-1}}{f'(t)}\right) + k_{n-1} T_{L/K}\left(\frac{t^n}{f'(t)}\right) \\ &= k_{n-2} + k_{n-1} T_{L/K}\left(\frac{t^n}{f'(t)}\right). \end{aligned}$$

Since $y \in C[t]^*$ and $t \in C[t]$, we have $T_{L/K}(yt) \in C$. Also, we have shown above the existence of $c_0, \dots, c_{n-1} \in C$ such that

$$t^n = c_0 + c_1 t + \cdots + c_{n-1}t^{n-1} \Longrightarrow T_{L/K}\left(\frac{t^n}{f'(t)}\right) \in C,$$

using **a.** It follows that $k_{n-2} \in C$. If we replace t by t^2, then we find that $k_{n-3} \in C$. Continuing the process we finally obtain that all the k_i belong to C, which implies that $C[t]^* \subset \frac{1}{f'(t)}C[t]$, as required. □

Corollary 15.4 *Let C be a Dedekind domain, K its field of fractions, L a finite Galois extension of K and D the integral closure of C in L. We also suppose that $L = K(t)$, where $t \in D$, and we denote $f = m(t, K) \in C[X]$. Then the different $\Delta(D|C) = Df'(t)$ if and only if $D = C[t]$.*

PROOF If $D = C[t]$, then

$$D^* = C[t]^* = \frac{1}{f'(t)}C[t] = \frac{1}{f'(t)}D \Longrightarrow \Delta(D|C) = f'(t)D = Df'(t),$$

because $D^{-1} = D$.

Now suppose that $\Delta(D|C) = Df'(t)$. As $C[t] \subset D$, we have $D^* \subset C[t]^*$, hence

$$D = D^{-1} = f'(t)D^* \subset f'(t)C[t]^* = C[t] \Longrightarrow C[t] = D,$$

because $C[t] \subset D$. $\square$

We now return to number rings, with the notation of the first paragraph of this section, i.e., $K \subset L$ are number fields such that L/K is Galois and $[L : K] = n < \infty$. We set $R = O_K$ and $S = O_L$ and suppose that P is a nonzero prime ideal in R which is totally ramified in S: $SP = Q^n$, where Q is a prime ideal in S. To simplify the notation, we write Δ_Q for $\Delta(S_Q|R_P)$. As Δ_Q is an ideal in S_Q, there exists an integer $s \geq 0$ such that $\Delta_Q = S_Q Q^s$. In addition, there exists $t \in S$ such that $S_Q Q = S_Q t$ (Theorem 12.12 and remark before Theorem 13.16).

Proposition 15.9 *The exponent at Q of $\Delta(S|R)$, i.e., the power of Q in the decomposition of $\Delta(S|R)$ into prime ideals of S ($s_Q(L|K)$), is equal to s.*

PROOF The decomposition of $\Delta(S|R)$ into prime ideals of S has the form

$$\Delta(S|R) = Q^{s_Q(L|K)} \prod_{i=1}^{r} Q_i^{\alpha_i},$$

where $Q_1, \ldots, Q_r$ are prime ideals in S. Setting $S' = (R \setminus P)^{-1}S$, from Proposition 12.16 the decomposition of $S'\Delta(L|K)$ into prime ideals has the form

$$S'\Delta(S|R) = (S'Q)^{s_Q(L|K)} \prod_{\substack{i=1 \\ S'Q_i \cap (S \setminus Q) = \emptyset}}^{r} (S'Q_!)^{\alpha_i}.$$

However, from Proposition 15.7, $S' = S_Q$, and from Theorem 15.2, $\Delta_Q = S_Q \Delta_Q$, thus

$$\Delta_Q = S_Q Q^{s_Q(L|K)} \prod_{\substack{i=1 \\ Q_i \cap (S \setminus Q) = \emptyset}}^{r} (S_Q Q_!)^{\alpha_i}$$

Since the decomposition of Δ_Q is unique, we must have $s_Q(L|K) = s$ and the product of the other ideals equal to S_Q. $\square$

There is an important relation between the exponent $s_Q(L|K)$ and the ramification groups V_i of Q in the extension L/K.

Theorem 15.6 *If L/K is a finite Galois extension of number fields, P a nonzero prime ideal of O_K totally ramified in O_L, Q the unique prime ideal in O_L lying over P and*

$$V_0 \supset V_1 \supset \cdots \supset V_r = \{\mathrm{id}\}$$

are the ramification groups of Q in L/K, then

$$s_Q(L|K) = \sum_{i=0}^{r-1} (|V_i| - 1).$$

PROOF We aim to apply Corollary 15.4, with $C = R_P$ and $D = S_Q$. However, we need to justify this.

First we show that $L = K(t)$. (As $t \in S$, we have $t \in S_Q$.) Since $K \subset L$ and $t \in S \subset L$, we must have $K(t) \subset L$. For the reverse inclusion, to begin we notice that the set $\mathcal{B} = \{1, t, \ldots, t^{n-1}\}$ is a K-basis of L (Corollary E.1). Thus, if $y \in L$, then there exist $a_0, a_1, \ldots, a_{n-1} \in K$ such that $y = \sum_{i=0}^{n-1} a_i t^i$, hence $y \in K[t] = K(t)$. We have shown that $L = K(t)$.

Now we show that S_Q is the integral closure of R_P in L. From Corollary 12.13, O_L is the integral closure of O_K in L. Setting $U = R \setminus P$, $R' = U^{-1}R$ and $S' = U^{-1}S$, from Proposition 12.20 we obtain that S' is the integral closure of R' in L. However, by definition $R' = R_P$ and, from Proposition 15.7, $S_Q = S'$. Thus S_Q is the integral closure of R_P in L.

Our next step is to show that $S_Q = R_P[t]$. As $\sigma(Q) = Q$, for all automorphisms $\sigma \in Gal(L/K)$, the decomposition group $D = D(Q|P) = Gal(L/K)$. Thus $L^D = K$. From Corollary 13.5 and the fact that $e = n$, we obtain $f = 1$. Now, using Proposition 13.10, we see that $L^E = K$ and so $E = Gal(L/K)$. It follows that

$$S^E = O_{L^E} = O_K = R \qquad \text{and} \qquad Q^E = P.$$

From Theorem 13.16 S_Q is a free module over $S_P^E = R_P$, with basis $\mathcal{B} = \{1, t, \ldots, t^{n-1}\}$, where $t \in S$ is a generator of the principal ideal $S_Q Q$. Hence $S_Q = R_P[t]$ as required.

We have shown that the conditions for applying Corollary 15.4, with $C = R_P$ and $D = S_Q$, are met. Thus $\Delta_Q = S_Q f'(t)$, where $f = m(t, K)$. (This makes sense, because $f \in R[X]$ and $R \subset R_P \subset S_Q$, which implies that $f'(t) \in S_Q$.) To simplify the notation we set $G = Gal(L/K)$. Then

$$f(X) = \prod_{\sigma \in G} (-\sigma(t) + X) \Longrightarrow f'(t) = \prod_{\substack{\sigma \in G \\ \sigma \neq \mathrm{id}}} (-\sigma(t) + t)\,.$$

We may partition the elements of G into disjoint subsets V_m/V_{m+1}, for $m = 0, 1, \ldots, r-1$. If $\sigma \in V_m \setminus V_{m+1}$, then, from Proposition 13.16, $\sigma(t) - t \in Q^{m+1} \setminus Q^{m+2}$. As $S_Q\,(-\sigma(t) - t)$ is an ideal of S_Q, there exists $s(\sigma) \in \mathbf{N}$ such that $S_Q\,(-\sigma(t) + t) = S_Q t^{s(\sigma)}$. With s as defined in the paragragh before Proposition 15.9, we obtain

$$S_Q t^s = \Delta_Q = S_Q f'(t) = S_Q \prod_{\substack{\sigma \in G \\ \sigma \neq \mathrm{id}}} (-\sigma(t) + t) = \prod_{\substack{\sigma \in G \\ \sigma \neq \mathrm{id}}} S_Q t^{s(\sigma)}.$$

Therefore

$$s = \sum_{\substack{\sigma \in G \\ \sigma \neq \mathrm{id}}} s(\sigma) = \sum_{m=0}^{r-1} \sum_{\sigma \in V_m \setminus V_{m+1}} s(\sigma).$$

We need to determine the values $s(\sigma)$, for $\sigma \in V_m \setminus V_{m+1}$. If $\sigma \in V_m \setminus V_{m+1}$, then

$$S_Q t^{s(\sigma)} = S_Q\,(-\sigma(t) + t) = S_Q Q^{m+1} = S_Q t^{m+1},$$

which implies that $s(\sigma) = m + 1$. As there are $|V_m| - |V_{m+1}|$ elements in $V_m \setminus V_{m+1}$, we have

$$\sum_{m=0}^{r-1} \sum_{\sigma \in V_m \setminus V_{m+1}} s(\sigma) = \sum_{m=0}^{r-1} (|V_m| - |V_{m+1}|)(m + 1).$$

Writing A for the sum on the right hand side, we have

$$A = (|V_0| - |V_1|)1 + (|V_1| - |V_2|)2 + \cdots + (|V_{r-1}| - |V_r|)r = |V_0| + |V_1| + \cdots + |V_{r-1}| - r,$$

because $V_r = \{\mathrm{id}\}$. Simplifying the right hand side, we find $\sum_{m=0}^{r-1}(|V_m| - 1)$. However, from Proposition 15.9, $s = s_Q(L|K)$, hence the result. □

Chapter 16

The Kronecker-Weber theorem

In this chapter we present and prove one of the principle theorems of algebraic number theory. The proof is long and needs certain preliminary results, which we handle in detail. The theorem states that any abelian finite normal extension of the rationals is included in a cyclotomic extension. Our proof follows that given in [18].

16.1 Preliminaries

We begin with a sufficient condition for a prime number to be totally ramified in a number ring.

Proposition 16.1 *If $L/\mathbf{Q}$ is a finite normal abelian extension such that the discriminant disc(O_L) is a power of a prime p, then p is totally ramified in O_L.*

PROOF We need to show that there is a unique prime ideal Q in S lying over p and that its inertial degree is 1. Let Q be a prime ideal in O_L lying over p. To simplify the notation we set $E = E(Q|\mathbf{Z}p)$. As usual we write L^E for the fixed field of E. We claim that no prime number divides the discriminant disc(O_{L^E}). Indeed, if q is such a prime number, then q ramifies in O_{L^E}, hence in O_L. Thus q divides disc(O_L), which is a power of p and so $q = p$. So we need to show that p does not ramify in O_{L^E}.

To see this, let Q_1 be a prime ideal in O_{L^E} lying over p and Q_2 a prime ideal in O_L lying over Q_1. Then Q and Q_2 are both prime ideals in O_L lying over p. As the Galois group $G = Gal(L/\mathbf{Q})$ is abelian, from Exercise 13.4 we deduce that $E(Q_2|\mathbf{Z}p) = E$. Now, Q_1 is the unique prime ideal in O_{L^E} lying under Q_2, so, from Proposition 13.14, we have $e(Q_1|\mathbf{Z}p) = 1$, i.e., p is unramified in O_{L^E}, as required, which implies that p does not divide disc(O_{L^E}).

As no prime number divides disc(O_{L^E}), from Theorem 14.5 we must have $L^E = \mathbf{Q}$. Since $\mathbf{Q} \subset L^D \subset L^E$, it is also the case that $L^D = \mathbf{Q}$. From Theorem 6.7, we obtain

$$Gal(L/\mathbf{Q}) = Gal(L/L^D) = D.$$

Let Q and Q' be prime ideals in O_L lying over p. Given that L/Q is normal, there exists $\sigma \in Gal(L/\mathbf{Q})$ such that $\sigma(Q) = Q'$. However, $Gal(L/\mathbf{Q}) = D(Q|\mathbf{Z}p)$, which implies that $Q = Q'$ and so there is a unique prime ideal in O_L lying over p.

We now consider the inertial degree $f(Q|p)$. Proposition 13.10 assures that $[L^E : L^D] = f(Q|p)$. As $L^E = L^D$, we have $f(Q|p) = 1$ and so p is totally ramified in O_L. □

Example Let ζ be a p^r primitive root of unity, where p is an odd prime and $r \geq 1$, and $K = \mathbf{Q}(\zeta)$. From Theorem 11.15 we know that the discriminant $\mathrm{disc}(O_K)$ is a power of p, hence p is totally ramified in O_K.

If L is a number field as in Proposition 16.1, i.e., $L/\mathbf{Q}$ is a finite normal abelian extension such that the discriminant $\mathrm{disc}(O_L)$ is a power of a prime p, and K a number field included in L, then $K/\mathbf{Q}$ is also a finite normal abelian extension. This follows from Theorem 6.6: We can write $K = L^H$, where H is a subgroup of $G = Gal(L/\mathbf{Q})$, which is normal, because the Galois group is abelian. It follows that $K/\mathbf{Q}$ is a normal extension. Also, the Galois group $G' = Gal(K/\mathbf{Q})$ is isomorphic to the quotient group G/H, which is abelian, because G is abelian. To simplify the notation we write $S = O_L$ and $R = O_K$. Let Q be the unique prime ideal of S lying over p and Q_1 the unique prime ideal of R lying under Q. We aim to show that, if $[K : \mathbf{Q}] = p$, then $s_{Q_1}(K|\mathbf{Q})$, the exponent at Q_1 of the different $\Delta(K|Q)$, is independant of the field K which we choose.

Proposition 16.2 *Let $L/\mathbf{Q}$ be a finite normal abelian extension such that the discriminant $disc(O_L)$ is a power of an odd prime p and K a number field included in L whose degree over $\mathbf{Q}$ is p. Then p is totally ramified in R and, if Q_1 denotes the unique prime ideal of R lying over p, then $s_{Q_1}(K|\mathbf{Q}) = 2(p-1)$, where $s_{Q_1}(K|\mathbf{Q})$ is the exponent at Q_1 of the different $\Delta(K|Q)$.*

PROOF Our first step is to show that p is totally ramified in R. Suppose that Q_2 and Q_3 are distinct prime ideals in R lying over p. Then Q_2 (resp. Q_3) lies under a prime ideal Q_2' (resp. Q_3') in S. Clearly Q_2' and Q_3' are distinct and lie over p. As p is totally ramified in S, this is impossible, hence there is a unique prime ideal in R lying over p. We also notice that

$$1 = f(Q|p) = f(Q|Q_1)f(Q_1|p) \Longrightarrow f(Q_1|p) = 1$$

and so p is totally ramified in R, or equivalently, $\mathbf{Z}p$ is totally ramified in R.

We now apply Theorem 15.6 to obtain

$$s_{Q_1}(K|\mathbf{Q}) = \sum_{i=0}^{r-1}(|V_i'| - 1),$$

where V_i' denotes the ith ramification group of Q_1 in the extension $K/\mathbf{Q}$. Now, each V_i' is a subgroup of $Gal(K/\mathbf{Q})$ and $|Gal(K/\mathbf{Q})| = [K : \mathbf{Q}] = p$, so $|V_i'|$ has the value 1 or p and it follows that $p-1$ divides $s_{Q_1}(K|\mathbf{Q})$.

In the spirit of the discussion before Proposition 15.9, we write $\Delta_{Q_1} = \Delta(R_{Q_1}|\mathbf{Z}_{\mathbf{Z}p})$, which is an ideal in R_{Q_1}. In addition, there exists $t \in R$ such that $R_{Q_1}Q_1 = R_{Q_1}t$ and an integer $s > 0$ such that $\Delta_{Q_1} = R_{Q_1}Q_1^s = R_{Q_1}t^s$. Proposition 15.9 tells us that $s_{Q_1}(K|\mathbf{Q}) = s$. We will use this relation to determine the precise value of $s_{Q_1}(K|\mathbf{Q})$.

We aim to use Corollary 15.4 with $C = \mathbf{Z}_{\mathbf{Z}p}$ and $D = R_{Q_1}$ and respective fields of fractions $\mathbf{Q}$ and K. We need to check that the conditions of the corollary are satisfied. $R = O_K$ is the integral closure of $\mathbf{Z}$ in K by definition; Proposition 15.7 then assures us that R_{Q_1} is the integral closure of $\mathbf{Z}_{\mathbf{Z}p}$ in K. Showing that $K = \mathbf{Q}(t)$, with $t \in R_{Q_1}$ is a little more difficult.

We claim that R_{Q_1} is a free module over $\mathbf{Z}_{\mathbf{Z}p}$, with basis $\mathcal{B} = \{1, t, \ldots, t^{p-1}\}$. To establish this we use Theorem 13.16. We set $E = E(Q_1|\mathbf{Z}p)$ and $D = D(Q_1|\mathbf{Z}p)$. From Proposition 13.10,

$$[K^E : K^D] = f(Q_1|p) = 1 \Longrightarrow K^E = K^D.$$

For all $\sigma \in G = Gal(K/\mathbf{Q})$, we have $\sigma(Q_1) = Q_1$, because Q_1 is the only prime ideal lying over p. This implies that $G \subset D$ and so $D = G$ Thus

$$K^E = K^D = K^G = \mathbf{Q}.$$

and so

$$R^E = O_{K^E} = O_{\mathbf{Q}} = \mathbf{Z}.$$

Continuing we have

$$Q_1^E = R^E \cap Q_1 = \mathbf{Z} \cap Q_1 = \mathbf{Z}p \Longrightarrow R^E_{Q_1^E} = \mathbf{Z}_{\mathbf{Z}p}.$$

In addition, $e = e(Q_1|p) = p$. From Theorem 13.16 we obtain that R_{Q_1} is a free module over $\mathbf{Z}_{\mathbf{Z}p}$, with basis $\mathcal{B} = \{1, t, \dots, t^{p-1}\}$, as required.

From Corollary E.1, $\mathcal{B}$ is a basis of K over $\mathbf{Q}$, which implies that $K = \mathbf{Q}[t] = \mathbf{Q}(t)$.

Now we have the conditions for applying Corollary 15.4. Also, we have seen that R_{Q_1} is a free module over $\mathbf{Z}_{\mathbf{Z}p}$ and so $R_{Q_1} = \mathbf{Z}_{\mathbf{Z}_p}[t]$. It follows that

$$\Delta(R_{Q_1}|\mathbf{Z}_{\mathbf{Z}p}) = R_{Q_1} f'(t),$$

where f is the minimal polynomial $m(t, \mathbf{Q})$. If

$$f(X) = a_0 + a_1 X + \cdots + a_{p-1} X^{p-1} + X^p,$$

then $f \in \mathbf{Z}[X]$ and

$$f'(t) = a_1 + 2a_2 t + \cdots + (p-1)a_{p-1} t^{p-2} + p t^{p-1}.$$

We notice that

$$Rp = R\mathbf{Z}p = Q_1^p,$$

because $\mathbf{Z}p$ is totally ramified in R and Q_1 is the unique prime ideal of R lying over $\mathbf{Z}p$. Hence,

$$R_{Q_1} p = R_{Q_1} R p = R_{Q_1} Q_1^p = R_{Q_1} t^p,$$

thus

$$R_{Q_1} p t^{p-1} = (R_{Q_1} p)(R_{Q_1} t^{p-1}) = R_{Q_1} t^{2p-1},$$

from which we deduce that there exists $\alpha_p \in R_{Q_1}$ such that $pt^{p-1} = \alpha_p t^{2p-1}$. It is important to notice that $t \not| \alpha_p$. If $t|\alpha_p$, then $pt^{p-1} = \alpha'_p t^{2p}$, with $\alpha'_p \in R_{Q_1}$ and we obtain

$$R_{Q_1} t^{2p-1} \subset R_{Q_1} t^{2p} \Longrightarrow R_{Q_1} t^{2p-1} = R_{Q_1} t^{2p},$$

Thus

$$(R_{Q_1})^{2p-1} = (R_{Q_1})^{2p},$$

which is impossible, because $R_{Q_1} Q_1$ is a nonzero prime ideal in the Dedekind domain R_{Q_1}.

For $i = 0, 1, \dots, p-1$ such that $v_p(ia_i) \geq 0$, we can write $ia_i = p^{v_p(a_i)} b_i$, where $p \not| b_i$. Then

$$R_{Q_1} i a_i t^{i-1} = (R_{Q_1} i a_i)(R_{Q_1} t^{i-1}) = (R_{Q_1} p^{v_p(ia_i)})(R_{Q_1} b_i)(R_{Q_1} t^{i-1}).$$

As $p \not| b_i$, b_i is invertible in R_{Q_1}, we have $R_{Q_1} b_i = R_{Q_1}$ and thus

$$R_{Q_1} i a_i t^{i-1} = R_{Q_1} t^{p v_p(ia_i)} R_{Q_1} t^{i-1} = R_{Q_1} t^{p v_p(ia_i) + i - 1},$$

from which we deduce that there exists $\alpha_i \in R_{Q_1}$ such that $ia_it^{i-1} = \alpha_i t^{pv_p(ia_1)+i-1}$. We notice that $t \not| \alpha_i$. If $t|\alpha_i$, then $ia_it^{i-1} = \alpha_i' t^{pv_p(ia_i)+i}$, with $\alpha_i' \in R_{Q_1}$ and so

$$R_{Q_1}t^{pv_p(ia_1)+i-1} \subset R_{Q_1}t^{pv_p(ia_i)+i} \Longrightarrow R_{Q_1}t^{pv_p(ia_1)+i-1} = R_{Q_1}t^{pv_p(ia_i)+i},$$

or

$$(R_{Q_1})^{pv_p(ia_1)+i-1} = (R_{Q_1})^{pv_p(ia_1)+i},$$

which is impossible, because $R_{Q_1}Q_1$ is a nonzero prime ideal in the Dedekind domain R_{Q_1}.

We notice that the integers $pv_p(ia_i) + i - 1$, for $i = 0, 1, \ldots, p-1$, with $ia_i \neq 0$, and $2p - 1$ are distinct. If m is the minimum of these integers and α_{i_0} corresponds to the minimum, then

$$f'(t) = (\alpha_{i_0} + \beta t)t^m,$$

where $\alpha_{i_0}, \beta \in R_{Q_1}$ and $t \not| \alpha_{i_0}$. Thus,

$$t \not| (\alpha_{i_0} + t\beta) \Longrightarrow \alpha_{i_0} + \beta t \notin R_{Q_1}t = R_{Q_1}Q_1,$$

the unique maximal ideal of R_{Q_1}. From Exercise 12.11, the element $\alpha_{i_0} + \beta t$ is invertible in R_{Q_1} and hence

$$R_{Q_1}f'(t) = R_{Q_1}t^m \Longrightarrow s_{Q_1}(K|\mathbf{Q}) = m.$$

We now conclude. By definition of the minimum m, we have $s_{Q_1}(K|\mathbf{Q}) \leq 2p - 1$. Also, from Theorem 15.5, $s_{Q_1}(K|\mathbf{Q}) \geq p - 1$. The characteristic of the field R/Q_1 is p, because $p \in Q_1$, hence $s_{Q_1}(K|\mathbf{Q}) \neq p - 1$, which implies that $s_{Q_1}(K|\mathbf{Q}) \geq p$. Putting this information together, we obtain

$$1 < \frac{p}{p-1} \leq \frac{s_{Q_1}(K|\mathbf{Q})}{p-1} \leq \frac{2p-1}{p-1} = 2 + \frac{1}{p-1} < 3,$$

because $p \neq 2$. Therefore $\frac{s_{Q_1}(K|\mathbf{Q})}{p-1} = 2$, as required. □

Having developed some preliminary results, we will now turn to the proof of the theorem. We will proceed by steps.

16.2 Step 1: $[L : \mathbf{Q}]$ and disc(O_L) are both powers of the same odd prime.

Let $L/\mathbf{Q}$ be a finite normal abelian extension such that the discriminant disc(O_L) is a power of a prime p. Then Proposition 16.1 ensures that p is totally ramified in O_L. We have also seen that

$$E(Q|p) = D(Q|p) = Gal(L/\mathbf{Q}),$$

where Q is the unique prime ideal of O_L lying over p. We now suppose that $[L : \mathbf{Q}]$ is a power of the same prime number p. Then Proposition 13.18 **b.** ensures that $E(Q|\mathbf{Z}p) = V_1(Q|\mathbf{Z}p)$. Indeed, as p is totally ramified $e(Q|p) = [L : \mathbf{Q}]$, which is a power of p; this in turn implies that $|E/V_1| = 1$ and it follows that $E(Q|\mathbf{Z}p) = V_1(Q|\mathbf{Z}p)$. We now aim to show that there is a unique field extension K of $\mathbf{Q}$ of degree p contained in L. To do this we will use Proposition 16.2.

Proposition 16.3 *Let $L/\mathbf{Q}$ be a finite normal abelian extension such that disc(O_L) and $[L:\mathbf{Q}]$ are both powers of the same odd prime p. We suppose that Q is the unique prime ideal of O_L lying over $\mathbf{Z}p$ and that $V_j(Q|\mathbf{Z}p)$, for $j \geq 0$, are the higher ramification groups. In addition, we let i be the smallest index j such that $V_j(Q|\mathbf{Z}p) \neq Gal(L/\mathbf{Q})$. Then $i \geq 2$, $[L^{V_i(Q|\mathbf{Z}p)} : \mathbf{Q}] = p$ and $L^{V_i(Q|\mathbf{Z}p)}$ is the only field extension of degree p over $\mathbf{Q}$ contained in L.*

PROOF From hereon, to simplify the notation, we will write E for $E(Q|\mathbf{Z}p)$ and V_j for $V_j(Q|\mathbf{Z}p)$.
By definition $V_0 = E$, and in the preamble to the proposition we have seen that $E = Gal(L/\mathbf{Q})$, which implies that $i \geq 1$. However, we have also seen that $V_1 = Gal(L/\mathbf{Q})$, hence $i \geq 2$. Now we establish that $[L^{V_i} : \mathbf{Q}] = p$. Since $V_{i-1} = Gal(L/\mathbf{Q})$, we have

$$[L^{V_i} : \mathbf{Q}] = |Gal(L/\mathbf{Q})/V_i)| = |V_{i-1}/V_i|.$$

From Theorem 13.18, V_{i-1}/V_i is isomorphic to a subgroup of the additive group of S/Q, because $i \geq 2$. As p is totally ramified in O_L, we have

$$1 = f(Q|\mathbf{Z}p) = [S/Q : \mathbf{Z}/\mathbf{Z}p],$$

which implies that S/Q is isomorphic to $\mathbf{F}_p$. It follows that $|V_{i-1}/V_i| = p$, because $V_{i-1} \neq V_i$.

Now let K be a number field contained in L whose degree over $\mathbf{Q}$ is p. We aim to show that $K = L^{V_i}$. We set $R^1 = O_K$ and $Q_1 = R^1 \cap Q$. Then Q_1 is totally ramified in $S = O_L$. There is a unique ideal in S lying over Q_1, namely Q, and

$$1 = f(Q|\mathbf{Z}p) = f(Q|Q_1)f(Q_1|\mathbf{Z}p) \Longrightarrow f(Q|Q_1) = 1.$$

By definition (Section 15.3), we have

$$\Delta_{Q_1}(L|K) = \Delta((R^1 \setminus Q_1)^{-1}S|R^1_{Q_1}).$$

Using Proposition 15.8 we obtain

$$\Delta_{Q_1}(L|K) = \Delta(S_Q|R^1_{Q_1}).$$

To simplify the notation we will write $\Delta_Q(L|K)$ for $\Delta_{Q_1}(L|K)$.

Next we set $R^2 = O_{L^{V_1}}$ and $Q_2 = R^2 \cap Q$. Then Q_2 is totally ramified in $S = O_L$: There is a unique ideal in S lying over Q_2, namely Q, and

$$1 = f(Q|\mathbf{Z}p) = f(Q|Q_2)f(Q_2|\mathbf{Z}p) \Longrightarrow f(Q|Q_2) = 1.$$

By definition (Section 15.3), we have

$$\Delta_{Q_2}(L|L^{V_i}) = \Delta((R^2 \setminus Q_2)^{-1}S|R^1_{Q_1})$$

and, using Proposition 15.8 again, we obtain

$$\Delta_{Q_1}(L|L^{V_i}) = \Delta(S_Q|R^2_{Q_2}).$$

We simplify the notation by writing $\Delta_Q(L|L^{V_i})$ for $\Delta_{Q_2}(L|L^{V_i})$.

From Theorem 15.1 we have

$$\Delta_Q(L|\mathbf{Q}) = \Delta_Q(L|K)S_Q\Delta_{Q_1}(K|\mathbf{Q}) \tag{16.1}$$

and

$$\Delta_Q(L|\mathbf{Q}) = \Delta_Q(L|L^{V_i})S_Q\Delta_{Q_2}(L^{V_i}|\mathbf{Q}). \tag{16.2}$$

To clarify these equalities, we recall the definitions of the ideals appearing in the equalities:

$$\Delta_Q(L|\mathbf{Q}) = \Delta(S_Q|\mathbf{Z}_{\mathbf{Z}p}),$$

$$\Delta_Q(L|K) = \Delta(S_Q|R^1_{Q_1}) \qquad \Delta_Q(L|L^{V_i}) = \Delta(S_Q|R^2_{Q_2})$$

and

$$\Delta_{Q_1}(K|\mathbf{Q}) = \Delta(R^1_{Q_1}|\mathbf{Z}_{\mathbf{Z}p}) \qquad \Delta_{Q_2}(L^{V_i}|\mathbf{Q}) = \Delta(R^2_{Q_2}|\mathbf{Z}_{\mathbf{Z}p}).$$

We now consider $\Delta_{Q_1}(K|\mathbf{Q})$ and $\Delta_{Q_2}(L^{V_i}|\mathbf{Q})$ more closely. From Proposition 16.2 we have

$$\Delta_{Q_1}(K|\mathbf{Q}) = R^1_{Q_1}Q_1^{2(p-1)}$$

and

$$\Delta_{Q_2}(L^{V_i}|\mathbf{Q}) = R^2_{Q_2}Q_1^{2(p-1)}.$$

As $R^1_{Q_1}$ is embedded in S_Q, we have

$$S_Q\Delta_{Q_1}(K|\mathbf{Q}) = S_QQ_1^{2(p-1)}.$$

Now Q_1 is totally ramified in S, so $SQ_1 = Q^{[L:K]}$ and we have

$$S_QSQ_1 = S_QQ^{[L:K]} \Longrightarrow S_QQ_1 = S_QQ^{[L:K]} \Longrightarrow S_Q\Delta_{Q_1}(K|\mathbf{Q}) = S_QQ^{[L:K]2(p-1)}.$$

In the same way

$$S_Q\Delta_{Q_2}(L^{V_i}|\mathbf{Q}) = S_QQ^{[L:L^{V_i}]2(p-1)}.$$

As $[L:K] = [L:L^{V_i}]$, we have

$$S_Q\Delta_{Q_1}(K|\mathbf{Q}) = S_Q\Delta_{Q_2}(L^{V_i}|\mathbf{Q})$$

and from equations (16.1) and (16.2) we derive

$$\Delta_Q(L|K) = \Delta_Q(L|L^{V_i}).$$

We now show that this equality ensures that $K = L^{V_i}$. First we notice that

$$\Delta_Q(L|K) = (S_QQ)^{s_Q(L|K)} \quad \text{and} \quad \Delta_Q(L|L^{V_i}) = (S_QQ)^{s_Q(L|L^{V_i})},$$

which implies that

$$s_Q(L|K) = s_Q(L|L^{V_i}).$$

From Theorem 15.6

$$s_Q(L|K) = \sum_{j=0}^{r_1-1}\left(|V_j(Q|Q_1)| - 1\right),$$

where $V_j(Q|Q_1)$, for $j = 0, 1, \ldots, r_1 - 1$, are the ramification groups of Q in the extension L/K. (Indeed, L/K is a Galois extension and Q_1 is totally ramified in S.) The same theorem ensures that

$$s_Q(L|L^{V_i}) = \sum_{j=0}^{r_2-1}\left(|V_j(Q|Q_2)| - 1\right),$$

where $V_j(Q|Q_2)$, for $j = 0, 1, \ldots, r_2 - 1$, are the ramification groups of Q in the extension L/L^{V_i}. (Indeed, L/L^{V_i} is a Galois extension and Q_2 is totally ramified in S.) We can take $r = \max(r_1, r_2)$ in both cases.

Now we consider orders of the ramification groups. We notice that

$$V_j(Q|Q_1) = V_j \cap H,$$

where $H = Gal(L/K)$ and

$$V_j(Q|Q_2) = V_j \cap V_i,$$

since $V_i = Gal(L|L^{V_i})$. Therefore, for $j = 0, 1, \ldots, i - 1$, we have

$$V_j(Q|Q_1) = H \qquad \text{and} \qquad V_j(Q|Q_2) = V_i.$$

Then

$$|H| = |Gal(L/K)| = [L : K] = \frac{[L : \mathbf{Q}]}{[K : \mathbf{Q}]} = \frac{[L : \mathbf{Q}]}{p}$$

and

$$p = [L^{V_i} : \mathbf{Q}] = |Gal(L/\mathbf{Q})/V_i| \Longrightarrow |V_i| = \frac{[L : \mathbf{Q}]}{p},$$

therefore $|H| = |V_i|$, i.e., $|V_j(Q|Q_1)| = |V_j(Q|Q_2)|$. If $j \geq i$, then $V_j(Q|Q_2) = V_j$, because $V_j \subset V_i$ and it follows that $|V_j(Q|Q_1)| \leq |V_j(Q|Q_2)|$. As

$$\sum_{j=0}^{r-1} (|V_j(Q|Q_1)| - 1) = \sum_{j=0}^{r-1} (|V_j(Q|Q_2)| - 1),$$

we must have

$$|V_i(Q|Q_1) = |V_i(Q|Q_2) \Longrightarrow V_i \cap H = V_i \Longrightarrow V_i \subset H.$$

However, this implies that $K = L^H \subset L^{V_i}$. As K and L^{V_i} are subspaces of L of the same dimension, they must be equal, as required. □

Our next step is to show that under the conditions we have assumed at the beginning of the section, i.e., p is an odd prime, L an abelian finite normal extension of $\mathbf{Q}$ of degree p^m and $\mathrm{disc}(O_L) = p^k$, where $m, k \in \mathbf{N}^*$, then L is a cyclic extension of $\mathbf{Q}$. We will use an elementary result from group theory, namely, an abelian group of order p^m, where p is a prime, with a unique subgroup of order p^{m-1}, is cyclic. We need a preliminary result.

Lemma 16.1 *Let G be an abelian group of order p^m, where p is a prime and $m \geq 1$. If G has a subgroup H of order p^k and $k < l \leq m$, then there is a subgroup K of G containing H and having order p^l.*

PROOF Suppose first that $l = k + 1 \leq m$ and let $\bar{G} = G/H$. Then $|\bar{G}| = p^{m-k}$ and so, by Cauchy's theorem, there exists an element $\bar{x} \in G/H$ of order p. Let K be the subgroup of G generated by H and x. Since $x \notin H$, the group H is properly contained in K. Also,

$$K = H \cup Hx \cup \cdots \cup Hx^{p-1} \Longrightarrow |K| = p^{k+1}.$$

Repeating the argument if necessary, we finally obtain the desired subgroup. □
where p is an odd prime and $m, k \in \mathbf{N}^*$

We may now prove the result concerning the cyclicity of G.

Proposition 16.4 *If G is an abelian group of order p^m, where p is a prime, with a unique subgroup H of order p^{m-1}, then G is cyclic.*

PROOF Let $x \in G \setminus H$. If x has order less than p^m, then, from Lemma 16.1, the cyclic group $\langle x \rangle$ is contained in a subgroup K of G of order p^{m-1}. By hypothesis, K must be equal to H, so $x \in H$, a contradiction. Hence x has order p^m and so G is cyclic. □

We may now show that, under the conditions given above, the extension $L/\mathbf{Q}$ is cyclic.

Theorem 16.1 *Let p be an odd prime, L a finite normal abelian extension of $\mathbf{Q}$ of degree p^m, where $m \in \mathbf{N}^*$, and $disc(O_L)$ a power of p. Then the extension $L/\mathbf{Q}$ is cyclic.*

PROOF By hypothesis the Galois group $G = Gal(L/\mathbf{Q})$ is abelian of order p^m. From Proposition 16.3 we know that G has a unique subgroup of order p^{m-1}. Applying Proposition 16.4 we find that G is cyclic. □

We are now in a position to prove the Kronecker-Weber theorem in a particular case. Further on we will extend the theorem to the general case.

Theorem 16.2 *If L is a finite normal abelian extension of $\mathbf{Q}$ of degree p^m, where p is an odd prime and $m \in \mathbf{N}^*$, and $disc(O_L)$ is a power of p, then there exists a root of unity ζ such that $L \subset \mathbf{Q}(\zeta)$.*

PROOF Let $K = \mathbf{Q}(\zeta)$, where ζ is a primitive $p^{m+1}th$ root of unity. The extension $K/\mathbf{Q}$ is a Galois extension and, writing $G = Gal(K/\mathbf{Q})$, from Theorem 7.7 we have

$$|G| = [K : \mathbf{Q}] = \deg \Phi_{p^{m+1}} = \phi(p^{m+1}) = p^m(p-1).$$

Also, by Theorem 7.7, G is isomorphic to $\mathbf{Z}_{p^{m+1}}^{\times}$, which is cyclic, because the group of units of $\mathbf{Z}_n$ is cyclic, when n is a power of an odd prime (see, for example, [4]).

The cyclic group G has a subgroup H of order $p-1$. (If σ is a generator of G, then σ^{p^m} has order $p-1$.) We set $K' = K^H$; then $[K' : \mathbf{Q}] = p^m$. Since H is a subgroup of G, H is cyclic, and so, by definition, K' is a cyclic extension of $\mathbf{Q}$. We claim that the discriminant $\mathrm{disc}(O_{K'})$ is a power of p. To see this, notice that a prime q dividing $\mathrm{disc}(O_{K'})$ is ramified in $O_{K'}$, hence also ramified in O_K, thus q divides $\mathrm{disc}(O_K)$, which is a power of p. It follows that $q = p$. This proves the claim.

Now we consider the composition field LK'. As L is a finite Galois extension of $\mathbf{Q}$, so is LK' (Theorem 6.8). Both L and K' are normal extensions of $\mathbf{Q}$, therefore, from Theorem 6.10, the Galois group $Gal(LK'/\mathbf{Q})$ is isomorphic to a subgroup of the product $Gal(L/\mathbf{Q}) \times Gal(K'/\mathbf{Q})$, which is abelian. Hence $Gal(LK'/\mathbf{Q})$ is abelian.

Now, from the proof of Corollary 6.1, we know that the Galois groups $Gal(LK'/K')$ and $Gal(L/L \cap K')$ are isomorphic, hence

$$[LK' : \mathbf{Q}] = [LK' : K'][K' : \mathbf{Q}] = [L : L \cap K'][K' : \mathbf{Q}],$$

which is a power of p, because $[L : L \cap K']$ divides $[L : \mathbf{Q}]$ and $[L : \mathbf{Q}] = p^m$. We claim that the discriminant $\mathrm{disc}(O_{LK'})$ is also a power of p. If q is a prime and $q|\mathrm{disc}(O_{LK'})$, then q is ramified in $O_{LK'}$. From Theorem 13.12, q is ramified in L or in K'. This means that $q|\mathrm{disc}(O_L)$ or $q|\mathrm{disc}(O_{K'})$. In both cases we obtain $q = p$, so $\mathrm{disc}(O_{LK'})$ is a power of p, as claimed.

We now apply Theorem 16.1 to LK': the Galois group $Gal(LK'/\mathbf{Q})$ is cyclic. Both L and K' are normal extensions of $L \cap K'$. With $L \cap K' = F$ in Theorem 6.10, we obtain

$$Gal(LK'/L \cap K') \simeq Gal(L/L \cap K') \times Gal(K'/L \cap K').$$

We notice that both $Gal(L/L \cap K')$ and $Gal(K'/L \cap K')$ have orders a power of p and are cyclic, because $Gal(L/L \cap K')$ is a subgroup of $Gal(L/\mathbf{Q})$ and $Gal(K'/L \cap K')$ a subgroup of $Gal(K'/\mathbf{Q})$.

We have seen that $Gal(LK'/\mathbf{Q})$ is abelian, thus $Gal(LK'/L \cap K'))$ is also abelian. The previous isomorphism gives us a primary decomposition of this finite abelian group. Moreover, $Gal(LK'/L \cap K')$ is a cyclic p-group, since $Gal(LK'/\mathbf{Q})$ is a cyclic p-group. Thus $Gal(LK'/L \cap K')$ is its own primary decomposition. The uniqueness of the primary decomposition ensures that $Gal(L/L \cap K')$ or $Gal(K'/L \cap K')$ is trivial. In the first case,

$$L = L \cap K' \Longrightarrow L \subset K'.$$

In the second case

$$K' = L \cap K' \Longrightarrow K' \subset L$$

hence

$$[L : \mathbf{Q}] = [L : K'][K' : \mathbf{Q}] \Longrightarrow [L : K'] = 1,$$

because $[L : \mathbf{Q}] = p^m = [K' : \mathbf{Q}]$. Therefore $L = K'$. In both cases we have found a cyclotomic extension containing L. This finishes the proof. $\square$

16.3 Step 2: $[L : \mathbf{Q}]$ and $\mathrm{disc}(O_L)$ are both powers of 2.

Up to here we have considered the case where the order of the Galois group $Gal(L/\mathbf{Q})$ is the power of an odd prime p and the discriminant $\mathrm{disc}(O_L)$ a power of the same prime. It should be clear that certain arguments we have used will not work if the prime p is 2. In this section we aim to look at this case. We will first consider real fields, i.e., subfields of the field of real numbers $\mathbf{R}$. To begin we establish a preliminary result analogous to Theorem 16.1.

Proposition 16.5 *Let L be a real field which is a finite normal abelian extension of $\mathbf{Q}$ of degree a power of 2 such that the discriminant $disc(O_L)$ is also a power of 2. Then the extension $L/\mathbf{Q}$ is cyclic.*

PROOF Let $[L : \mathbf{Q}] = 2^m$, with $m \in \mathbf{N}^*$. We first consider the case where $m = 1$, i.e., $[L : \mathbf{Q}] = 2$. Then $L = \mathbf{Q}(\sqrt{d})$, where d is a square-free integer. In this case $\mathrm{disc}(O_L) = d$, if $d \equiv 1 \pmod 4$, and $\mathrm{disc}(O_L) = 4d$, if $d \equiv 2, 3 \pmod 4$. As $\mathrm{disc}(O_L)$ is a power of 2, the only possibility is $d = 2$ and so $L = \mathbf{Q}(\sqrt{2})$ (and $\mathrm{disc}(O_L) = 8$). Thus the extension $L/\mathbf{Q}$ is cyclic.

Now suppose that $m \geq 2$. From Lemma 16.1 we know that the Galois group $Gal(L/\mathbf{Q})$ contains a subgroup H whose order is 2^{m-1}. For any such subgroup H, from Theorem 6.6,

$$[L^H : \mathbf{Q}] = |\frac{Gal(L/\mathbf{Q})}{H}| = 2.$$

Moreover, $\mathrm{disc}(O_L)$ is a power of 2, since any prime q dividing $\mathrm{disc}(O_{L^H})$ ramifies in O_{L^H} and so ramifies in O_L. As 2 is the only prime ramifying in O_L, $q = 2$. Thus $\mathrm{disc}(O_{L^H})$ is a power of 2 up to sign. As $[L^H : \mathbf{Q}] = 2$, $L^H = \mathbf{Q}(\sqrt{d})$, where d is a square-free integer, and $\mathrm{disc}(O_{L^H}) = d$ or $\mathrm{disc}(O_{L^H}) = 4d$. It follows that $d = \pm 2$. Since $L^H \subset L$, $d = 2$ and so $L^H = \mathbf{Q}(\sqrt{2})$ and $H = Gal(L/\mathbf{Q}(\sqrt{2}))$. We conclude that the Galois group $Gal(L/\mathbf{Q})$ has a unique subgroup of order 2^{m-1}. Applying Proposition 16.4 we obtain that $Gal(L/\mathbf{Q})$ is cyclic. $\square$

We now establish another result concerning real extensions.

Proposition 16.6 *If $m \in \mathbf{N}^*$ and ζ a primitive root of order 2^{m+2}, then $L = \mathbf{Q}(\zeta) \cap \mathbf{R}$ is the unique real finite normal abelian extension K of $\mathbf{Q}$ such that $[K : \mathbf{Q}] = 2^m$ and disc(O_K) is a power of 2. In addition, $L \subset \mathbf{Q}(\zeta)$.*

PROOF We will begin by showing that L satisfies the conditions. L is clearly a real field and $L \subset \mathbf{Q}(\zeta)$. Any prime q dividing the discriminant $\mathrm{disc}(O_L)$ ramifies in O_L, hence in $\mathbf{Q}(\zeta)$. This implies that q divides $\mathrm{disc}(O_{\mathbf{Q}(\zeta)})$, which is a power of 2, by Theorem 11.15. Thus $q = 2$ and It follows that $\mathrm{disc}(O_L)$ is a power of 2.

Now

$$[\mathbf{Q}(\zeta) : \mathbf{Q}] = \deg \Phi_{2^{m+2}} = \phi(2^{m+2}) = 2^{m+1},$$

where ϕ is Euler's totient function. From the primitive element theorem (Theorem 3.4), there exists $\alpha \in \mathbf{Q}(\zeta)$ such that $\mathbf{Q}(\zeta) = L(\alpha)$. If $\alpha = a + bi$, then α is a root of the polynomial $f(X) = (a^2 + b^2) - 2aX + X^2$. Moreover, $\bar{\alpha} = a - bi \in \mathbf{Q}(\zeta)$, because $\bar{\alpha}$ is a root of the minimal polynomial $m(\alpha, \mathbf{Q})$ and $\mathbf{Q}(\zeta)$ is a normal extension of $\mathbf{Q}$. Hence

$$a = \frac{\alpha + \bar{\alpha}}{2} \in L \quad \text{and} \quad b = \frac{\alpha - \bar{\alpha}}{2i} \in L,$$

since $i = \zeta_4 = \zeta^{2^m} \in \mathbf{Q}(\zeta)$. It follows that $f \in L[X]$ and $\deg m(\alpha, L)$ is 1 or 2. As $\alpha \notin L$, we have $\deg m(\alpha, L) = 2$ and so $[\mathbf{Q}(\zeta) : L] = 2$. As

$$[\mathbf{Q}(\zeta) : \mathbf{Q}] = [\mathbf{Q}(\zeta) : L][L : \mathbf{Q}],$$

we have $[L : \mathbf{Q}] = 2^m$, as required.

It remains to show that L is unique. Let F and K be two fields satisfying the conditions in the statement of the proposition. We aim to show that $F = K$. Both F and K satisfy the assumptions of Proposition 16.5, so the compositum FK also satisfies the assumptions. Indeed, the extensions $F/\mathbf{Q}$ and $K/\mathbf{Q}$ are both normal, so $FK/\mathbf{Q}$ is normal and the Galois group $Gal(FK/\mathbf{Q})$ is isomorphic to a subgroup of the product $Gal(F/\mathbf{Q}) \times Gal(K/\mathbf{Q})$, by Theorem 6.10. Therefore $Gal(FK/\mathbf{Q})$ is abelian of order a power of 2. If a prime q divides the discriminant $\mathrm{disc}(O_{FK})$, then it is ramified in O_{FK} and hence ramified in O_F or in O_K (Theorem 13.12). Thus q divides $\mathrm{disc}(O_F)$ or $\mathrm{disc}(O_K)$, which are both powers of 2. Hence $q = 2$ and it follows that $\mathrm{disc}(O_{FK})$ is a power of 2.

Now, from Theorem 6.10,

$$Gal(FK/F \cap K) \simeq Gal(F/F \cap K) \times Gal(K/F \cap K).$$

As $Gal(FK/F \cap K)$ is a subgroup of the abelian group $Gal(FK/\mathbf{Q})$, $Gal(FK/F \cap K)$ is abelian. Both $Gal(F/F \cap K)$ and $Gal(K/F \cap K)$ are cyclic and of order a power of 2, being respectively subgroups of $Gal(F/\mathbf{Q})$ and $Gal(K/\mathbf{Q})$, which are cyclic by Proposition 16.5. Thus the previous isomorphism is a primary decomposition of the finite abelian group $Gal(FK/F \cap K)$. However, $Gal(FK/F \cap K)$ is cyclic of order a power of 2, being a subgroup of $Gal(FK/\mathbf{Q})$, which is cyclic by Proposition 16.5. The uniqueness of the primary decomposition of a finite abelian group ensures that $Gal(F/F \cap K)$ or $Gal(K/F \cap K)$ is trivial. Therefore $F = F \cap K$ or $K = F \cap K$, which implies in the first case that $F \subset K$ and in the second that $K \subset F$. As $[F : \mathbf{Q}] = [K : \mathbf{Q}]$, we must have $F = K$. □

We have shown in the previous section that when the extension $L/\mathbf{Q}$ is abelian of degree a power of p, with p an odd prime, and $\mathrm{disc}(O_L)$ a power of p, then there exists a root of unity ζ such that $L \subset \mathbf{Q}(\zeta)$.We will now establish an an analogous result for the prime 2.

Theorem 16.3 *Let $L/\mathbf{Q}$ be a finite normal abelian of degree a power of 2, with disc(O_L) a power of 2. Then there exists a root of unity ζ such that $L \subset \mathbf{Q}(\zeta)$.*

PROOF In Proposition 16.6 we have already proved the theorem in the case where L is a real field. Our aim is now to generalize this to any field contained in $\mathbf{C}$.

Let $K = L(i) \cap \mathbf{R}$. Then K is a real extension of $\mathbf{Q}$. As $L(i) = \mathbf{Q}(i)L$ and both $\mathbf{Q}(i)/\mathbf{Q}$ and $L/\mathbf{Q}$ are finite normal abelian extensions, $L(i)/\mathbf{Q}$ is also a finite normal abelian extension (Theorem 6.10). Since K is a subfield of $L(i)$, K is a finite normal abelian extension of $\mathbf{Q}$.

Next we notice that $[K : \mathbf{Q}]$ is a power of 2. Indeed,

$$[L(i) : \mathbf{Q}] = [L(i) : L][L : \mathbf{Q}].$$

As $m(i, L)$ divides $f(X) = 1 + X^2$, the degree of $m(i, L)$ is 1 or 2 and so $[L(i) : L]$ is equal to 1 or 2. By hypothesis $[L : \mathbf{Q}]$ is a power of 2, so $[L(i) : \mathbf{Q}]$ is a power of 2. However, $[K : \mathbf{Q}]$ divides $[L(i) : \mathbf{Q}]$, hence $[K : \mathbf{Q}]$ is a power of 2.

Our next step is to show that the discriminant disc(O_K) is also a power of 2. If q is a prime number dividing disc$(O_{L(i)})$, the q ramifies in $L(i) = \mathbf{Q}(i)L$, which implies that q ramifies in $\mathbf{Q}(i)$ or in L (Theorem 13.12), i.e., q divides disc$(O_{\mathbf{Q}(i)})$ or q divides disc(O_L). Now, by hypothesis disc(O_L) is a power of 2, and disc$(O_{\mathbf{Q}(i)}) = -4$, because $-1 \equiv 3 \pmod 4$ implies that disc$(O_{\mathbf{Q}(i)}) = 4(-1) = -4$. It follows that $q = 2$ and so disc$(O_{L(i)})$ is a power of 2. As K is a subfield of $L(i)$, disc(O_K) is also a power of 2. Indeed, if q is a prime dividing disc(O_K), then q ramifies in O_K and hence in $O_{L(i)}$; thus q divides disc$(O_{L(i)})$ and so $q = 2$.

We now apply Proposition 16.6: there exists a root of unity ζ such that $K \subset \mathbf{Q}(\zeta)$. From the primitive element theorem (Theorem 3.4), there exists $\alpha \in L(i)$ such that $L(i) = K(\alpha)$. Let $\alpha = a + ib$. As $\bar{\alpha} = a - ib$ is a root of the minimal polynomial $m(\alpha, K)$ and $L(i)$ is a normal extension of K, $a = \frac{\alpha+\bar{\alpha}}{2} \in K$ and $b = \frac{\alpha-\bar{\alpha}}{2i} \in K$. Also, $i = \zeta_4$, so $\alpha = a + ib \in \mathbf{Q}(\zeta_4)\mathbf{Q}(\zeta)$. Then

$$L \subset L(i) = K(\alpha) \subset \mathbf{Q}(\zeta_4)\mathbf{Q}(\zeta) = \mathbf{Q}(\xi),$$

where ξ is a root of unity, by Exercise 7.3. □

Exercise 16.1 *With K and L as defined in Theorem 16.3, show that $L(i) = K(i)$.*

16.4 Step 3: $[L : \mathbf{Q}]$ is a power of a prime p.

We have shown that a normal abelian extension L of the rationals of degree a power of a prime p such that the discriminant disc(O_L) is also a power of p can be considered as a subfield of a cyclotomic extension of the rationals. In this section we aim to show that we may dispense with the condition on the discriminant. We will begin with a preliminary result.

Proposition 16.7 *Suppose that $L/\mathbf{Q}$ is a normal abelian extension of degree n and q a prime dividing disc(O_L) but not dividing n. Then there exists a normal abelian extension $L'/\mathbf{Q}$ and a primitive qth root of unity ζ such that*

- $[L' : \mathbf{Q}]$ *divides n;*
- $L \subset L'(\zeta)$*;*
- *q does not divide disc$(O_{L'})$;*
- *any prime q' dividing disc$(O_{L'})$ also divides disc(O_L).*

PROOF We consider two cases, namely when L contains a primitive qth root of unity and then when this is not the case.

Case 1: L contains a primitive qth root of unity ζ.

Suppose that Q is a prime ideal in O_L lying above q: $Q \cap \mathbf{Z} = \mathbf{Z}q$. To simplify the notation we write e for the ramification index $e(Q|q)$, V_1 for the corresponding ramification group $V_1(Q|\mathbf{Z}q)$ and E for the corresponding inertia group $E(Q|\mathbf{Z}q)$.

The assumption that q does not divide $[L : \mathbf{Q}]$ ensures that $L = L^{V_1}$. Indeed, from Proposition 13.18 we know that V_1 is a q-group, i.e., the order of V_1 is a power of q, thus Theorem 6.7 ensures that $[L : L^{V_1}]$ is a power of q. Moreover, $[L : L^{V_1}]$ divides $[L : \mathbf{Q}]$. Since q does not divide $[L : \mathbf{Q}]$ we must have $[L : L^{V_1}] = 1$, i.e., $L = L^{V_1}$.

Now we consider L^E. As $L/\mathbf{Q}$ is normal, by Proposition 13.11 we have $[L : L^E] = e$. Now, from Theorem 6.7 we obtain $Gal(L/L^E) = E$ and so

$$e = [L^{V_1} : L^E] = |E/V_1|, \tag{16.3}$$

by Theorem 6.6. Since $Gal(L/\mathbf{Q})$ is abelian, the decomposition group $D(\mathbf{Q}|\mathbf{Z}q)$, being a subgroup of $Gal(L/\mathbf{Q})$, is also abelian. Given that $L/\mathbf{Q}$ is normal, Corollary 13.9 ensure that $|E/V_1|$ divides $q' - 1$, where

$$q' = |O_{\mathbf{Q}}/\mathbf{Z}q| = |\mathbf{Z}/\mathbf{Z}q| = q. \tag{16.4}$$

We now set $L' = L^E$. As E is a subgroup of $Gal(L/\mathbf{Q})$, $[L' : \mathbf{Q}]$ divides n. Also, $L'/\mathbf{Q}$ is a normal abelian extension, because $L' = L^E$ and E is a normal subgroup of $Gal(L/\mathbf{Q})$, which is abelian.

By hypothesis there is a primitive qth root of unity ζ in L. We claim that $L = L'(\zeta)$. As $\mathbf{Q} \subset L$ and $\zeta \in L$, we have $\mathbf{Q}(\zeta) \subset L$. The prime ideal Q in O_L lies over a unique prime ideal Q' in $O_{\mathbf{Q}(\zeta)}$. To simplify the notation we write e' for the ramification index $e(Q|Q')$ and E' for the inertia group $E(Q|Q')$. We notice that $E' = E \cap Gal(L/\mathbf{Q}(\zeta))$, the intersection of two subgroups of $Gal(L/\mathbf{Q})$. Using Theorem 6.9 we have

$$\begin{aligned} L^{E'} &= L^E L^{Gal(L/\mathbf{Q}(\zeta))} \\ &= L^E \mathbf{Q}(\zeta) \\ &= L^E(\zeta) \\ &= L'(\zeta). \end{aligned}$$

To establish the claim it is sufficient to show that $L^{E'} = L$. By Proposition 5.3 $L/\mathbf{Q}(\zeta)$ is a normal extension, so we may use Proposition 13.11 to obtain $[L : L^{E'}] = e'$. Also,

$$e = e' e(\mathbf{Q}'|q). \tag{16.5}$$

From equations (16.3) and (16.4) we obtain $e|q-1$. However, we also have $q-1|e$. From Theorem 11.15, $\mathrm{disc}(O_{\mathbf{Q}(\zeta)})$ is a power of q, so q is totally ramified in $O_{\mathbf{Q}(\zeta)}$, by Proposition 16.1, which implies that $e(\mathbf{Q}'|q) = q - 1$, because $[\mathbf{Q}(\zeta) : \mathbf{Q}] = q - 1$. Therefore, by equation (16.5), $q - 1|e$. It follows that $e = q - 1$ and so $e' = 1$, which implies that $[L : L^{E'}] = 1$. We have shown that $L^{E'} = L$ and hence established the claim.

We now show that the remaining two conditions of the proposition are satisfied. First we show that q does not divide $\mathrm{disc}(O_{L'})$. Let Q_1 be a prime ideal of $O_{L'}$ lying over q and Q_2 a prime ideal in O_L lying over Q_1. Both Q_2 and Q are prime ideals in O_L lying over q. As $Gal(L/\mathbf{Q})$ is abelian, Exercise 13.4 ensures that $E(Q_2|\mathbf{Z}q) = E(Q|\mathbf{Z}q)$. Hence $L' = L^{E(Q_2|\mathbf{Z}q)}$.

The ideal Q_1 is the unique prime ideal in O_{L^E} ($=O_{L'}$) lying under Q_2, so, by Proposition 13.14, $e(Q_1|\mathbf{Z}q) = 1$, i.e., q is unramified in $O_{L'}$, which implies that q does not divide $\text{disc}(O_{L'})$.

Finally, we show that, if q' is a prime dividing $\text{disc}(O_{L'})$, then q' divides $\text{disc}(O_L)$. If q' is a prime dividing $\text{disc}(O_{L'})$, then q' ramifies in $O_{L'}$, which implies that q' ramifies in O_L, because $L' \subset O_L$; hence q' divides $\text{disc}(O_L)$. □

Case 2: L does not contain a primitive qth root of unity.

We begin by adding a primitive qth root of unity ζ to L. We may apply Case 1 to $L(\zeta)$. Indeed, $L(\zeta) = L\mathbf{Q}(\zeta)$. As both L and $\mathbf{Q}(\zeta)$ are normal extensions of $\mathbf{Q}$, by Theorem 6.8, $L\mathbf{Q}(\zeta)$ is a normal extension of $\mathbf{Q}$. In addition, by Theorem 6.10, $Gal(L\mathbf{Q}(\zeta)/\mathbf{Q})$ is a subset of $Gal(L/\mathbf{Q}) \times Gal(\mathbf{Q}(\zeta)/\mathbf{Q})$, hence abelian. By construction, $L(\zeta)$ contains a primitive qth root of unity. Moreover, q divides $\text{disc}(O_{L(\zeta)})$, because q divides $\text{disc}(O_L)$ and $O_L \subset O_{L(\zeta)}$, It remains to show that q does not divide $[L(\zeta) : \mathbf{Q}]$. As

$$[L(\zeta) : \mathbf{Q}] = [L(\zeta) : L][L : \mathbf{Q}],$$

if $q|[L(\zeta) : \mathbf{Q}]$, then either $q|[L(\zeta) : L]$ or $q|[L : \mathbf{Q}]$. By hypothesis, the second alternative is not possible. Also, by Theorem 7.4, the Galois group $Gal(L(\zeta)/L)$ is a subset of $\mathbf{Z}_q^\times$, which implies that $[L(\zeta) : L]|q-1$. As q does not divide $q-1$, the second alternative is also not possible. We have shown that q does not divide $[L(\zeta) : \mathbf{Q}]$.

As all the conditions of Case 1, with L replaced by $L(\zeta)$, are satisfied, there exists a finite normal extension L' of $\mathbf{Q}$ and a primitive qth root of unity ξ such that

- $[L' : \mathbf{Q}]$ divides $[L(\zeta) : \mathbf{Q}]$;
- $L(\zeta) \subset L'(\xi)$;
- q does not divide $\text{disc}(O_{L'})$;
- any prime q' dividing $disc(O_{L'})$ also divides $\text{disc}(O_{L(\zeta)})$.

As $L'(\zeta) = L'(\xi)$, we may suppose that $\xi = \zeta$. In the course of proving Case 1 we showed that $e = q-1$, thus by Theorem 13.11 $[L : L^E] = q-1$, i.e., $[L : L'] = q-1$. Replacing L by $L(\zeta)$ we obtain $[L(\zeta) : L'] = q-1$. In a similar way, we obtain $L' \subset L(\zeta)$.

We maintain that L' has the required properties of the proposition.

- $[L' : \mathbf{Q}]$ divides $n = [L : \mathbf{Q}]$: Using Corollary 6.1, we have
$$[L(\zeta) : \mathbf{Q}] = [L\mathbf{Q}(\zeta) : \mathbf{Q}] = \frac{[L : \mathbf{Q}][\mathbf{Q}(\zeta) : \mathbf{Q}]}{[L \cap \mathbf{Q}(\zeta) : \mathbf{Q}]} = \frac{[L : \mathbf{Q}](q-1)}{[L \cap \mathbf{Q}(\zeta) : \mathbf{Q}]}.$$
Thus
$$[L : \mathbf{Q}][(q-1) = [L \cap \mathbf{Q}(\zeta) : \mathbf{Q}][L(\zeta) : L'][L' : \mathbf{Q}],$$
which implies that
$$[L : \mathbf{Q}] = [L \cap \mathbf{Q}(\zeta) : \mathbf{Q}][L' : \mathbf{Q}],$$
because $[L(\zeta) : L'] = q-1$. Hence $[L' : \mathbf{Q}]$ divides $[L : \mathbf{Q}]$.
- $L \subset L'(\zeta)$, since $L \subset L(\zeta) \subset L'(\zeta)$.
- q does not divide $\text{disc}(O_{L'})$: Here there is nothing to prove.

- Any prime q' dividing $\mathrm{disc}(O_{L'})$ also divides $\mathrm{disc}(O_L)$: As $L' \subset L(\zeta)$, $q'|\mathrm{disc}(O_{L'}) \implies q'|\mathrm{disc}(O_{L(\zeta)})$, which implies that q' ramifies in $O_{L(\zeta)}$. However, $L(\zeta) = L\mathbf{Q}(\zeta)$, so q' ramifies in O_L or in $O_{\mathbf{Q}(\zeta)}$ (Theorem 13.12). As q does not divide $\mathrm{disc}(O_{L'})$, $q' \neq q$, so q' does not ramify in $O_{\mathbf{Q}(\zeta)}$, so q' must ramify in O_L, which implies that q' divides $\mathrm{disc}(O_L)$.

This finishes the proof. □

We are now in a position to dispense with the condition on the discriminant in Theorems 16.2 and 16.3.

Theorem 16.4 *If $L/\mathbf{Q}$ is a normal abelian extension of degree p^m, for some prime p, then there exists a root of unity ζ such that $L \subset \mathbf{Q}(\zeta)$.*

PROOF If the discriminant $\mathrm{disc}(O_L)$ is also a power of p, then there is nothing to prove, so let us suppose that this is not the case. Then there is a prime $q \neq p$ dividing the discriminant. From Proposition 16.7 there is an abelian extension $L_1/\mathbf{Q}$ and a qth root of unity ζ_1 such that

- $[L_1 : \mathbf{Q}]$ divides p^m and so is a power of p;
- $L \subset L_1(\zeta_1)$;
- q does not divide $\mathrm{disc}(O_{L_1})$;
- any prime q' dividing $\mathrm{disc}(O_{L_1})$ also divides $\mathrm{disc}(O_L)$.

Thus $\mathrm{disc}(O_{L_1})$ has fewer prime factors than $\mathrm{disc}(O_L)$. We can repeat the process and so find a normal abelian extension $L_2/\mathbf{Q}$ and a root of unity ζ_2 such that $L_1 \subset L_2(\zeta_2)$, $[L_2 : \mathbf{Q}]$ is a power of p and $\mathrm{disc}(O_{L_2})$ has fewer prime factors than $\mathrm{disc}(O_{L_1})$. Continuing in the same way, we finally obtain a normal abelian extension $L_r/\mathbf{Q}$ and a root of unity ζ_r such that $L_{r-1} \subset L_r(\zeta_r)$, $[L_r : \mathbf{Q}]$ is a power of p and $\mathrm{disc}(O_{L_r})$ is also a power of p, possibly 1, in which case $L_r = \mathbf{Q}$ (Theorem 14.5). It follows from Theorems 16.2 and 16.3 that there is a root of unity ζ_{r+1} such that $L_r \subset \mathbf{Q}(\zeta_{r+1})$. To sum up, we have the inclusions

$$L \subset L_1(\zeta_1), L_1 \subset L_2(\zeta_2), \ldots, L_{r-1} \subset L_r(\zeta_r), L_r \subset \mathbf{Q}(\zeta_{r+1}),$$

which implies that

$$L \subset \mathbf{Q}(\zeta_1, \zeta_2, \ldots, \zeta_{r+1}) \subset \mathbf{Q}(\zeta),$$

where ζ is a root of unity (Exercise 7.3). This ends the proof. □

16.5 Step 4: The general case

We are now in a position to prove the general case of the Kronecker-Weber theorem.

Theorem 16.5 *If $L/\mathbf{Q}$ is a finite normal abelian extension, then there is a primitive root of unity ζ such that $L \subset \mathbf{Q}(\zeta)$.*

PROOF As $Gal(L/\mathbf{Q})$ is abelian, there exist prime numbers $p_1, \ldots, p_s$ and p_i-subgroups $H_1, \ldots, H_s$ such that

$$Gal(L/\mathbf{Q}) \simeq H_1 \times \cdots \times H_s.$$

If $|H_i| = p_i^{\alpha_i}$, then $|Gal(L/\mathbf{Q}| = \prod_{i=1}^s p_i^{\alpha_i}$. Let $\hat{H}_j = \prod_{i \neq j} H_i$ and $L_j = L^{\hat{H}_j}$. Then $[L_j : \mathbf{Q}] = p_j^{\alpha_j}$. Moreover, since $L/\mathbf{Q}$ is assumed normal, Theorem 6.9 ensures that

$$L^{\cap_{i=1}^s \hat{H}_i} = \prod_{i=1}^s L^{\hat{H}_i} = \prod_{i=1}^s L_i.$$

Since $\cap_{i=1}^s \hat{H}_i = \{e\}$, we obtain $\prod_{i=1}^s L_i = L$. Also, each subgroup $\hat{H}_i$ is normal in $Gal(L/\mathbf{Q})$, so, by Theorem 6.6, $L_i/\mathbf{Q}$ is normal and $Gal(L_i/\mathbf{Q}) \simeq Gal(L/\mathbf{Q})/\hat{H}_i$. Therefore $L_i/\mathbf{Q}$ is a finite normal abelian extension, with degree a power of a prime, and so there exists a root of unity ζ_i such that $L_i \subset \mathbf{Q}(\zeta_i)$. Thus

$$L = L_1 \cdots L_s \subset \mathbf{Q}(\zeta_1) \cdots \mathbf{Q}(\zeta_s) \subset \mathbf{Q}(\zeta),$$

where ζ is a primitive root of unity (Exercise 7.3), i.e., L is included in a cyclotomic extension of $\mathbf{Q}$. $\square$

The Kronecker-Weber theorem answers an important question. Earlier we saw that a cyclotomic extension of the rationals is normal and abelian; it follows that any subextension of a cyclotomic extension of the rationals is also normal and abelian. It is natural to ask whether there are other finite normal abelian extensions of the rationals. The Kronecker-Weber theorem gives a negative response to this question.

Chapter 17

Factoring primes in extensions

In a unique factorization domain R any element x which is neither the identity for the addition nor a unit can be expressed as product of prime factors and a unit : $x = up_1^{\alpha_1} \cdots p_n^{\alpha_n}$, where u is a unit and $p_1, \dots, p_n$ are prime factors, which are not associated. There may be different such factorizations, but the number n is always the same, as are the powers $\alpha_1, \dots, \alpha_n$. If we take the powers of the primes in increasing order, then we obtain a finite sequence of positive integers, which we call the form of the decomposition. For example, $12 = 3.2^2$, so the form of the decomposition of 12 is $(1, 2)$. Similarly, $30 = 2.3.5$ has the form $(1, 1, 1)$, $36 = 2^2.3^2$ the form $(2, 2)$ and $20 = 5.2^2$ the form $(1, 2)$. We should notice that the factorizations of 12 and 20 have the same form $(1, 2)$; thus different elements may have factorizations with the same form.

If K is a number field and O_K its number ring, then any nonzero ideal of O_K not equal to O_K has a unique factorization into prime ideals, because O_K is a Dedekind domain. For a prime number p we will be concerned in this chapter with the form of the factorization of the ideal $O_K p$.

17.1 Preliminary results

Proposition 17.1 *Let K be a number field of degree n over $\mathbf{Q}$ and R an order of O_K. Then*

$$|disc(R)| = [O_K : R]^2 |disc(O_K)|,$$

where $[O_K : R]$ is the index of R as an additive subgroup of O_K.

PROOF We argue as in Section 14.1, defining ϕ in the same way. If $\mathcal{B} = (\beta_1, \dots, \beta_n)$ is a basis of R, then $\mathcal{B}' = (\phi(\beta_1), \dots, \phi(\beta_n))$ generates $\phi(R)$ over $\mathbf{Z}$ and is an independant set, hence $\phi(R)$ is a sublattice of Λ_{O_K}, which we note Λ_R. We have

$$[\Lambda_{O_K} : \Lambda_R] = \frac{\det \Lambda_R}{\det \Lambda_{O_K}} \Longrightarrow \det \Lambda_{O_K} [\Lambda_{O_K} : \Lambda_R] = \det \Lambda_R.$$

However, from Section 14.1 we have

$$\det \Lambda_{O_K} = 2^{-s} \sqrt{|\mathrm{disc}(O_K)|} \qquad \text{and} \qquad \det \Lambda_R = 2^{-s} \sqrt{|\mathrm{disc}(R)|},$$

hence

$$|\mathrm{disc}(R)| = [O_K : R]^2 |\mathrm{disc}(O_K)|,$$

because $[\Lambda_{O_K} : \Lambda_R] = [O_K : R]$. $\square$

A particular application of this result is when $\alpha \in O_K$, $K = \mathbf{Q}(\alpha)$ and $R = \mathbf{Z}[\alpha]$. In this case the elements $1, \alpha, \ldots, \alpha^{n-1}$ form an integral basis of $\mathbf{Z}[\alpha]$. As we will see presently, it is often important to know whether a given prime number p does not divide $[O_K : \mathbf{Z}[\alpha]]$. In particular, if the discriminant $\mathrm{disc}(\mathbf{Z}[\alpha])$ is square-free, then $[O_K : \mathbf{Z}[\alpha]] = 1$ and so $\mathbf{Z}[\alpha] = O_K$.

In fact, we may improve the equality of Proposition 17.1.

Lemma 17.1 *Let K be a number field such that $[K : \mathbf{Q}] = n$. We suppose that there are r real embeddings of K in $\mathbf{C}$ and $2s$ complex embeddings. Then the sign of the discriminant of an order R in K is $(-1)^s$.*

PROOF Let $\mathcal{B} = \{b_1, \ldots, b_n\}$ be an integral basis of R. Then

$$\mathrm{disc}(R) = \det(\sigma_i(b_j))^2,$$

where $\sigma_1, \ldots, \sigma_r$ are the real embeddings of K into $\mathbf{C}$ and $\sigma_{r+1}, \ldots, \sigma_{r+2s}$ the complex embeddings of K into $\mathbf{C}$. We have

$$\overline{\det(\sigma_i(b_j))} = (-1)^s \det(\sigma_i(b_j)),$$

because complex conjugation interchanges s rows. If s is even, then $\det(\sigma_i(b_j))$ is real, so its square is positive. On the other hand, if s is odd, then $\det(\sigma_i(b_j))$ is purely imaginary, so its square is negative. $\square$

We may now improve Proposition 17.1:

Theorem 17.1 *Let K be a number field of degree n over $\mathbf{Q}$ and R an order of O_K. Then*

$$disc(R) = [O_K : R]^2 disc(O_K),$$

where $[O_K : R]$ is the index of R as an additive subgroup of O_K.

PROOF From Lemma 17.1 the discriminants of both R and O_K have the sign $(-1)^s$. $\square$

We also need some elementary results from group theory.

Lemma 17.2 *Let G be a finite (additive) abelian group of order n. If p is a prime and p does not divide n, then the mapping*

$$\phi : G \longrightarrow G, x \longmapsto px$$

is an automorphism.

PROOF The mapping ϕ is clearly a homomorphism. As G is finite, it is sufficient to show that ϕ is injective. Suppose that $px = 0$. If $x \neq 0$, then $1 < o(x) \leq p$, which implies that $o(x) = p$. Then we have $p|n$, a contradiction. So ϕ is injective. $\square$

Proposition 17.2 *Let $\psi : G' \longrightarrow G$ be an injective homomorphism of (additive) abelian groups. If $H = \psi(G')$ and $|\frac{G}{H}|$ is finite and not divisible by the prime p, then the induced mapping*

$$\bar{\psi} : \frac{G'}{pG'} \longrightarrow \frac{G}{pG} : x' + pG' \longmapsto \psi(x') + pG$$

is an isomorphism.

PROOF It is clear that $\bar{\psi}$ is a homomorphism. From Lemma 17.2 the mapping

$$\psi : \frac{G}{H} \longrightarrow \frac{G}{H}, x + H \longmapsto px + H$$

is an automorphism. If $x \in G$, then there exists $x_1 \in G$ such that

$$x + H = px_1 + H \Longrightarrow x - px_1 \in H \Longrightarrow x - px_1 = \psi(x'),$$

with $x' \in G'$. Then

$$x + pG = px_1 + \psi(x') + pG = \psi(x') + pG = \bar{\psi}(x' + pG'),$$

so $\bar{\psi}$ is surjective.

We now show that $\bar{\psi}$ is injective. Let $x' + pG' \in \frac{G'}{pG'}$ be such that $\bar{\psi}(x' + pG') = 0$, i.e., $\psi(x') \in pG$. Then there exists $x_1 \in G$ such that $\psi(x') = px_1$. We now set $x = \psi(x') = px_1$. Then $x \in H \cap pG$. Now

$$p(x_1 + H) = px_1 + H = x + H = H = 0.$$

From Lemma 17.2 the mapping ψ is an automorphism, hence $x_1 + H = H$, which implies that $x_1 \in H$. Thus we may write $x_1 = \psi(x_1')$, with $x_1' \in G'$. We have

$$x = \psi(x') \quad \text{and} \quad x = px_1 = p\psi(x_1') = \psi(px_1'),$$

which implies that $x' = px_1'$, because ψ is injective. This shows that $x' \in pG'$ and so $x' + pG' = 0$. It follows that $\bar{\psi}$ is injective. □

17.2 Dedekind's factorization theorem

In the following discussion which will lead to Dedekind's factorization theorem we will use some general results from ring theory. Let us begin with these results.

Proposition 17.3 *If $f : R \longrightarrow S$ is a surjective ring homomorphism, then the inverse image of a maximal ideal M in S is maximal. If N is a maximal ideal in R, then its image in S is either S or a maximal ideal.*

PROOF Let M be a maximal ideal in S. If $f^{-1}(M) = R$, then $f(x) \in M$, for every $x \in R$. As f is surjective, this is not possible, so $f^{-1}(M)$ is a proper ideal in R. We set $h = \pi \circ f$, where π is the canonical projection of S onto $\frac{S}{M}$. Then h is a surjective homomorphism, with kernel $f^{-1}(M)$. Moreover, $\frac{S}{M}$ is a field, so $\frac{R}{f^{-1}(M)}$ is a field. It follows that $f^{-1}(M)$ is a maximal ideal.

Now let N be a maximal ideal in R and suppose that $f(N)$ is properly contained in S. Let J be an ideal of S properly containing $f(N)$. Then $N \subset f^{-1}(f(N)) \subset f^{-1}(J)$. We claim that $N \neq f^{-1}(J)$. Let $x \in J \setminus f(N)$. As f is surjective, there exists $y \in R$ such that $f(y) = x$, which implies that $y \in f^{-1}(J)$. If $y \in N$, then $x = f(y) \in f(N)$, a contradiction. Hence $N \neq f^{-1}(J)$, as claimed. Since $f^{-1}(J)$ is an ideal in R, the maximality of N ensures that $f^{-1}(J) = R$ and so $f(f^{-1}(J)) = f(R)$. Using the surjectivity of f, we obtain $J = S$, and it follows that $f(N)$ is a maximal ideal. □

Proposition 17.4 *If I and J are coprime ideals in a commutative ring R and $m, n \in \mathbf{N}^*$, then I^m and J^n are coprime.*

PROOF As $I + J = R$, we have $(I + J)^{m+n} = R^{m+n} = R$. Each term in the development of $(I + J)^{m+n}$ is included in I^m or J^n, therefore R is included in $I^m + J^n$. The reverse inclusion is trivial, so we have $I^m + J^n = R$, i.e., I^m and J^n are coprime. □

Proposition 17.5 *Let R be a commutative ring and I an ideal in R. The projection $\pi : R \longrightarrow \frac{R}{I}$ defines a bijection from the set of ideals containing I onto the set of ideals in $\frac{R}{I}$. If restricted to prime (resp. maximal) ideals, then we obtain a bijection of the set of prime (resp. maximal) ideals containing I onto the set of prime (resp. maximal) ideals in $\frac{R}{I}$.*

PROOF Let A be the set of ideals in R containing I and B the set of ideals in $\frac{R}{I}$. Using the fact that π is a surjective homomorphism, there is no difficulty in seeing that π defines a mapping from A into B, which we will write $\bar{\pi}$. If $J \in B$, then $\pi^{-1}(J)$ is an ideal in R and $\pi(\pi^{-1}(J) = J$, so $\bar{\pi}$ is surjective.

Suppose now that there exist ideals I_1, I_2 containing I such that $\bar{\pi}(I_1) = \bar{\pi}(I_2)$, i.e., $\frac{I_1}{I} = \frac{I_2}{I}$. If $s \in I_1$, then $s+I = t+I$, for some $t \in I_2$. Hence there exist $x_1, x_2 \in I$ such that $s+x_1 = t+x_2$, which implies that $s = t + x_2 - x_1 \in I_2$. Thus $I_1 \subset I_2$. In the same way; $I_2 \subset I_1$, so $I_1 = I_2$ and $\bar{\pi}$ is injective.

Now let us restrict $\bar{\pi}$ to prime ideals. If P is a prime ideal, then it is easy to see that $\pi(P)$ is a prime ideal in $\frac{R}{I}$. Suppose that Q is a prime ideal in $\frac{R}{I}$; then $\pi^{-1}(Q)$ is a prime ideal in R containing I and $\pi(\pi^{-1}(Q)) = Q$. Thus $\bar{\pi}$ as a mapping from the prime ideals containing I into the prime ideals in $\frac{R}{I}$ is surjective. Since $\bar{\pi}$ is injective, the mapping $\bar{\pi}$ must be injective when restricted to prime ideals.

Finally let us consider maximal ideals. Let N be a maximal ideal in R containing I. We claim that $\bar{\pi}(N)$ is properly contained in R/I. If $\bar{\pi}(N) = R/I$, then, for any $r \in R$, there exists $x \in N$ such that $r - x \in I$. Thus $r \in N$, because N contains I; this implies that $R = N$, which is not possible, because N is a maximal ideal in R. Thus $\bar{\pi}(N) \neq R/I$. From Proposition 17.3 we deduce that $\bar{\pi}(N)$ is a maximal ideal in R/I. Hence $\bar{\pi}$ takes maximal ideals to maximal ideals. If M is a maximal ideal in R/I, then $\pi^{-1}(M)$ is a maximal ideal in R and $\pi(\pi^{-1}(M) = M$, so $\bar{\pi}$ is surjective when restricted to maximal ideals. As $\bar{\pi}$ is injective, $\bar{\pi}$ is injective when restricted to maximal ideals. □

Exercise 17.1 *Let I be an ideal in the commutative ring R and π the canonical projection of R onto R/I. If M is a maximal ideal in R/I, then we know that there is a unique maximal ideal N of R containing I such that $\pi(N) = M$. Show that the field $(R/I)/M$ is isomorphic to the field R/N.*

The principle result which we will establish in this section enables us, in all but a finite number of cases, to find the form of the factorization into prime ideals of an ideal which is the extension of a prime number in a number ring. Let K be a number field with associated number ring O_K, $\alpha \in O_K$ and $K = \mathbf{Q}(\alpha)$. We suppose that p is a prime which does not divide $[O_K : \mathbf{Z}[\alpha]]$. From Proposition 17.2, the natural ring inclusion ψ of $\mathbf{Z}[\alpha]$ into O_K induces an additive group isomorphism

$$\bar{\psi} : \frac{\mathbf{Z}[\alpha]}{\mathbf{Z}[\alpha]p} \longrightarrow \frac{O_K}{O_K p}.$$

There is no difficulty in seeing that $\bar{\psi}$ is also a ring isomorphism.

It is worth studying the mapping $\bar{\psi}$ in more detail. If $\bar{I}$ is an ideal in $\frac{\mathbf{Z}[\alpha]}{\mathbf{Z}[\alpha]p}$, then its image is an ideal in $\frac{O_K}{O_K p}$. However, there is is a minor difficulty. The ideal $\bar{I}$ has the form $\frac{I}{\mathbf{Z}[\alpha]p}$, where I is an ideal containing $\mathbf{Z}[\alpha]p$ in $\mathbf{Z}[\alpha]$ and $\bar{\psi}(\bar{I}) = \frac{I}{O_K p}$ is composed of the classes of $\frac{O_K}{O_K p}$ having a representative in I. At first viewing it is not clear how $\frac{I}{O_Kp}$ can be an ideal in $\frac{O_K}{O_Kp}$. In particular, when we multiply an element in $\frac{I}{O_Kp}$ by an element in $\frac{O_K}{O_Kp}$, how can we be sure that the result lies in $I + O_Kp$? This in fact is the case. We consider the case

$$(a + O_Kp)(x + O_Kp),$$

where $a \in O_K$ and $x \in I$. As $\bar{\psi}$ is bijective, there exists $a' \in \mathbf{Z}[\alpha]$ such that $a + O_Kp = a' + O_Kp$. Hence we may write

$$(a + O_Kp)(x + O_Kp) = (a' + O_Kp)(x + O_Kp) = a'x + O_Kp \in \frac{I}{O_Kp},$$

which resolves the apparent problem.

The mapping $\bar{\psi}$ provides us with a bijection from the set of ideals in $\frac{\mathbf{Z}[\alpha]}{\mathbf{Z}[\alpha]p}$ onto the set of ideals in $\frac{O_K}{O_Kp}$ and maps a prime ideal to a prime ideal. We may find an interesting expression for the image of an ideal in $\frac{\mathbf{Z}[\alpha]}{\mathbf{Z}[\alpha]p}$. First $\bar{\psi}(\frac{I}{\mathbf{Z}[\alpha]p}) = \frac{I}{O_Kp}$. As $I \subset O_KI$, we have $\frac{I}{O_Kp} \subset \frac{O_KI}{O_Kp}$. Now let $u \in \frac{O_KI}{O_Kp}$. Then we may write $u = \sum_{i=1}^{s} a_ix_i + O_Kp$ with $a_i \in O_K$, $x_i \in I$. As above, for each a_i, there exists $a_i' \in \mathbf{Z}[\alpha]$ such that $a_i + O_Kp = a_i' + O_Kp$, thus

$$\begin{aligned}\sum_{i=1}^{s} a_ix_i + O_Kp &= \sum_{i=1}^{s}(a_i + O_Kp)(x_i + O_Kp)\\ &= \sum_{i=1}^{s}(a_i' + O_Kp)(x_i + O_Kp)\\ &= \sum_{i=1}^{s} a_i'x_i + O_Kp.\end{aligned}$$

As $a_i'x_i \in I$, for each i, we see that $u \in \frac{I}{O_Kp}$. It follows that $\frac{O_KI}{O_Kp} \subset \frac{I}{O_Kp}$. Thus for an ideal $\frac{I}{\mathbf{Z}[\alpha]p}$ in $\frac{\mathbf{Z}[\alpha]}{\mathbf{Z}[\alpha]p}$, we have $\bar{\psi}(\frac{I}{\mathbf{Z}[\alpha]p}) = \frac{O_KI}{O_Kp}$.

Remark The mapping $\bar{\psi}$ enables us to define a bijection between prime ideals containing p in $\mathbf{Z}[\alpha]$ and prime ideals in O_K containing p. Let π_1 be the projection of $\mathbf{Z}[\alpha]$ onto $\mathbf{Z}[\alpha]p$ and π_2 the projection of O_K onto O_Kp. If P is a prime ideal in $\mathbf{Z}[\alpha]$ containing p (or, equivalently $\mathbf{Z}[\alpha]p$), then, from Proposition 17.5, $\pi_1(P) = \frac{P}{\mathbf{Z}[\alpha]p}$ is a prime ideal in $\frac{\mathbf{Z}[\alpha]}{\mathbf{Z}[\alpha]p}$. As $\bar{\psi}$ is an isomorphism, $\bar{\psi}(\frac{P}{\mathbf{Z}[\alpha]p})$ is a prime ideal in $\frac{O_K}{O_Kp}$, i.e., $\frac{O_KP}{O_K}$ is a prime ideal in $\frac{O_K}{O_Kp}$. Then $O_KP = \pi_2^{-1}(\frac{O_KP}{O_K})$ is a prime ideal in O_K containing O_Kp (or, equivalently p). Thus the mapping $P \longmapsto O_KP$ sends prime ideals in $\mathbf{Z}[\alpha]$ containing p to prime ideals in O_K containing p. Since $O_KP = \pi_2^{-1}(\bar{\psi}(\pi(P))$, this mapping is a bijection. We should also notice that it is multiplicative, i.e., if I, J are ideals in $\mathbf{Z}[\alpha]$ such that $p \in I$, $p \in J$ and $p \in IJ$, then $O_K(IJ) = (O_KI)(O_KJ)$.

We now study the quotient ring $\frac{\mathbf{Z}[\alpha]}{\mathbf{Z}[\alpha]p}$ in more detail. We write $\bar{g}$ for the polynomial $g \in \mathbf{Z}[X]$ reduced modulo p.

Let h be the minimal polynomial $m(\alpha, \mathbf{Q})$. By Corollary 11.1, h belongs to $\mathbf{Z}[X]$. The mapping $e_\alpha : \mathbf{Z}[X] \longrightarrow \mathbf{Z}[\alpha]$ defined by $e_\alpha(g) = g(\alpha)$ is a surjective ring homomorphism. As h is monic and $h(\alpha) = 0$, the kernel of ϕ is the ideal (h). It follows that the mapping

$$\bar{e}_\alpha : \mathbf{Z}[X]/(h) \longrightarrow \mathbf{Z}[\alpha], g + (h) \longmapsto g(\alpha)$$

is an isomorphism. We set $\Psi = e_\alpha^{-1}$. Notice that, for $a \in \mathbf{Z} \subset \mathbf{Z}[\alpha]$, we have $\Psi(a) = a + (h)$.

Proposition 17.6 *We have*

$$\frac{\mathbf{Z}[\alpha]}{\mathbf{Z}[\alpha]p} \simeq \frac{\mathbf{F}_p[X]}{(\bar{h})}.$$

PROOF First we notice that the image of the ideal $\mathbf{Z}[\alpha]p$ under Ψ can be written $\frac{\mathbf{Z}[X]p}{(h)}$, so we obtain an isomorphism $\bar{\Psi}$ from $\frac{\mathbf{Z}[\alpha]}{\mathbf{Z}[\alpha]p}$ onto $\frac{\mathbf{Z}[X]}{(h)}/\frac{\mathbf{Z}[X]p}{(h)}$. We now consider the mapping

$$\delta : \frac{\mathbf{Z}[X]}{(h)}/\frac{\mathbf{Z}[X]p}{(h)} \longrightarrow \frac{\frac{\mathbf{Z}}{\mathbf{Z}p}[X]}{(\bar{h})}, (g + (h)) + \frac{\mathbf{Z}[X]p}{(h)} \longmapsto \bar{g} + (\bar{h}).$$

The mapping δ is clearly a surjective ring homomorphism. We need to show that δ is also injective. If $\bar{f} \in (\bar{h})$, then there exists $\bar{u} \in \frac{\mathbf{Z}}{\mathbf{Z}p}[X]$ such that $\bar{f} = \bar{u}\bar{h} = \overline{uh}$. Thus $\bar{f} - \overline{uf} = \bar{0}$, so $f - uh$ is a polynomial in $\mathbf{Z}[X]$, all of whose coefficients are multiples of p, i.e., $f - uh \in \mathbf{Z}[X]p$. Then

$$f + (h) = (f - uh) + (h) \in \frac{\mathbf{Z}[X]p}{(h)} \Longrightarrow (f + (h)) = 0 \quad \text{in} \quad \frac{\mathbf{Z}[X]}{(h)}/\frac{\mathbf{Z}[X]p}{(h)}.$$

Hence δ is injective and so we have the required isomorphism, namely $\eta = \delta \circ \bar{\Psi}$. Explicitly η maps $g(\alpha) + \mathbf{Z}[\alpha]p$ to $\bar{g} + (\bar{h})$. □

Remark The image of $\mathbf{Z}[\alpha]p$ is $(\bar{h})$. □

Corollary 17.1 *If p is a prime which does not divide $[O_K : \mathbf{Z}[\alpha]]$, then the rings $\frac{O_K}{O_K p}$ and $\frac{\mathbf{F}_p[X]}{(\bar{h})}$ are isomorphic.*

Now let us turn to Dedekind's theorem. We first consider the prime ideals in $\frac{\mathbf{F}_p[X]}{(\bar{h})}$. From Proposition 17.5 the prime ideals in $\frac{\mathbf{F}_p[X]}{(\bar{h})}$ are of the form $\frac{I}{(\bar{h})}$, where I is a prime ideal in $\mathbf{F}_p[X]$ containing $(\bar{h})$. As $\mathbf{F}_p[X]$ is a PID, every ideal I is principal, i.e., $I = (f)$ for some $f \in \mathbf{F}_p[X]$. If (f) is an ideal containing $(\bar{h})$, then f divides $\bar{h}$. Moreover, if (f) is a prime ideal, then f is a prime element. Given that a PID is a UFD, f must be an irreducible polynomial. Hence we are looking for irreducible polynomials in $\mathbf{F}_p[X]$ dividing $\bar{h}$. If $\bar{h} = A_1^{e_1} \cdots A_s^{e_s}$ is the factorization of $\bar{h}$ into irreducible polynomials in $\mathbf{F}_p[X]$, then the A_i are the irreducible polynomials we are looking for. Hence the prime ideals in $\frac{\mathbf{F}_p[X]}{(\bar{h})}$ are of the form $\bar{J}_i = \frac{(A_i)}{(\bar{h})}$. As the (A_i) are maximal ideals, so are the $\bar{J}_i$.

Our next step is to consider prime ideals in $\mathbf{Z}[\alpha]/\mathbf{Z}[\alpha]p$. The inverse image of the mapping η defined in Proposition 17.6 is given by the evaluation at α, namely, if $f \in \mathbf{F}_p[X]$ and $g \in \mathbf{Z}[X]$ is such that $\bar{g} = f$, then the preimage of $f + (\bar{h})$ is $g(\alpha) + \mathbf{Z}[\alpha]p$. (There is no difficulty in seeing that, if $g, g_1 \in \mathbf{Z}[X]$ and $\bar{g} = \bar{g}_1$, then $g(\alpha) + \mathbf{Z}[\alpha]p = g_1(\alpha) + \mathbf{Z}[\alpha]p$.) In particular, if (f) is an ideal in $\mathbf{F}_p[X]$ containing $(\bar{h})$, then $\bar{J} = \frac{(f)}{(\bar{h})}$ is an ideal in $\frac{\mathbf{F}_p[X]}{(\bar{h})}$ and its preimage is $\frac{(g(\alpha))}{\mathbf{Z}[\alpha]p}$. Clearly, if (f) is a prime ideal, then so is $\bar{J}$.

For each A_i, let $h_i \in \mathbf{Z}[X]$ be such that $\bar{h}_i = A_i$. For $i = 1, \ldots, s$, we set $\bar{P}_i = \eta^{-1}(\bar{J}_i) = \frac{(h_i(\alpha))}{\mathbf{Z}[\alpha]p}$. The $\bar{P}_i$ are the prime ideals in $\frac{\mathbf{Z}[\alpha]}{\mathbf{Z}[\alpha]p}$. As the $\bar{P}_i$ correspond to maximal ideals in $\frac{\mathbf{F}_p[X]}{(\bar{h})}$, they are also maximal.

Let π be the natural projection of $\mathbf{Z}[\alpha]$ onto $\frac{\mathbf{Z}[\alpha]}{\mathbf{Z}[\alpha]p}$. Then $P_i = \pi^{-1}(\bar{P}_i)$ is a prime ideal in $\mathbf{Z}[\alpha]$ containing $\mathbf{Z}[\alpha]p$ (or, equivalently, containing p). From Proposition 17.5, we know that these are the only prime ideals in $\mathbf{Z}[\alpha]$ containing $\mathbf{Z}[\alpha]p$. Setting $Q_i = O_K P_i$, for $i = 1, \ldots, s$, we obtain the prime ideals in O_K containing p. The fact that Q_i contains p may be written $Q_i | O_K p$. Thus the decomposition of $O_K p$ into prime ideals has the form

$$O_K p = Q_1^{e'_1} \cdots Q_1^{e'_s},$$

where e'_i is the ramification index of Q_i. We aim to show that $e'_i = e_i$.

To begin with, we show that $e'_i \leq e_i$. We claim that $(\pi^{-1}(\bar{P}_i))^{e_i} \subset \pi^{-1}(\bar{P}_i^{e_i})$. Let $u \in (\pi^{-1}(\bar{P}_i))^{e_i}$. Then u is a finite sum of products of the form $a_1 \cdots a_{e_i}$ such that $\pi(a_1), \ldots, \pi(a_{e_i}) \in \bar{P}_i$. Suppose, for example, that $u = a_1 \ldots a_{e_i} + b_1 \ldots b_{e_i}$ Then

$$\pi(a_1) \cdots \pi(a_{e_i}) + \pi(b_1) \cdots \pi(b_{e_i}) \in \bar{P}_i^{e_i} \Longrightarrow \pi(a_1 \ldots a_{e_i} + b_1 \ldots b_{e_i}) \in \bar{P}_i^{e_i} \Longrightarrow u \in \pi^{-1}(\bar{P}_i^{e_i}).$$

The other cases, with more or less products in the sum, can be handled in an analogous way, hence $(\pi^{-1}(\bar{P}_i))^{e_i} \subset \pi^{-1}(\bar{P}_i^{e_i})$, as claimed.

We now consider the intersection $\cap_{i=1}^s \pi^{-1}(\bar{P}_i^{e_i})$. Let $u \in \cap_{i=1}^s \pi^{-1}(\bar{P}_i^{e_i})$. For $i = 1, \ldots, s$, we have

$$\pi(u) \in \frac{(h_i^{e_i}(\alpha))}{\mathbf{Z}[\alpha]p} \Longrightarrow \eta(\pi(u)) \in \frac{(\bar{h}_i^{e_i})}{(\bar{h})},$$

and so $\eta(\pi(u)) = \frac{(\bar{h})}{(\bar{h})}$, which in turn implies that $\pi(u) = \frac{\mathbf{Z}[\alpha]p}{\mathbf{Z}[\alpha]p}$. Therefore, $u \in \mathbf{Z}[\alpha]p$ and it follows that $\cap_{i=1}^s \pi^{-1}(\bar{P}_i^{e_i}) \subset \mathbf{Z}[\alpha]p$. From this and the preceding paragraph we obtain

$$\mathbf{Z}[\alpha]p \supset \cap_{i=1}^s \pi^{-1}(\bar{P}_i^{e_i}) \supset \cap_{i=1}^s (\pi^{-1}(\bar{P}_i))^{e_i} = \cap_{i=1}^s P_i^{e_i}.$$

We claim that $\cap_{i=1}^s P_i^{e_i} = \prod_{i=1}^s P_i^{e_i}$. In the light of Proposition 12.4, it is sufficient to show that the ideals $P_i^{e_i}$ are coprime, when $i \neq j$. First, π is a surjective homomorphism and, for each i, the ideal $\bar{P}_i$ is maximal, so P_i is a maximal ideal from Lemma 17.3. It follows that P_i and P_j are coprime, when $i \neq j$. Now, from Lemma 17.4, $P_i^{e_i}$ and $P_j^{e_j}$ are coprime and thus we obtain

$$\mathbf{Z}[\alpha]p \supset \prod_{i=1}^s P_i^{e_i}.$$

Therefore

$$O_K p \supset O_K \left(\prod_{i=1}^s P_i^{e_i} \right) = \prod_{i=1}^s Q_i^{e_i},$$

This implies that $e'_i \leq e_i$, for $i = 1, \ldots, s$, as $O_K p = \prod_{i=1}^s Q_i^{e'_i}$.

We now show that $e'_i = e_i$, for all i. We need to consider the inertial degree $f_i = f(Q_i|p)$, i.e., the degree of the extension $\frac{O_K}{Q_i}$ over $\mathbf{F}_p$. We notice that the mapping

$$f : \frac{\mathbf{Z}}{\mathbf{Z}p} \longrightarrow \frac{O_K}{Q_i}, a + \mathbf{Z}p \longmapsto a + Q_i$$

is a monomorphism, so $\frac{O_K}{Q_i}$ is a field containing $\mathbf{F}_p$. Now, we have the following chain of additive group isomorphisms:

$$\frac{O_K}{Q_i} \simeq \frac{O_K}{O_K p} / \frac{Q_i}{O_K p} \simeq \frac{\mathbf{Z}[\alpha]}{\mathbf{Z}[\alpha]p} / \frac{P_i}{\mathbf{Z}[\alpha]p} = \frac{\mathbf{Z}[\alpha]}{\mathbf{Z}[\alpha]p} / \bar{P}_i \simeq \frac{\mathbf{F}_p[X]}{(\bar{h})} / \frac{(A_i)}{(\bar{h})} \simeq \frac{\mathbf{F}_p[X]}{(A_i)}.$$

These spaces are also $\mathbf{F}_p$-vector spaces and it is not difficult to see that the additive group isomorphisms are also $\mathbf{F}_p$-vector space isomorphisms. Therefore the dimension of the field $\frac{O_K}{Q_i}$ over $\mathbf{F}_p$ is that of $\frac{\mathbf{F}_p[X]}{(A_i)}$ over $\mathbf{F}_p$. This vector space has the dimension d_i, the degree of the polynomial A_i: If $f \in \mathbf{F}_p[X]$, then there exist $g, r_i \in \mathbf{F}_p[X]$ such that : deg $(r_i) < d_i$ and $f = gA_i + r_i$. Then

$$f + (A_i) = gA_i + r_i + (A_i) = r_i + (A_i)$$

and it follows that $\mathcal{B} = \{1 + (A_i), X + (A_i), \ldots, X^{d_i - 1} + (A_i)\}$ is a generating set of $\frac{\mathbf{F}_p[X]}{(A_i)}$. $\mathcal{B}$ is also an independant set. Let

$$\lambda_0(1 + (A_i)) + \lambda_1(X + (A_i)) + \cdots + \lambda_{d_i - 1}(X^{d_i - 1} + (A_i)) = (A_i),$$

where the $\lambda_i \in \mathbf{F}_p$. Then $U(X) = \sum_{j=0}^{d_i - 1} \lambda_j X^j \in (A_i)$. As deg $(U) < d_i$, U is the zero polynomial and it follows that the λ_i all have the value 0. Therefore $\mathcal{B}$ is an independant set and so a basis of $\frac{\mathbf{F}_p[X]}{(A_i)}$. We have shown that $\frac{\mathbf{F}_p[X]}{(A_i)}$ has dimension d_i. It follows that the inertial degree f_i is equal to d_i.

We now use Proposition 13.7:

$$n = [K : \mathbf{Q}] = \sum_{i=1}^{s} e'_i f_i \leq \sum_{i=1}^{s} e_i d_i.$$

As the degree of the polynomial $A_i^{e_i}$ is $e_i d_i$, the product $A_1^{e_1} \cdots A_s^{e_s}$ has degree $\sum_{i=1}^{s} e_i d_i$. Given that this product is $\bar{h}$, which has degree n, we have $\sum_{i=1}^{s} e_i d_i = n$.

To conclude we have

$$n = [K : \mathbf{Q}] = \sum_{i=1}^{s} e'_i f_i \leq \sum_{i=1}^{s} e_i d_i = n.$$

As $d_i = f_i$ and $e'_i \leq e_i$, we must have $e'_i = e_i$, as required.

To sum up, we have proved the following result, known as Dedekind's factorization theorem:

Theorem 17.2 *Let $K = \mathbf{Q}(\alpha)$ be a number field, with $\alpha \in O_K$, and $h = m(\alpha, \mathbf{Q})$. If p is a prime number and $p \nmid [O_K : \mathbf{Z}[\alpha]]$, then the factorization of $O_K p$ into prime ideals has the same form as that of $\bar{h}$ (=h modulo p) into irreducible polynomials.*

Remark In proving Theorem 17.2, we have seen that $d_i = f_i$. If Q_i is the ideal corresponding to $\bar{h}_i$ and Q_i lies over the prime p, then $\|Q_i\| = p^{d_i}$. This follows from the proof of Proposition 13.7.

Theorem 17.2 may be difficult to use in practice, since, in order to know that p does not divide the index $[O_K : \mathbf{Z}[\alpha]]$, we have to know this index. The corollary which follows provides us with a condition which is easier to check.

Corollary 17.2 *Let $K = \mathbf{Q}(\alpha)$ be a number field, with $\alpha \in O_K$, and $h = m(\alpha, \mathbf{Q})$. If p is a prime number and $p \nmid disc(\mathbf{Z}[\alpha])$, then the factorization of $O_K p$ into prime ideals has the same form as that of $\bar{h}$ (=h modulo p) into irreducible polynomials.*

PROOF As

$$\mathrm{disc}(\mathbf{Z}[\alpha]) = [O_K : \mathbf{Z}[\alpha]]^2 \mathrm{disc}(O_K),$$

if $p \nmid \mathrm{disc}(\mathbf{Z}[\alpha])$, then $p \nmid [O_K : \mathbf{Z}[\alpha]]$ and Theorem 17.2 applies. □

Examples 1. Let $K = \mathbf{Q}(\sqrt{d})$, where d is a square-free integer. Then $O_K = \mathbf{Z}[\omega]$, where $\omega = \sqrt{d}$, if $d \equiv 2, 3 \pmod 4$ and $\omega = \frac{1+\sqrt{d}}{2}$, if $d \equiv 1 \pmod 4$. In both cases $[O_K : \mathbf{Z}[\omega]] = 1$, so no prime number p divides $[O_K : \mathbf{Z}[\omega]]$, hence Theorem 17.2 is applicable. In the first case $m(\omega, \mathbf{Q}) = -d + X^2$ and in the second case $m(\omega, \mathbf{Q}) = \frac{1-d}{4} - X + X^2$.

For instance, if $d = 2$ and $p = 3$, then

$$m(\omega, \mathbf{Q}) = -2 + X^2 \equiv 1 + X^2 \pmod 3,$$

which is irreducible. It follows that $O_K 3 = Q$, for some prime ideal Q.

To take another example, if $d = 5$ and $p = 5$, then we have

$$m(\omega, \mathbf{Q}) = -1 - X + X^2 \equiv 4 + 4X + X^2 = (2 + X)^2 \pmod 5.$$

Hence $O_K 5 = Q^2$, for some prime ideal Q, i.e., 5 is totally ramified in O_K.

2. Let $K = \mathbf{Q}(\sqrt[3]{10})$ An elementary calculation shows that $\mathrm{disc}(\mathbf{Z}[\sqrt[3]{10}]) = -2700 = -2^2.3^3.5^3$. From Corollary 17.2, for any prime number p other than 2, 3 or 5, the form of the factorization of $O_K p$ can be determined from that of $m(\sqrt[3]{10}, \mathbf{Q}) \pmod p$.

For instance,

$$m(\sqrt[3]{10}, \mathbf{Q}) = -10 + X^3 \equiv 4 + X^3 \pmod 7,$$

which is irreducible, so $O_K 7 = Q$, for some prime ideal Q.

We now consider $O_K 3$. We look for an element $\beta \in O_K$ such that $K = \mathbf{Q}(\beta)$ and $3 \not| [O_K : \mathbf{Z}[\beta]]$. (Of course, $\beta \neq \alpha$). If $\beta = \frac{1}{3}(1 + \sqrt[3]{10} + \sqrt[3]{100}))$, then β is a root of the polynomial $f(X) = -3 - 3X - X^2 + X^3$. As f has no rational root, f is irreducible over $\mathbf{Q}$ and so $f = m(\beta, \mathbf{Q})$. It is not difficult to see that $\mathbf{Q}(\beta) \subset K$, so we have

$$[K : \mathbf{Q}] = [K : \mathbf{Q}(\beta)][\mathbf{Q}(\beta) : \mathbf{Q}] \Longrightarrow [K : \mathbf{Q}(\beta)] = 1,$$

because $[K : \mathbf{Q}] = [\mathbf{Q}(\beta) : \mathbf{Q}] = 3$. Hence $K = \mathbf{Q}(\beta)$. As $\mathrm{disc}(\mathbf{Z}[\beta]) = -300 = -2^2.3.5^2$, from the formula

$$\mathrm{disc}(\mathbf{Z}[\beta]) = [O_K : \mathbf{Z}[\beta]]^2 \mathrm{disc}(O_K),$$

we see that $3 \not| [O_K : \mathbf{Z}[\beta]]$ and we may apply Theorem 17.2:

$$m(\beta, \mathbf{Q}) = -3 - 3X - X^2 + X^3 \equiv (-1 + X)X^2 \pmod 3,$$

so $O_K 3 = Q_1 Q_2^2$, for prime ideals Q_1, Q_2.

3. If $K = \mathbf{Q}(\zeta)$, where ζ is a primitive root of unity, i.e., K is a cyclotomic extension of $\mathbf{Q}$, then $O_K = \mathbf{Z}[\zeta]$, so in this case $[O_K : \mathbf{Z}[\zeta]] = 1$ and no prime number p divides $[O_K : \mathbf{Z}[\zeta]]$. We may apply Theorem 17.2 for any prime p. Let us consider the case where $\zeta = e^{\frac{2\pi i}{p^n}}$.Then

$$m(\zeta, \mathbf{Q}) = \Phi_{p^n}(X) = \Phi_p(X^{p^{n-1}}),$$

where Φ_{p^n} is the cyclotomic polynomial of order p^n. Now,

$$\Phi_p(X)(-1 + X) = -1 + X^p \equiv (-1 + X)^p \pmod p,$$

so

$$\Phi_p(X) \equiv (-1 + X)^{p-1} \pmod p \Longrightarrow \Phi_{p^n}(X) \equiv (-1 + X^{p^{n-1}})^{p-1} \pmod p,$$

and finally

$$\Phi_{p^n}(X) \equiv (-1 + X)^{p^{n-1}(p-1)} \pmod p.$$

It follows that

$$O_K p = Q^{p^{n-1}(p-1)},$$

for some prime ideal Q, i.e., p is totally ramified in O_K.

Let us consider the case where $p = 5$ and $n = 1$. Then

$$\Phi_5(X) = 1 + X + X^2 + X^3 + X^4$$

and $O_K 5 = Q^4$, for some prime ideal Q. Now let us consider $O_K p$, where $p \neq 5$. We have

$$\Phi_5(X) \equiv 1 + X + X^2 + X^3 + X^4 \pmod 3,$$

which is irreducible modulo 3. (To check this it is sufficient to observe that the polynomial has no root in $\mathbf{F}_3$ and is not divisible by any irreducible polynomial of degree 2 in $\mathbf{F}_3[X]$.) Thus $O_K 3 = Q$, where Q is a prime ideal. A similar situation applies for $p = 7$.

On the other hand,

$$\Phi_5(X) \equiv (-3 + X)(-4 + X)(-5 + X)(-9 + X) \pmod{11},$$

so $O_K 11 = Q_1 Q_2 Q_3 Q_4$, where the Q_i are distinct prime ideals.

Remark We could have obtained the results in this example by applying the theory we develloped in Section 13.9.

Chapter 18

Monogenic fields

A *monogenic field* is an algebraic number field K for which there exists an element α in the ring of integers O_K such that $O_K = \mathbf{Z}[\alpha]$. Such an element α is called a *power generator* . We have seen that quadratic fields and cyclotomic fields are monogenic. Also, from Proposition 17.1, if the discriminant of $\mathbf{Z}[\alpha]$ is square-free, then K is monogenic. If K is monogenic, then we may apply Dedekind's factorization theorem to find the form of the factorization into prime ideals of the ideal $O_K p$ for any prime p. If K is monogenic and $O_K = \mathbf{Z}[\alpha]$, then O_K has an integral basis composed of powers of α, called a *power basis* , and the discriminant $\mathrm{disc}(O_K)$ may be calculated using this basis, which is simpler than in the general case. In addition, such fields have other interesting properties as we will presently see.

Remark If the number field K is monogenic and α is a power generator, then α is not unique. In fact, for any integer n, $\alpha + n$ is also a power generator. It is interesting to know whether there are other power generators. This may well be the case. The following result gives us an example.

Proposition 18.1 *Let ζ be a primitive pth root of unity, with p an odd prime, and $K = \mathbf{Q}(\zeta)$. If $\eta = 1 + \zeta^2 + \zeta^4 + \cdots + \zeta^{p-1}$ (even powers), then ζ and η do not differ by an integer and $\mathbf{Z}[\zeta] = \mathbf{Z}[\eta]$.*

PROOF Let us suppose that there is an integer k such that $\zeta - \eta = k$. We notice that $\eta = \frac{1}{1+\zeta}$, so

$$\frac{1}{1+\zeta} - \zeta = k \Longrightarrow 1 = (k+\zeta)(1+\zeta) \Longrightarrow 0 = (k-1) + (k+1)\zeta + \zeta^2.$$

However,

$$(k+1)^2 - 4(k-1) = 5 - 2k + k^2,$$

which is positive for all values of k. This implies that ζ is a real number, a contradiction. Hence ζ and η do not differ by an integer.

Clearly $\mathbf{Z}[\eta] \subset \mathbf{Z}[\zeta]$. To establish that $\mathbf{Z}[\zeta] \subset \mathbf{Z}[\eta]$, it is sufficient to show that $\zeta \in \mathbf{Z}[\eta]$. We have seen that η is a unit with inverse $1 + \zeta$. As η is invertible, from Proposition 11.3, the norm $N_{K/\mathbf{Q}}(\eta)$ has the value ± 1 and so the constant term of the minimal polynomial $f = m(\eta, \mathbf{Q})$ has the value ± 1. Without loss of generality let us suppose that the constant term is positive. Then

$$f(X) = 1 + a_1 X + a_2 X^2 + \cdots + a_{s-1} X^{s-1} + X^s,$$

where the a_i are integers. From this we obtain

$$1 = -a_1\eta - a_2\eta^2 - \cdots - a_{s-1}\eta^{s-1} - \eta^s \Longrightarrow 1 + \zeta = -a_1 - a_2\eta - \cdots - a_{s-1}\eta^{s-2} - \eta^{s-1},$$

and it follows that $\zeta \in \mathbf{Z}[\eta]$. $\square$

Remark It can be shown that a monogenic field can only have a finite number of distinct power generators, i.e., power generators which do not differ by an integer ([11]).

18.1 Monogenic and non-monogenic fields: examples

Other number fields than those we have already mentioned are monogenic; however, many number fields are not. Before giving examples of non-monogenic number fields, we will give some further examples of monogenic fields.

Suppose that p is an odd prime and ζ a primitive pth root of unity in $\mathbf{C}$. Let $K = \mathbf{Q}(\zeta)$. We set $K_0 = \mathbf{Q}(\zeta + \zeta^{-1})$. We claim that K_0 is monogenic. First, K_0 is a real subfield of K and $[K : \mathbf{Q}] = [K : K_0][K_0 : \mathbf{Q}]$. We set $f(x) = 1 - (\zeta + \zeta^{-1})X + X^2 \in K_0[X]$. Then $f(\zeta) = 0$ and $\zeta \notin K_0$, so $f = m(\zeta, K_0)$ and it follows that $[K : K_0] = 2$. From this we deduce that $[K_0 : \mathbf{Q}] = \frac{p-1}{2}$ and that K_0 is a maximal subfield of K. Now we show that K_0 is monogenic, with $\zeta + \zeta^{-1}$ as power generator.

As $\zeta + \zeta^{-1}$ is the sum of two algebraic integers, it is an algebraic integer. Clearly, $\zeta + \zeta^{-1}$ belongs to K_0, thus $\mathbf{Z}[\zeta + \zeta^{-1}] \subset O_{K_0}$. The reverse inclusion requires more work.

Let $u \in O_{K_0}$. Then, by Proposition 11.10, we may write $u = \sum_{i=1}^{p-1} u_i\zeta^i$, with $u_i \in \mathbf{Z}$. Then

$$u = \sum_{i=1}^{p-1} u_i\zeta^i = \sum_{i=1}^{\frac{p-1}{2}} u_i\zeta^i + \sum_{i=\frac{p+1}{2}}^{p-1} u_i\zeta^i = \sum_{i=1}^{\frac{p-1}{2}} u_i\zeta^i + \sum_{i=1}^{\frac{p-1}{2}} u_{p-i}\zeta^{p-i}.$$

Because u is real, we have $u = \bar{u}$, hence

$$u = \sum_{i=1}^{p-1} u_i\zeta^i = \sum_{i=1}^{p-1} u_i\zeta^{-i} = \sum_{i=1}^{p-1} u_i\zeta^{p-i}$$

Hence, for $i = 1, \dots, \frac{p-1}{2}$, we have $u_i = u_{p-i}$ and so

$$u = \sum_{i=1}^{\frac{p-1}{2}} u_i(\zeta^i + \zeta^{-i}).$$

We claim that each of the elements $\zeta^i + \zeta^{-i}$ are linear sums of powers of $\zeta + \zeta^{-1}$. We use an induction on i. For $i = 1$ there is nothing to prove. Suppose that the result is true up to a given i and consider the case $i + 1$. We have

$$(\zeta + \zeta^{-1})^{i+1} = \zeta^{i+1} + (i+1)\zeta^i\zeta^{-1} + \cdots + (i+1)\zeta\zeta^{-i} + \zeta^{-(i+1)},$$

from which we deduce

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

Using the induction hypothesis, we obtain that $\zeta^{i+1} + \zeta^{-(i+1)}$ is a linear sum of powers of $\zeta + \zeta^{-1}$. Thus we have proved the claim. It follows that u belongs to $\mathbf{Z}[\zeta + \zeta^{-1}]$ and we have the inclusion

$O_{K_0} \subset \mathbf{Z}[\zeta + \zeta^{-1}]$, as required. Thus $\mathbf{Q}(\zeta + \zeta^{-1})$ is a monogenic field.

We now turn to cubic number fields. This case is more complex than that of quadratic number fields. We will first show that the field $\mathbf{Q}(\sqrt[3]{2})$ is monogenic. To prove this we need a preliminary result.

Proposition 18.2 *Let $K = \mathbf{Q}(\alpha)$, with $\alpha \in O_K$, be such that $[K : \mathbf{Q}] = n$ and $f = m(\alpha, \mathbf{Q})$. If p is a prime number and f is Eisenstein at p, then $p \not| [O_K : \mathbf{Z}[\alpha]]$.*

PROOF Let

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

where $p|a_i$, for $i = 0, 1, \ldots, n-1$ and $p^2 \not| a_0$. We have

$$a_0 + a_1\alpha + \cdots + a_{n-1}\alpha^{n-1} + \alpha^n = 0 \Longrightarrow \mathbf{Z}[\alpha] = \mathbf{Z} + \mathbf{Z}\alpha + \cdots + \mathbf{Z}\alpha^{n-1}$$

and $\frac{\alpha^n}{p} \in \mathbf{Z}[\alpha]$. Also,

$$N_{K/\mathbf{Q}}(\alpha) = (-1)^n a_0 \not\equiv 0 \ (\mathrm{mod}\ p^2).$$

Suppose that $p|[O_K : \mathbf{Z}[\alpha]]$. Then there is an element of order p in the quotient group $O_K/\mathbf{Z}[\alpha]$. This means that there exists $x \in O_K$, but not in $\mathbf{Z}[\alpha]$, such that $px \in \mathbf{Z}[\alpha]$. Thus

$$px = b_0 + b_1\alpha + \cdots + b_{n-1}\alpha^{n-1},$$

with $b_i \in \mathbf{Z}$. As $x \notin \mathbf{Z}[\alpha]$, there is at least one b_i which is is not divisible by p. Let j be the smallest index with this property. So

$$y = x - \left(\frac{b_0}{p} + \frac{b_1}{p}\alpha + \cdots + \frac{b_{j-1}}{p}\alpha^{j-1}\right) = \frac{b_j}{p}\alpha^j + \frac{b_{j+1}}{p}\alpha^{j+1} + \cdots + \frac{b_{n-1}}{p}\alpha^{n-1}.$$

Because both x and $\frac{b_0}{p} + \frac{b_1}{p}\alpha + \cdots + \frac{b_{j-1}}{p}\alpha^{j-1}$ belong to O_K, y belongs to O_K and so this is the case for $y\alpha^{n-j-1}$. Now

$$y\alpha^{n-j-1} = \frac{b_j}{p}\alpha^{n-1} + \frac{\alpha^n}{p}\left(b_{j+1} + b_{j+2}\alpha + \cdots + b_{n-1}\alpha^{n-j-2}\right).$$

Since $\frac{\alpha^n}{p} \in \mathbf{Z}[\alpha] \subset O_K$, we have $\frac{b_j}{p}\alpha^{n-1} \in O_K$. Also, the norm of an algebraic integer is an integer, hence

$$|N_{K/\mathbf{Q}}(\frac{b_j}{p}\alpha^{n-1})| = \frac{b_j^n |N_{K/\mathbf{Q}}(\alpha)^{n-1}|}{p^n} = \frac{b_j^n |a_0|^{n-1}}{p^n} \in \mathbf{Z}.$$

However,

$$p \not| b_j \quad \text{and} \quad p^2 \not| a_0,$$

so $|N_{K/\mathbf{Q}}(\frac{b_j}{p}\alpha^{n-1})| \notin \mathbf{Z}$ and we have a contradiction. It follows that $p \not| [O_K : \mathbf{Z}[\alpha]]$. □

We are now in a position to show that the field $K = \mathbf{Q}(\sqrt[3]{2})$ is monogenic. From Theorem 17.1 we have

$$\mathrm{disc}(\mathbf{Z}[\sqrt[3]{2}]) = [O_K : \mathbf{Z}[\sqrt[3]{2}]]^2 \mathrm{disc}(O_K).$$

The polynomial $m(\sqrt[3]{2}, \mathbf{Q})$ has the form $f(X) = -2 + X^3$ and its discriminant is $-108 = -2^2.3^3$, so 2 and 3 are the only primes which could divide $[O_K : \mathbf{Z}[\sqrt[3]{2}]]$. As f is Eisenstein at 2, by Proposition 18.2, $2 \not| [O_K : \mathbf{Z}[\sqrt[3]{2}]]$. The number $1 + \sqrt[3]{2}$ is a root of the polynomial $g(X) = (-1+X)^3 - 2 = -3 + 3X - 3X^2 + X^3$, which is Eisenstein at 3, so $3 \not| [O_K : \mathbf{Z}[1 + \sqrt[3]{2}]]$. However, $\mathbf{Z}[1 + \sqrt[3]{2}] = \mathbf{Z}[\sqrt[3]{2}]$, so $3 \not| [O_K : \mathbf{Z}[\sqrt[3]{2}]]$. As both 2 and 3 do not divide $[O_K : \mathbf{Z}[\sqrt[3]{2}]]$, we must have $[O_K : \mathbf{Z}[\sqrt[3]{2}]] = 1$, i.e., $O_K = \mathbf{Z}[\sqrt[3]{2}]$ and K is monogenic.

Exercise 18.1 *Show that* $K = \mathbf{Q}(\sqrt[3]{5})$ *is monogenic.*

Remark We may generalize these results in the following way. If q is a prime such that $3|(1+q)$ and $3^2 \not|(1+q)$, then the field $\mathbf{Q}(\sqrt[3]{q})$ is monogenic. For example, $\mathbf{Q}(\sqrt[3]{11})$ and $\mathbf{Q}(\sqrt[3]{23})$ are monogenic. In this way we obtain a family of monogenic cubic fields. We may be tempted to think that all cubic number fields are monogenic. The following example, due to Dedekind, shows that this is not the case.

Proposition 18.3 *(Dedekind) If* θ *is a root of the polynomial* $f(X) = -8 - 2X - X^2 + X^3$*, then* $K = \mathbf{Q}(\theta)$ *is non-monogenic.*

PROOF First we calculate the discriminant of O_K. As the polynomial f has no root in $\mathbf{Q}$, f is irreducible over $\mathbf{Q}$. Let $\eta = \frac{\theta+\theta^2}{2}$. Then the set $S = \{1, \theta, \eta\}$ is independant over $\mathbf{Q}$. (If the set S is not independant, then θ is the root of rational polynomial of degree 2 and it follows that f is reducible over $\mathbf{Q}$.) Now $A = \mathbf{Z} \oplus \mathbf{Z}\theta \oplus \mathbf{Z}\eta$ is a free $\mathbf{Z}$-module of rank 3 contained in O_K, with basis S. To calculate the discriminant of A, we use the formula developped in Proposition 10.7, i.e., $\mathrm{disc}(A) = \det(\mathbf{X})$, where

$$\mathbf{X} = \begin{bmatrix} T_{K/\mathbf{Q}}(1) & T_{K/\mathbf{Q}}(\theta) & T_{K/\mathbf{Q}}(\eta) \\ T_{K/\mathbf{Q}}(\theta) & T_{K/\mathbf{Q}}(\theta^2) & T_{K/\mathbf{Q}}(\theta\eta) \\ T_{K/\mathbf{Q}}(\eta) & T_{K/\mathbf{Q}}(\eta\theta) & T_{K/\mathbf{Q}}(\eta^2) \end{bmatrix}.$$

To determine the elements of this matrix we first find the respective matrices M_θ and M_η of the applications $x \longmapsto \theta x$ and $x \longmapsto \eta x$ in the basis $\mathcal{B} = \{1, \theta, \theta^2\}$:

$$M_\theta = \begin{bmatrix} 0 & 0 & 8 \\ 1 & 0 & 2 \\ 0 & 1 & 1 \end{bmatrix} \qquad M_\eta = \begin{bmatrix} 0 & 4 & 8 \\ \frac{1}{2} & 1 & 6 \\ \frac{1}{2} & 1 & 2 \end{bmatrix}.$$

Multiplying these matrices we find those of the applications $x \longmapsto \theta^2 x$, $x \longmapsto \theta\eta x$ and $x \longmapsto \eta^2 x$: $M_{\theta^2} = M_\theta^2$, $M_{\theta\eta} = M_\theta M_\eta$ and $M_{\eta^2} = M_\eta^2$. We obtain

$$M_{\theta^2} = \begin{bmatrix} 0 & 8 & 8 \\ 1 & 2 & 10 \\ 1 & 1 & 3 \end{bmatrix} \qquad M_{\theta\eta} = \begin{bmatrix} 4 & 8 & 16 \\ 1 & 6 & 12 \\ 1 & 2 & 8 \end{bmatrix} \qquad M_{\eta^2} = \begin{bmatrix} 6 & 12 & 40 \\ \frac{7}{2} & 9 & 22 \\ \frac{3}{2} & 5 & 14 \end{bmatrix}.$$

Therefore

$$\mathbf{X} = \begin{bmatrix} 3 & 1 & 3 \\ 1 & 5 & 18 \\ 3 & 18 & 29 \end{bmatrix}$$

The determinant of $\mathbf{X}$ has the value -503, so the discriminant of A is -503. From Theorem 17.1 we have

$$\mathrm{disc}(A) = [O_K : A]^2 \mathrm{disc}(O_K).$$

As 503 is a prime number, we must have $[O_K : A] = 1$, i.e., the free groups O_K and A are the same. Thus any element $\alpha \in O_K$ can be written $a + b\theta + c\eta$, with $a, b, c \in \mathbf{Z}$. We aim to show that $\mathrm{disc}(\mathbf{Z}[\alpha])$ is even and so $O_K \neq \mathbf{Z}[\alpha]$. To begin with, we determine the matrix M_α of the application $x \longmapsto \alpha x$ in the basis $\mathcal{B}' = \{1, \theta, \eta\}$:

$$M_\alpha = \begin{bmatrix} a & 4c & 4b \\ b & a-b & 2c \\ c & 2b+2c & a+2b+3c \end{bmatrix}$$

Reducing modulo 2, we obtain

$$M_\alpha \equiv \begin{bmatrix} a & 0 & 0 \\ b & a-b & 0 \\ c & 0 & a+c \end{bmatrix} \pmod 2.$$

Then for the trace of the application $x \longmapsto \alpha^k x$ we have

$$\operatorname{tr} M_{\alpha^k} = \operatorname{tr}(M_\alpha^k) \equiv a^k + (a-b)^k + (a+c)^k \equiv a + (a-b) + (a-c) \equiv a - b + c \pmod 2.$$

We now set

$$\mathbf{Y} = \begin{bmatrix} \operatorname{tr}(1) & \operatorname{tr}(\alpha) & \operatorname{tr}(\alpha^2) \\ \operatorname{tr}(\alpha) & \operatorname{tr}(\alpha^2) & \operatorname{tr}(\alpha^3) \\ \operatorname{tr}(\alpha^2) & \operatorname{tr}(\alpha^3) & \operatorname{tr}(\alpha^4) \end{bmatrix}.$$

From Proposition 10.7, we have $\operatorname{disc}(\mathbf{Z}[\alpha]) = \det(\mathbf{Y})$. All the elements of $\mathbf{Y}$ are equivalent to $a-b+c \pmod 2$. If $a-b+c \equiv 0 \pmod 2$, then the the last column of the matrix $\mathbf{Y}$ is composed of even numbers, hence $\det(\mathbf{Y})$ is an even number. On the other hand, if $a-b+c \equiv 1 \pmod 2$, then all the elements of the matrix are odd. The determinant is composed of a sum of 3! products of 3 elements of the matrix, i.e., of a sum of 6 odd numbers, which is an even number. Therefore, in this case too, $\det(\mathbf{Y})$ is an even number. We have shown that $\operatorname{disc}(\mathbf{Z}[\alpha])$ is an even number. As $\operatorname{disc}(O_K)$ is odd, we cannot have $O_K = \mathbf{Z}[\alpha]$, i.e., K is not monogenic. □

Up to here we have only seen one example of a non-monogenic number field. We now turn to *biquadratic number fields* . (We recall that a number field is biquadratic if it is obtained by adjoining to $\mathbf{Q}$ the square roots of two square-free integers.) The family of such fields, which we will present, will provide us of infinite number of non-monogenic fields.

Let $d \neq 1$ be a square-free integer such that $d \equiv 1 \pmod 3$, then $m(\sqrt{d}, \mathbf{Q}) = -d + X^2$. Let us write f for this minimal polynomial. Reducing modulo 3 we obtain $\bar{f}(X) = (1+X)(-1+X)$, so from Dedekind's factorization theorem we obtain $O_{\mathbf{Q}(\sqrt{3})}3 = P_1P_2$, where P_1, P_2 are prime ideals in $O_{\mathbf{Q}(\sqrt{3})}$, i.e., 3 splits completely in $O_{\mathbf{Q}(\sqrt{3})}$.

Now let d_1, d_2 be distinct square-free integers such that $d_i \neq 1$ and $d_i \equiv 1 \pmod 3$, for $i = 1, 2$. From Theorem 13.12, the prime 3 splits completely in O_K, where $K = \mathbf{Q}(\sqrt{d_1}, \sqrt{d_2})$, i.e.,

$$O_K 3 = P_1P_2P_3P_4,$$

where the P_i are prime ideals in O_K. Suppose that there exists $\alpha \in O_K$ such that $O_K = \mathbf{Z}[\alpha]$; then $3 \nmid [O_K : \mathbf{Z}[\alpha]]$. If we set $f = m(\alpha, \mathbf{Q})$, then from Dedekind's factorization theorem we obtain

$$\bar{f}(X) = (-a_1 + X)(-a_2 + X)(-a_3 + X)(-a_4 + X),$$

where $\bar{f}$ denotes the reduction of f modulo 3 and $a_1, a_2, a_3, a_4 \in \mathbf{F}_3$. However, $\mathbf{F}_3$ contains only 3 distinct elements, a contradiction. It follows that $O_K \neq \mathbf{Z}[\alpha]$ and so K is not monogenic.

Example The number field $\mathbf{Q}(\sqrt{7}, \sqrt{10})$ is not monogenic.

More on biquadratic number fields can be found, for example, in the articles [9], [16]).

Remark Proposition 18.2 together with Theorem 17.2 may be used to prove the following result:

Proposition 18.4 *If $K = \mathbf{Q}(\alpha)$ and the polynomial minimal h is Eisenstein at p, then $\bar{h} = X^n$, so the factorization of $O_K p$ into prime ideals has the form $O_K = P^n$, i.e., p is totally ramified in O_K.*

PROOF We leave the proof as an exercise.

18.2 Properties of orders in a number ring

We recall that an order in a number ring K is a subring R of O_K whose index as a subgroup of O_K is finite. We know that O_K is a Dedekind domain, but what can we say of an order R which is a proper subring of O_K? It turns out that certain properties of O_K carry over to R, but not all. (Of course, we are primarily interested in orders of the form $\mathbf{Z}[\alpha]$, where $\mathbf{Z}[\alpha]$ is a proper subset of O_K.)

Proposition 18.5 *If R is an order, then R is noetherian.*

PROOF It is sufficient to show that every ideal in R is finitely generated. If I is the zero ideal, then there is nothing to prove, so let us suppose that this is not the case. Let I be a nonzero ideal. As I is a subgroup of O_K, I is a free group of rank at most that of O_K. Hence I has a finite basis, which implies that it is finitely generated. □

We now consider the fraction field of R. But first a preliminary result (not without interest). For an order R, we write $\mathbf{Q}R$ for the collection of sums of the form $\sum_{i=1}^k q_i r_i$, with $q_i \in \mathbf{Q}$ and $r_i \in R$.

Lemma 18.1 *Let K be a number field with ring of integers O_K. If R is an order in K, then $\mathbf{Q}O_K = \mathbf{Q}R = K$.*

PROOF First we show that $\mathbf{Q}O_K = K$. Clearly $\mathbf{Q}O_K \subset K$. Suppose now that $\alpha \in K$. As α is algebraic over $\mathbf{Q}$, from Lemma 11.2 there exists a positive integer k such that $k\alpha$ is an algebraic integer, i.e., $k\alpha \in O_K$. Hence $\alpha \in \mathbf{Q}O_K$ and so $K \subset \mathbf{Q}O_K$. As $\mathbf{Q}O_K \subset K$, we have an equality.

Now suppose that R is any order in O_K. As $R \subset O_K$, we have $\mathbf{Q}R \subset \mathbf{Q}O_K = K$. We now consider the reverse inclusion. There exists a basis $\{e_1, \ldots, e_n\}$ of O_K and positive integers $d_1, \ldots, d_n$ such that $\{d_1 e_1, \ldots, d_n e_n\}$ is a basis of R. Let $\alpha \in K$. From Lemma 11.2 there exists a positive integer k such that $k\alpha \in O_K$. Therefore we can find integers $k_1, \ldots, k_n$ such that

$$k\alpha = \sum_{i=1}^n k_i e_i = \frac{k_i}{d_i} d_i e_i \in \mathbf{Q}R \Longrightarrow \alpha \in \mathbf{Q}R.$$

Therefore $K \subset \mathbf{Q}R$ and it follows that $K = \mathbf{Q}R$. □

We recall that the fraction field of O_K is K. It turns out that this is also the case for any order in O_K.

Proposition 18.6 *Let $R \subset O_K$ be an order. Then the fraction field of R is K.*

PROOF Let us write $Frac(R)$ for the fraction field of R. If $\alpha \in K$, then, from Lemma 18.1, there exist $q_1, \ldots, q_k \in \mathbf{Q}$ and $r_1, \ldots, r_k \in R$ such that $\alpha = \sum_{i=1}^k q_i r_i$. We may write $q_i = \frac{a_i}{b_i}$, with $a_i, b_i \in \mathbf{Z}$ and $b_i \neq 0$. Then

$$\alpha = \sum_{i=1}^k \frac{a_i}{b_i} r_i = \sum_{i=1}^k \frac{a_i r_i}{b_i} \in Frac(R),$$

because both $a_i r_i$ and b_i belong to R. Thus $K \subset Frac(R)$. By definition $Frac(R) \subset K$, hence the equality $Frac(R) = K$. □

As O_K is a Dedekind domain, every nonzero prime ideal in O_K is maximal. This is also the case for orders.

Proposition 18.7 *If $R \subset O_K$ is an order, then every nonzero prime ideal is maximal.*

PROOF Let P be a nonzero prime ideal in R and a a nonzero element of P. Let $f = m(a, \mathbf{Q})$. Then $f(X) = \sum_{i=0}^{n-1} c_i X^i + X^m \in \mathbf{Z}[X]$. As f is minimal, $c_0 \neq 0$. Given that $f(a) = 0$, we have

$$-c_0 = c_1 a + \cdots + c_{n-1} a^{n-1} + a^n \Longrightarrow c_0 \in P.$$

The quotient R/P is a finitely generated $\mathbf{Z}$-module, such that $c_0(R/P) = 0$ ($c_0 \in P$). From the theorem of the decomposition of finitely generated modules over a P.I.D., we know that R/P is a direct sum of cyclic submodules [5]. As $c_0(R/P) = 0$, all these submodules must be finite and so R/P is finite. However, R/P is an integral domain and a finite integral domain is a field. It follows that P is a maximal ideal. □

Exercise 18.2 *In the proof of the above proposition we have used the fact that a finite integral domain is a field. Prove this statement.*

Up to here the properties of rings of integers have carried over to orders. However, one important property does not carry over and this prevents orders which are not rings of integers from being Dedekind domains. We recall that an integral domain R is normal if its integral closure in its field of fractions is R itself. This is so for rings of integers (Proposition 11.7), but is not true for other orders.

Theorem 18.1 *Let K be a number field, with ring of integers O_K. If R is an order in K and $R \neq O_K$, then R is not a normal domain.*

PROOF Since $R \neq O_K$, there exists $\beta \in O_K \setminus R$. As $O_K \subset Frac(O_K) = Frac(R)$, β lies in $Frac(R)$. Moreover, β is an algebraic integer, there exists a monic polynomial $f \in \mathbf{Z}[X] \subset R[X]$ such that $f(\beta) = 0$. Hence β lies in the integral closure of R. However, $\beta \notin R$, so the integral closure of R in its field of fractions is not R, i.e., R is not normal. □

Corollary 18.1 *An order R in a number field K is a Dedekind domain if and only if $R = O_K$.*

An important property of Dedekind domains is the expression of a nonzero fractional ideal as a unique product of powers of prime ideals, with positive powers for integral ideals. This property does not carry over to orders which are proper subrings of number rings.

Proposition 18.8 *Let K be a number field with ring of integers O_K. If the order R is a proper subset of O_K, then the unique factorization of fractional ideals fails.*

PROOF Suppose that R has the factorization property. We will show that this implies that every prime ideal is invertible. Let P be a prime ideal of R and a a nonzero element of P. By hypothesis

$$(a) = Q_1 \cdots Q_s,$$

where the Q_i are prime ideals in R. Then

$$R = Q_1(\frac{1}{a} Q_2 \cdots Q_s),$$

so Q_1 is invertible. In the same way, the ideals $Q_2, \ldots, Q_s$ are also invertible. If no Q_i is contained in P, then for each i there is an element $c_i \in Q_i$ which does not belong to P. However, the product $c_1 \cdots c_s \in P$, which is impossible because P is a prime ideal. Therefore, for some i, we have $Q_i \subset P$. As every nonzero prime ideal is maximal, we must have $Q_i = P$ and so P is invertible.

We now consider a nonzero fractional ideal I. By hypothesis we can write

$$I = P_1^{a_1} \cdots P_n^{a_n},$$

where the $a_1, \ldots a_n \in \mathbf{Z}$. Then I is invertible, with

$$I^{-1} = P_n^{-a_n} \cdots P_1^{-a_1}.$$

Thus every nonzero fractional ideal is invertible.

In the proof of Proposition 12.9 we showed that, if R is an integral domain such that every nonzero fractional ideal is invertible, then R is integrally closed in its fraction field, i.e., R is normal. From Theorem 18.1 we see that $R = O_K$, a contradiction. Therefore the factorization property does not apply to orders which are not maximal. □

18.3 Different of a number ring

We now return to the different, which we defined in Chapter 15 for a general Dedekind domain. We will be particularly interested in number rings and will first summarize the discussion of the different in this context.

The ring of integers $\mathbf{Z}$ is a Dedekind domain and $\mathbf{Q}$ is its field of fractions. (In the language of Chapter 15, $\mathbf{Z} = C$ and $\mathbf{Q} = K$.) Let L be a number field and O_L its ring of integers. O_L is the integral closure of $\mathbf{Z}$ in L. (In the language of Chapter 15, $O_L = D$.) We set

$$O_L^* = \{x \in L : T_{L/\mathbf{Q}}(xy) \in \mathbf{Z}, \forall y \in O_L\}.$$

From Proposition 15.3, O_L^* is a fractional ideal of O_L. We now set $\Delta(O_L|\mathbf{Z}) = O_L^{*-1}$. (To simplify the notation we will write Δ for $\Delta(O_L|\mathbf{Z})$. Δ is called the different of O_L over $\mathbf{Z}$, or simply the different of O_L. From Proposition 15.4 we know that Δ is an integral ideal of O_L.

The bilinear form defined on $L \times L$ by $(x, y) \longmapsto T_{L/\mathbf{Q}}(xy)$ is nondegenerate. If $\mathcal{B} = \{x_1, \ldots, x_n\}$ is an integral basis of O_L, then $\mathcal{B}$ is a basis of L over $\mathbf{Q}$. There is a basis $\mathcal{B}^* = \{x_1^*, \ldots, x_n^*\}$ of L over $\mathbf{Q}$ such that $T_{L/\mathbf{Q}}(x_i x_j^*) = \delta_{ij}$, where δ_{ij} is the Kronecker symbol. This second basis is called the dual basis of $\mathcal{B}$ and, from Proposition 15.2, is a basis of the free $\mathbf{Z}$-module O_L^*.

Different and discriminant

In this subsection our principal aim is to prove a relation between the discriminant and the different of a number ring O_L.

Theorem 18.2 *For a number ring O_L we have*

$$\|\Delta(O_L|\mathbf{Z})\| = |disc(O_L)|.$$

PROOF As O_L^* is a fractional ideal of O_L, there exists a nonzero element of α in O_L such that αO_L^* is an ideal of O_L. We claim that we may choose $\alpha \in \mathbf{N}^*$. As L is a finite extension of $\mathbf{Q}$, each x_i^* is algebraic over $\mathbf{Q}$. From Lemma 11.2, there is a positive integer α_i such that $\alpha_i x_i^*$ is an algebraic integer and so belongs to O_L. If $\alpha = \alpha_1 \cdots \alpha_n$, then $\alpha x_i^* \in O_L$, for all i, and it follows that $\alpha O_L^* \subset O_L$.

Now

$$\alpha O_L^* = \mathbf{Z}\alpha x_1^* + \cdots + \mathbf{Z}\alpha x_n^*.$$

Given that $\alpha x_i^* \in O_L$, we may write

$$\alpha x_i^* = \sum_{j=1}^n a_{ij} x_j \Longrightarrow x_i^* = \sum_{j=1}^n \frac{a_{ij}}{\alpha} x_j,$$

where the a_{ij} are rational numbers. Also, for $i = 1, \ldots, n$, we have

$$x_i = \sum_{j=1}^n b_{ij} x_j^*,$$

with the b_{ij} rational numbers. Let us set $A = (a_{ij})$, $A' = (\frac{a_{ij}}{\alpha})$ and $B = (b_{ij})$. These matrices have their components in $\mathbf{Q}$ and $A'B^t = I_n$, i.e., $B^t = A'^{-1}$. Then

$$T_{L/\mathbf{Q}}(x_i x_j) = T_{L/\mathbf{Q}}\left(\sum_{k=1}^n b_{ik} x_k^* x_j\right) = \sum_{k=1}^n b_{ik} T_{L/\mathbf{Q}}(x_k^* x_j) = b_{ij}.$$

Therefore, by Proposition 10.7,

$$\det(B) = \mathrm{disc}(O_L). \tag{18.1}$$

Now αO_L^* is an ideal in O_L and has the integral basis $\mathcal{B}' = \{\alpha x_1^*, \ldots, \alpha x_n^*\}$. Using Theorem 13.3 we obtain

$$\mathrm{disc}_{L/\mathbf{Q}}(\alpha x_1^*, \ldots, \alpha x_n^*) = \|\alpha O_L^*\|^2 \mathrm{disc}(O_L).$$

However, from Proposition 10.6 we also have

$$\mathrm{disc}_{L/\mathbf{Q}}(\alpha x_1^*, \ldots, \alpha x_n^*) = \det(A)^2 \mathrm{disc}(O_L),$$

which shows that

$$|\det(A)| = \|\alpha O_L^*\| \Longrightarrow |\det(A')| = \frac{\|\alpha O_L^*\|}{\alpha^n}.$$

Moreover,

$$\|\alpha O_L^*\| \|O_L^{*-1}\| = \|\alpha O_L^* O_L^{*-1}\| = \|(\alpha)\| = \alpha^n \Longrightarrow \|O_L^{*-1}\| = \frac{\alpha^n}{\|\alpha O_L^*\|}.$$

Since A' is the inverse of B^t, we have

$$\|O_L^{*-1}\| = |\det(B)| = |\mathrm{disc}(O_L)|,$$

where we have used the relation (18.1). □

Corollary 18.2 *If the discriminant of O_L is a prime, then Δ is a prime ideal.*

PROOF If $\mathrm{disc}(O_L)$ is equal to a prime number, then so is $\|\Delta(O_L|\mathbf{Z})\|$. From Proposition 13.5, Δ is a prime ideal. □

Factorizing the different

The different is an ideal and so has a factorization into prime ideals. Here we will be concerned with this factorization. We will first study some examples where the number field is monogenic before giving a more general result.

Some examples in the monogenic case

The goal of this paragraph is to provide the decomposition into prime ideals of the differents of the number rings of the cyclotomic fields $\mathbf{Q}(\zeta_p)$ and the quadratic field $\mathbf{Q}(\sqrt{10})$, using the tools which we have previously developped. In particular, we will reconsider Corollary 15.4. We may interpret this result in the context of number fields. Let L be a number field which is a normal extension of $\mathbf{Q}$. If L is monogenic, α a power generator and $f = \min(\alpha, \mathbf{Q})$, then $\Delta(O_L|\mathbf{Z}) = O_L(f'(\alpha))$.

We start with cyclotomic fields. Let ζ_p be a primitive pth root of unity and $L = \mathbf{Q}(\zeta_p)$. We know that L is monogenic and that the minimal polynomial $m(\zeta_p, \mathbf{Q})$ has the form $f(X) = \frac{-1+X^p}{-1+X} = 1 + X + \cdots + X^{p-1}$. Then

$$f'(X) = \frac{pX^{p-1}(-1+X) - (-1+X^p)}{(-1+X)^2} \Longrightarrow f'(\zeta_p) = \frac{p\zeta_p^{p-1}}{-1+\zeta_p}.$$

Since ζ_p^{p-1} is a unit, we find

$$\Delta = O_L \frac{p}{-1+\zeta_p}.$$

Moreover, in the proof of Proposition 11.10 (equation (11.2)) we saw that $O_{\mathbf{Q}(\zeta_p)}p = O_{\mathbf{Q}(\zeta_p)}(1-\zeta_p)^{p-1}$, therefore

$$\Delta = O_L(1-\zeta_p)^{p-2}. \tag{18.2}$$

From Section 13.9, $O_L(1-\zeta_p)$ is a prime ideal, so the expression (18.2) is the decomposition of Δ into prime ideals.

Now let us look at quadratic number fields. If $L = \mathbf{Q}(\sqrt{d})$, with $d \equiv 2, 3 \pmod 4$, then $O_L = \mathbf{Z}[\sqrt{d}]$ and the minimal polynomial $m(\sqrt{d}, \mathbf{Q})$ has the form $f(X) = -d + X^2$. It follows that $\Delta = O_L(2\sqrt{d})$. On the other hand, if $d \equiv 1 \pmod 4$, then $L = \mathbf{Q}(\frac{1+\sqrt{d}}{2})$ and $O_L = \mathbf{Z}[\frac{1+\sqrt{d}}{2}]$. In this case the minimal polynomial $m(\frac{1+\sqrt{d}}{2}, \mathbf{Q})$ has the form $f(X) = \frac{1-d}{4} - X + X^2$ and so $f'(X) = -1 + 2X$. Therefore $\Delta = O_L\sqrt{d}$.

Finding the factorization of the different may not be so easy as in the case of the cyclotomic field above. From Corollary 15.3 a nonzero prime ideal Q in O_L divides the different Δ if and only if Q lies over a prime which ramifies in O_L. Thus we can find the factors in the decomposition, but not necessarily their powers. Let us consider an example. Let $L = \mathbf{Q}(\sqrt{10})$. Then $\Delta = O_L(2\sqrt{10})$. The discriminant of O_L has the value $40 = 2^3 5$, so the primes which ramify in O_L are 2 and 5. As $O_L = \mathbf{Z}[\sqrt{10}]$, from Theorem 17.2, there exist prime ideals Q_2 and Q_5 in $\mathbf{Z}[\sqrt{10}]$ such that

$$\mathbf{Z}[\sqrt{10}]2 = Q_2^2 \qquad \text{and} \qquad \mathbf{Z}[\sqrt{10}]5 = Q_5^2.$$

Therefore Q_2 and Q_5 are the prime divisors of Δ and $e_{Q_2} = e_{Q_5} = 2$. In fact,

$$Q_2 = (2, \sqrt{10}) \qquad \text{and} \qquad Q_5 = (5, \sqrt{10}).$$

To see this, we notice that

$$\frac{\mathbf{Z}[\sqrt{10}]}{(2, \sqrt{10})} \simeq \mathbf{Z}_2 \qquad \text{and} \qquad \frac{\mathbf{Z}[\sqrt{10}]}{(5, \sqrt{10})} \simeq \mathbf{Z}_5,$$

hence $(2, \sqrt{10})$ and $(5, \sqrt{10})$ are maximal ideals, and therefore prime ideals. There is a unique prime ideal in $\mathbf{Z}[\sqrt{10}]$ dividing $\mathbf{Z}[\sqrt{10}]2$ and $(2, \sqrt{10})$ is such an ideal. Therefore $Q_2 = (2, \sqrt{10})$. In the same way $Q_5 = (5, \sqrt{10})$. In addition, the characteristics of $\frac{\mathbf{Z}[\sqrt{10}]}{Q_2}$ and $\frac{\mathbf{Z}[\sqrt{10}]}{Q_5}$ are respectively 2 and 5. From Theorem 15.5, as the characteristic of $\frac{\mathbf{Z}[\sqrt{10}]}{Q_5}$ (=5) does not divide $e_{Q_5}(= 2)$, we have $s_{Q_5} = e_{Q_5} - 1 = 2 - 1 = 1$. On the other hand, the characteristic of $\frac{\mathbf{Z}[\sqrt{10}]}{Q_2}(= 2)$ divides $e_{Q_2}(= 2)$ and so from Theorem 15.5 we can only deduce that $s_{Q_2} \geq e_{Q_2} - 1 = 2 - 1 = 1$, which of course we already know.

To determine s_{Q_2} we turn to Theorem 15.6. We recall the definition of the ramification groups in the context of number rings. We suppose that L is a finite normal extension of $\mathbf{Q}$, p a prime in $\mathbf{Z}$ and $Q \subset O_L$ a prime ideal lying over p. We set $G = Gal(L/\mathbf{Q})$. Then, for $i \in \mathbf{N}$, we define the ramification groups V_i by

$$V_i = \{\sigma \in G : \sigma(\alpha) \equiv \alpha \ (\text{mod}\ Q^{i+1})\ \forall \alpha \in O_L\}.$$

The particular case V_0 is called the inertia group. The V_i form a descending sequence and from Corollary 13.9 there is an index r such that $V_r = \{\text{id}\}$. From Theorem 15.6, if p is totally ramified in O_L and Q is the unique prime ideal in O_L lying over p, then

$$s_Q = \sum_{i=1}^{r-1} (|V_i| - 1).$$

Thus, in order to determine the value of s_{Q_2} we need to find the corresponding ramification groups V_i, i.e., the V_i with $G = Gal(\mathbf{Q}(\sqrt{10})/\mathbf{Q})$ and $Q = Q_2 = (2, \sqrt{10})$. The Galois group G has two elements, namely the identity and the automorphism σ for which $\sigma(\sqrt{10}) = -\sqrt{10}$. Hence V_i is equal to the Galois group or contains only the identity. The former will be the case if and only if $-\sqrt{10} \equiv \sqrt{10} \ (\text{mod}\ Q_2^{i+1})$, i.e., when $2\sqrt{10} \in Q_2^{i+1}$. This is the case for $i = 0, 1, 2$, but not for $i = 3$, because

$$(2, \sqrt{10})^4 = (\mathbf{Z}[\sqrt{10}]2)^2 = \mathbf{Z}[\sqrt{10}]4.$$

Therefore,

$$|V_0| = |V_1| = |V_2| = 2,\ |V_3| = 1 \Longrightarrow s_{Q_2} = (2 - 1) + (2 - 1) + (2 - 1) = 3.$$

To conclude

$$\Delta(O_{\mathbf{Q}(\sqrt{10})}|\mathbf{Z}) = (2, \sqrt{10})^3 (5, \sqrt{10}).$$

The non-monogenic case

If L is a monogenic field, then there exists an algebraic number $\alpha \in O_L$ such that $L = \mathbf{Q}(\alpha)$ and $O_L = \mathbf{Z}[\alpha]$. We have seen that in this case $\Delta(O_L|\mathbf{Z}) = O_L f'(\alpha)$, where $f = m(\alpha, \mathbf{Q})$. From Proposition 10.1, f is the characteristic polynomial of α, so we may say that Δ divides the principal ideal generated by the derivative of the characteristic polynomial of α evaluated at α. We may generalise this to the case of a field which is not monogenic.

Proposition 18.9 *Let L be a number field which is a normal extension of $\mathbf{Q}$ and not monogenic and $\alpha \in O_L$. If g is the characteristic polynomial of α, then $\Delta(O_L|\mathbf{Z})$ divides $O_L g'(\alpha)$.*

PROOF If $L \neq \mathbf{Q}(\alpha)$, then $[L : \mathbf{Q}(\alpha)] = r > 1$. From Proposition 10.1, $g = f^r$, where $f = m(\alpha, \mathbf{Q})$. It follows that $g'(\alpha) = 0$ and so $\Delta | O_L g'(\alpha)$.

Now suppose that $L = \mathbf{Q}(\alpha)$. Using Proposition 15.8 we have

$$\mathbf{Z}[\alpha] \subset O_L \Longrightarrow O_L^* \subset \mathbf{Z}[\alpha]^* \Longrightarrow \Delta^{-1} \subset \frac{1}{f'(\alpha)}\mathbf{Z}[\alpha] \subset \frac{1}{f'(\alpha)}O_L.$$

Taking inverses we obtain

$$O_L f'(\alpha) \subset \Delta \Longrightarrow \Delta | O_L f'(\alpha).$$

From Proposition 15.8, $g = f$ and hence the result. □

Chapter 19

Elementary class groups

The determination of class groups is not easy. In this chapter we identify class groups of some number fields in each case using a particular set of generators. We will certainly not be exhaustive. In Chapter 14, for a number field K of degree n over $\mathbf{Q}$, we defined the Minkowski bound

$$\lambda = \frac{n!}{n^n}\left(\frac{4}{\pi}\right)^s \sqrt{|\mathrm{disc}(O_K)|},$$

where $2s$ is the number of complex embeddings of K into $\mathbf{C}$. We observed that if λ is less than 2, then the class number must be 1, because every class contains a nonzero ideal J whose norm is less than λ. This is a sufficient condition, but is not necessary as we will presently show.

Let us look more closely into the structure of the class group. Each class contains a nonzero ideal J whose norm is bounded by λ. If P is a prime ideal in the decomposition of J, then, by Proposition 13.6, P contains a unique prime number p and $\|P\| = p^m$, for some $m \in \mathbf{N}^*$; clearly $p \leq \lambda$. Therefore the class group is generated by the classes of prime ideals P in O_K containing a prime $p \leq \lambda$. Certain of these classes may contain a principal ideal, in which case they are equal to the identity e, the class composed of principal ideals and we may eliminate them. Finally, we are left with the identity e alone, in which case the group is trivial, or a set of generators distinct from e and we look for relations between them. To understand the procedure we will look at some examples.

Example 1. $K = \mathbf{Q}(\sqrt{14})$

First we calculate the Minkowski bound:

$$\lambda = \frac{2!}{2^2}\sqrt{4.14} = \sqrt{14} \quad \text{and} \quad 3 < \sqrt{14} < 4,$$

so we look for prime ideals P containing 2 or 3.

There is a unique prime ideal P containing 3. Indeed, 3 belongs to P implies that P contains $O_K 3$. We set $f = m(\sqrt{14}, \mathbf{Q})$. Then $f(X) = -14 + X^2$ and the reduction modulo 3 of f is $f_2(X) = 1 + X^2$, which is irreducible. Then Theorem 17.2 ensures that $O_K 3$ is a prime ideal and so $P = O_K 3$. Thus there is a unique prime ideal containg 3, which we will note P_3. P_3 is clearly principal.

Now we consider prime ideals containing 2. In fact, there is only one such ideal P. Indeed, 2 belongs to P implies that P contains $O_K 2$. By Proposition 18.4 there exists a prime ideal

P_2 in O_K such that $O_K 2 = P_2^2$. Hence $P = P_2$. We claim that P_2 is principal. Since $2 = (4+\sqrt{14})(4-\sqrt{14})$, we may write

$$P_2^2 = O_K 2 = O_K(4+\sqrt{14})O_K(4-\sqrt{14}) \Longrightarrow P_2 = O_K(4+\sqrt{14}) = O_K(4-\sqrt{14}),$$

using the unique decomposition of ideals. Hence P_2 is principal.

As P_2 and P_3 are principal, the class number is 1, i.e., the class group is reduced to the identity. This example shows that the Minkowski bound may be greater than 2 and at the same time the class number 1.

Example 2. $K = \mathbf{Q}(\sqrt{-5})$

We calculate the Minkowski bound:

$$\lambda = \frac{2!}{2^2}(\frac{4}{\pi})^1\sqrt{4.5} = \frac{2}{\pi}\sqrt{20} = \frac{4}{\pi}\sqrt{5} \quad \text{and} \quad 2 < \frac{4}{\pi}\sqrt{5} < 3.$$

The only prime we need to consider is 2. We set $f = m(\sqrt{-5}, \mathbf{Q})$. Then $f(X) = 5 + X^2$. The reduction modulo 2 of f is $f_2(X) = 1 + X^2 = (1+X)^2$, so there is a prime ideal P_2 in O_K such that $O_K 2 = P_2^2$. Thus there is a unique prime ideal lying over 2. This implies that the class group is cyclic. We now determine its order, which must be 1 (if P_2 is principal) or 2.

We claim that P_2 is not principal. If P_2 is principal, then we can write

$$P_2 = O_K(a+b\sqrt{-5}) \Longrightarrow P_2^2 = O_K(a+b\sqrt{-5})^2 \Longrightarrow 2 = (a+b\sqrt{-5})^2 u,$$

where u is a unit in O_K. Taking norms we obtain

$$N_{K/\mathbf{Q}}(2) = N_{K/\mathbf{Q}}(a+b\sqrt{-5})^2 N_{K/\mathbf{Q}}(u) \Longrightarrow 4 = \pm(a^2+5b^2)^2,$$

which is impossible with $a, b \in \mathbf{Z}$. Hence P_2 is not principal and we have two distinct classes, i.e., the class group is cyclic of order 2.

If the class number is prime, then we know that the class group is cyclic. On the other hand, if the class number is greater than 1 and not prime, then we need to find the distinct classes and study the relation between them.

Example 3. $K = \mathbf{Q}(\sqrt{-14})$

We calculate the Minkowski bound:

$$\lambda = \frac{2!}{2^2}(\frac{4}{\pi})^1\sqrt{4.14} = \frac{4}{\pi}\sqrt{14} \quad \text{and} \quad 4 < \frac{4}{\pi}\sqrt{14} < 5.$$

We need to consider the primes less than 5, namely 2 and 3.

There is a unique prime ideal P containing 2. Let $f = m(\sqrt{-14}, \mathbf{Q})$. Then $f(X) = 14 + X^2$. The polynomial f is Eisenstein at 2, so there is a prime ideal P_2 such that $O_K 2 = P_2^2$ and it follows that $P = P_2$.

The situation is different for 2. In fact, there are two prime ideals containing 3. The reduction of f modulo 3 is $f_3(X) = -1 + X^2 = (-1+X)(1+X)$, therefore there are prime ideals P_3 and P_3' such that $O_K 3 = P_3 P_3'$. Thus the class group is generated by the classes $[P_2]$, $[P_3]$ and $[P_3']$. However, the product $P_3 P_3'$ is a principal ideal, hence $[P_3'] = [P_3]^{-1}$ and we may neglect $[P_3']$: the class group is generated by $[P_2]$ and $[P_3]$.

We claim that P_2 and P_3 are not principal. If P_2 is principal, then there exist $a, b \in \mathbf{Z}$ such that

$$2 = (a + b\sqrt{-14})^2 u$$

where u is a unit. Taking norms we find

$$4 = \pm(a^2 + 14b^2)^2,$$

which is impossible, therefore P_2 is not principal. Suppose now that P_3 is principal, with $P_3 = O_K(a + b\sqrt{-14})$. There must be an element $c + d\sqrt{-14} \in P_3'$ such that

$$3 = (a + b\sqrt{-14})(c + d\sqrt{-14}).$$

Taking norms we find

$$9 = (a^2 + 14b^2)(c^2 + 14d^2),$$

which is impossible. So P_3 is not principal.

We now investigate the relation between the classes $[P_2]$ and $[P_3]$. We consider the principal ideal $I = O_K(2 + \sqrt{-14})$. As $\|I\| = N_{K/\mathbf{Q}}(2 + \sqrt{-14}) = 18 = 2.3^2$, there must be a prime ideal containing 3 which divides I, i.e., P_3 divides I or P_3' divides I. However, P_3 and P_3' cannot both divide I. If this is the case, then their product $O_K 3$ divides I, which implies that 3 is a multiple of $2 + \sqrt{-14}$ (in O_K), which is not the case. Therefore only P_3 or P_3' can divide I. Without loss of generality, let us suppose that P_3 divides I. We also notice that $\|P_3\| = 3$, because $\|O_K 3\| = N_{K/\mathbf{Q}}(3) = 9$ and $\|O_K 3\| = \|P_3\|\|P_3'\|$.

Since

$$[P_2][P_3]^2 = e \Longrightarrow [P_3]^2 = [P_2]^{-1} = [P_2],$$

the class group is generated by $[P_3]$ and is cyclic. Also,

$$[P_3]^4 = [P_2]^2 = e \quad \text{and} \quad [P_3]^2 = [P_2] \neq e,$$

so the order of the group is 4.

Our next example provides a group of order 4 which is not cyclic.

Example 4. $K = \mathbf{Q}(\sqrt{-30})$

We begin by calculating the Minkowski bound:

$$\lambda = \frac{2!}{2^2}(\frac{4}{\pi})^1\sqrt{4.30} = \frac{4}{\pi}\sqrt{30} \quad \text{and} \quad 6 < \frac{4}{\pi}\sqrt{30} < 7.$$

We consider the primes 2, 3 and 5. There are unique prime ideals P_2, P_3 and P_5, containing respectively 2, 3 and 5.

We set $f = m(\sqrt{-30}, \mathbf{Q})$. Then $f(X) = 30 + X^2$. The polynomial f is Eisenstein at each of the primes 2, 3 and 5, hence there are prime ideals P_2, P_3 and P_5 in O_K such that

$$O_K 2 = P_2^2 \qquad O_K 3 = P_3^2 \qquad O_K 5 = P_5^2.$$

We claim that P_2, P_3 and P_5 are not principal. For example, if P_2 is principal, than there exist $a, b \in \mathbf{Z}$ such that $P_2 = O_K(a + b\sqrt{-30})$ and so

$$O_K(a + b\sqrt{-30})^2 = O_K 2 \Longrightarrow (a + b\sqrt{-30})^2 u = 2,$$

where u is a unit. Taking norms we obtain

$$N_{K/\mathbf{Q}}(2) = \pm N_{K/\mathbf{Q}}((a+b\sqrt{-30})^2) \Longrightarrow 4 = \pm(a^2+30b^2)^2,$$

which is impossible. Thus P_2 is not principal; we show in an analogous manner that P_3 and P_5 are not principal. Therefore each of the elements $[P_2]$, $[P_3]$ and $[P_5]$ are of order 2 in the class group.

Next we notice that

$$P_2|O_K2, \;\; P_3|O_K3, \;\; P_5|O_K5 \Longrightarrow P_2P_3P_5|O_K30,$$

hence there exists an ideal Q such that $P_2P_3P_5Q = O_K30$. Taking norms we find

$$2.3.5\|Q\| = 30 \Longrightarrow \|Q\| = 1 \Longrightarrow P_2P_3P_5 = O_K30.$$

Therefore

$$[P_2][P_3][P_5] = e \Longrightarrow [P_2][P_3] = [P_5]^{-1} = [P_5],$$

which implies that the group is generated by $[P_2]$ and $[P_3]$.

Our next step is to show that $[P_2]$ and $[P_3]$ are distinct. If $[P_2] = [P_3]$, then $[P_5] = [P_2]^2 = e$, which is false. Hence $[P_2] \neq [P_3]$ and so the group is generated by two distinct elements of order 2 and thus is isomorphic to a product of two cyclic groups of order 2.

We now consider a cubic number field, for which we will use some new ideas.

Example 5. $K = \mathbf{Q}(\sqrt[3]{2})$

We have already seen that the field K is monogenic. As usual we determine the Minkowski bound. There are three monomorphisms from K into $\mathbf{C}$, namely the identity, which is real, and a pair of complex embeddings. We have

$$\lambda = \frac{3!}{3^3}(\frac{4}{\pi})^1\sqrt{108} = \frac{8}{9\pi}\sqrt{4.9.3} = \frac{16}{3\pi}\sqrt{3} \quad \text{and} \quad 6 < \frac{16}{\pi}\sqrt{3} < 7.$$

Thus we consider the primes 2, 3 and 5. There is a unique prime ideal P_2 (resp. P_3) containing 2 (resp. 3) and two prime ideals, P_5 and P_5', containg 5.

Let $f = m(\sqrt[3]{2}, \mathbf{Q})$. Then $f(X) = -2 + X^3$. As f is Eisenstein at 2, there exists a prime ideal P_2 in O_K such that $O_K2 = P_2^3$.

The reduction of f modulo 3 is $f_3(X) = 1 + X^3 = (1+X)^3$, so there exists a prime ideal P_3 in O_K such that $O_K3 = P_3^3$.

The reduction of f modulo 5 is $f_5(X) = -2 + X^3 = (-3+X)(-1+3X+X^2)$. As $g_2(X) = -1 + 3X + X^2$ has no root in $\mathbf{F}_5$, g_2 is irreducible, hence there exist prime ideals P_5, P_5' in O_K such that that $O_K5 = P_5P_5'$.

We claim that the prime ideals P_2, P_3, P_5 and P_5' are all principal. We set $\alpha = \sqrt[3]{2}$. Then

$$8 = \|O_K2\| = \|O_K\alpha\|^3 \Longrightarrow \|O_K\alpha\| = 2.$$

From Proposition 13.4 $O_K\alpha$ is a prime ideal. Given that P_2 is the unique prime ideal in O_K lying over 2, we have $P_2 = O_K\alpha$, i.e., P_2 is a principal ideal, as asserted.

For P_3 we proceed in a similar manner. We have

$$27 = \|O_K3\| = \|O_K(1+\alpha)\|^3 \Longrightarrow \|O_K(1+\alpha)\| = 3.$$

Hence $O_K(1+\alpha)$ is a prime ideal. Given that P_3 is the unique prime ideal in O_K lying over 3, we have $P_3 = O_K(1+\alpha)$, i.e., P_3 is a principal ideal.

Before considering P_5 and P_5' we will establish a preliminary result.

Lemma 19.1 *If $K = \mathbf{Q}(\beta)$, $f = m(\beta, \mathbf{Q})$, $\deg(f) = d$ and $r \in \mathbf{Q}$, then $f(r) = (-1)^d N_{K/\mathbf{Q}}(\beta - r)$.*

PROOF First we notice that

$$f(X) = (-\beta_1 + X)(-\beta_2 + X)\cdots(-\beta_d + X),$$

where the β_i are the conjugates of β. It follows that

$$f(X+r) = (-\beta_1 + r + X)(-\beta_2 + r + X)\cdots(-\beta_d + r + X).$$

As $f(X+r) = m(\beta - r, \mathbf{Q})$, the elements $\beta_1 - r, \ldots, \beta_d - r$ are the conjugates of $\beta - r$ and so, using Corollary 10.1, we have

$$f(r) = (-\beta_1 + r)(-\beta_2 + r)\cdots(-\beta_d + r) = (-1)^d N_{K/\mathbf{Q}}(\beta - r),$$

as required. □

Now we turn to P_5 and P_5'. We suppose that P_5 corresponds to the factor $g_1(X) = -3 + X$ and P_5' corresponds to g_2. Then $\|P_5\| = 5$ and $\|P_5'\| = 25$. From Lemma 19.1 we obtain

$$N_{K/\mathbf{Q}}(\alpha + 2) = N_{K/\mathbf{Q}}(\alpha - (-2)) = (-1)^3(-2 + (-2)^3) = 10 \Longrightarrow O_K(2+\alpha) = P_5 O_K \alpha,$$

because P_5 and $O_K\alpha$ are the only prime ideals in O_K with respective norms 5 and 2. Therefore

$$P_5 = O_K(2+\alpha)O_K(\frac{1}{\alpha}) = O_K(\frac{2}{\alpha} + 1) = O_K(\alpha^2 + 1).$$

We have shown that P_5 is principal. Now we consider P_5'. We have

$$O_K 5 = O_K(1+\alpha^2)P_5' = (1+\alpha^2)P_5',$$

so, from Lemma 12.3, P_5' is principal.

As P_2, P_3, P_5 and P_5' are all principal, the class group is trivial.

The following proposition summarizes the previous calculations:

Proposition 19.1 *We have:*

- *The ideal class group of $\mathbf{Q}(\sqrt{14})$ is trivial, hence the number ring of $\mathbf{Q}(\sqrt{14})$ is a PID;*
- *The ideal class group of $\mathbf{Q}(\sqrt{-5})$ is isomorphic to the cyclic group of order 2 C_2;*
- *The ideal class group of $\mathbf{Q}(\sqrt{-14})$ is isomorphic to the cyclic group of order 4 C_4;*
- *The ideal class group of $\mathbf{Q}(\sqrt{-30})$ is isomorphic to the product $C_2 \times C_2$;*
- *The ideal class group of $\mathbf{Q}(\sqrt[3]{2})$ is trivial, hence the number ring of $\mathbf{Q}(\sqrt[3]{2})$ is a PID.*

There are various problems raised by the class number of a number field, some of which were originally considered by Gauss. Probably the most well-known of these is the Gauss Class Number Problem, namely to determine the imaginary quadratic number fields with class number 1. Gauss supposed that there were only nine such number fields: $\mathbf{Q}(\sqrt{k})$, with $k = -1, -2, -3, -7, -11, -19, -43, -67, -163$. This was subsequently proved in the 20th century (long after Gauss). There has also been work on determining the imaginary quadratic number fields with class number n, for certain other n.

Another question raised by Gauss is known as the Gauss Conjecture, namely $h(\mathbf{Q}(\sqrt{-d})) \to +\infty$ as $d \to +\infty$, where $h(\mathbf{Q}(\sqrt{-d}))$ denotes the class number of the number field $\mathbf{Q}(\sqrt{-d})$. This too was only proved in the 20th century. This result shows that there can only be a finite number of imaginary quadratic number fields with a fixed class number.

Gauss also conjectured that there is an infinite number of real quadratic number fields of class number 1. This has yet to be proved (or disproved).

Chapter 20

The distribution of ideals

Let K be a number field of degree n over $\mathbf{Q}$. For each real number $d > 0$, we note $i(d)$ the number of nonzero ideals I in O_K with $\|I\| \leq d$, which is finite by Theorem 13.5. For each ideal class C we write $i_C(d)$ for the number of ideals I in C such that $\|I\| \leq d$. In addition, Theorem 14.4 ensures that there is a finite number of ideal classes and so $i(d) = \sum_C i_C(d)$. We aim to show that there is a constant k, independant of C, such that

$$i_C(d) = kd + O(d^{1-\frac{1}{n}}). \tag{20.1}$$

We will refer to this equation as the *ideal counting equation*. If h_K is the class number, then

$$i(d) = h_K kd + O(d^{1-\frac{1}{n}}). \tag{20.2}$$

Our treatment of the question is inspired from that in [15].

20.1 Transformation of the problem

We consider a class C and fix an ideal $J \in C^{-1}$. Let A be the set of nonzero ideals in C with $\|I\| \leq d$. We define an application ϕ on A by multiplication by J, i.e., for $I \in A$, we set $\phi(I) = IJ$. From Corollary 12.1 the mapping ϕ is injective. Let B be the image of ϕ. We claim that B is the set of nonzero principal ideals $(\alpha) \subset J$ satisfying the inequality $\|(\alpha)\| \leq d\|J\|$. There is no difficulty in seeing that IJ is a nonzero ideal included in J and, by the choice of J, IJ is principal. If $IJ = (\alpha)$, then

$$\|(\alpha)\| = \|IJ\| = \|I\|\|J\| \leq d\|J\|.$$

Finally, suppose that (α) is a nonzero principal ideal included in J with $\|(\alpha)\| \leq d\|J\|$. Then J divides (α), so there exists an ideal I such that $IJ = (\alpha)$. In addition,

$$\|I\|\|J\| = \|IJ\| = \|(\alpha)\| \leq d\|J\|,$$

from which we deduce that $\|I\| \leq d$. This concludes the proof of our claim concerning B.

To determine $i_C(d)$, the number of elements in A, given that there is a bijection from A onto B, we may count the number of elements in B. We notice that two nonzero principal ideals (α) and (β) are the same if and only if β is a multiple of α by a unit.

Let D be any set of coset representatives of $U = U_K$ in O_K^*. The cardinal of B is then the cardinal of the set of elements α in D such that $\alpha \in J$ and $|N_{K/\mathbf{Q}}(\alpha)| \leq d\|J\|$. Instead of using the set D to determine $|B|$, we proceed indirectly.

Dirichlet's unit theorem (Theorem 14.6) ensures that

$$U = W \times V,$$

where W is the group of roots of unity of K and V a subgroup of U generated by a fundamental system of $t = r + s - 1$ units. We set $w = |W|$. Let D' be any set of coset representatives of V in O_K^*. Then $w|B|$ is the cardinal of the set of α in D' such that $\alpha \in J$ and $|N_{K/\mathbf{Q}}(\alpha)| \leq d\|J\|$. Thus to determine $|B|$ we calculate $w|B|$.

20.2 Preliminary results

We begin with an elementary group result.

Lemma 20.1 *Let G be a commutative semigroup and G' an abelian group. We suppose that $f : G \longrightarrow G'$ is multiplicative, i.e., $f(xy) = f(x)f(y)$, for $x, y \in G$, and that S is a group included in G. Also, we suppose that f restricted to S is an isomorphism onto its image S' in G'. If D' is a set of coset representatives of S' in G', then $D = f^{-1}(D')$ is a set of coset representatives of S in G. If f is injective, then there is a bijection of D' onto D.*

PROOF Let $z \in G$ and consider the coset zS. As $f(z)S'$ is a coset of S' in G', there exists $x' \in D'$ such that $f(z)S' = x'S'$. Thus there exists $w' \in S'$ such that $f(z)w' = x'$. However, there exists $w \in S$ such that $f(w) = w'$ and so $f(z)w' = f(z)f(w) = f(zw)$. Hence $zw \in f^{-1}(D') = D$. Therefore zS has a representative in D.

Suppose now that there are two elements $x, y \in D$ representing the same coset zS. Then $x = zw_1$ and $y = zw_2$, with $w_1, w_2 \in S$ and we have

$$f(zw_1) = f(z)f(w_1) \qquad \text{and} \qquad f(zw_2) = f(z)f(w_2).$$

Since $f(w_1)$ and $f(w_2)$ lie in S', $f(zw_1)$ and $f(zw_2)$ represent the same coset of S' in G'. Let x' be the representative of this coset in D'. Then

$$f(zw_1) = x' = f(zw_2) \Longrightarrow f(w_1) = f(w_2).$$

As f restricted to S is an isomorphism, we have $w_1 = w_2$. Thus there is a unique representative of the coset zS in D.

Suppose now that f is injective and let $x' \in D'$. If $x_1, x_2 \in f^{-1}(x')$, then $f(x_1) = x' = f(x_2)$. As f is injective, we have $x_1 = x_2$. Thus the mapping $\phi : D' \longrightarrow D, x' \longmapsto f^{-1}(x')$ is well-defined. There is no difficulty in seeing that ϕ is bijective. $\square$

Remark As a group is a semigroup, we may replace semigroup G by group G in the statement of the lemma.

For the second result we need some definitions. Let $[0, 1]^{n-1}$ denote the unit cube in $\mathbf{R}^{n-1}$. A function

$$f : [0, 1]^{n-1} \longrightarrow \mathbf{R}^n$$

is said to be *Lipschitz* if there is a constant κ, referred to as a Lipschitz constant, such that

$$\|f(x) - f(y)\| \leq \kappa\|x - y\|,$$

for all $x, y \in [0,1]^{n-1}$, where $\|\cdot\|$ denotes the length in $\mathbf{R}^{n-1}$ or $\mathbf{R}^n$. If B is a nonempty bounded region in $\mathbf{R}^n$, then we say that the boundary ∂B of B is $(n-1)$-*Lipschitz parametrizable*, or *Lipschitz*, if it can be covered by the images of a finite number of Lipschitz functions $f : [0,1]^{n-1} \longrightarrow \mathbf{R}^n$.

Lemma 20.2 *Let Λ be a lattice in $\mathbf{R}^n$ and B a bounded set in $\mathbf{R}^n$ whose boundary is $(n-1)$-Lipschitz parametrizable. Then*

$$|\Lambda \cap aB| = \frac{\mathrm{vol}\, B}{\det \Lambda} a^n + O(a^{n-1}),$$

for a sufficiently large a.

PROOF Let us first suppose that $\Lambda = \mathbf{Z}^n$. We will call a translate of the unit cube $[0,1]^n$ whose centre is a point z of $\mathbf{Z}^n$ an n-cube. We will write $C(z)$ for such a cube. An n-cube contains a unique lattice point, namely its centre, and has volume 1. We may divide the n-cubes intersecting aB into two classes, namely those containing no boundary points of aB and those containing boundary points of aB. We will write X for the set of n-cubes of the first type and Y for the set of n-cubes of the second type.

Together the sets X and Y form a covering of aB and so we have the the relation

$$\mathrm{vol}\, aB \leq |X| + |Y|.$$

In addition, a lattice point in aB must lie either in an n-cube in X or in an n-cube in Y. This implies that

$$|\mathbf{Z}^n \cap aB| \leq |X| + |Y|.$$

Putting these two relations together, we obtain

$$-|Y| \leq |X| - \mathrm{vol}\, aB \leq 0 \leq |\mathbf{Z}^n \cap aB| - |X| \leq |Y|,$$

from which we deduce

$$-|Y| \leq |\mathbf{Z}^n \cap aB| - \mathrm{vol}\, aB \leq |Y| \quad \text{or} \quad ||\mathbf{Z}^n \cap aB| - \mathrm{vol}\, aB| \leq |Y|.$$

We aim now to estimate $|Y|$. Unfortunately this is a quite arduous. The boundary of B is covered by a finite number of sets of the form $f([0,1]^{n-1})$, where f is a Lipschitz function. We may suppose that the functions all have the same Lipschitz constant κ (by taking, for example, the maximum of the constants). Then the boundary of aB is covered by the sets $af([0,1]^{n-1})$. We suppose that $a \geq 1$ and subdivide the cube $[0,1]^{n-1}$ into $\lfloor a \rfloor^{n-1}$ subcubes S. The subcubes have side length $\frac{1}{\lfloor a \rfloor}$. If $x = (x_1, \ldots, x_{n-1}) \in [0, \frac{1}{\lfloor a \rfloor}]^{n-1}$, then

$$x_1^2 + \cdots + x_{n-1}^2 \leq \frac{n-1}{\lfloor a \rfloor^2} \Longrightarrow \|x\| \leq \frac{\sqrt{n-1}}{\lfloor a \rfloor},$$

so the largest distance between two points in $f(S)$ is $\kappa \frac{\sqrt{n-1}}{\lfloor a \rfloor}$. This is the same for any of the small cubes S (by translation). It follows that the distance between two points in $af(S)$ is at most $a\kappa \frac{\sqrt{n-1}}{\lfloor a \rfloor} < 2\kappa\sqrt{n-1}$, because

$$1 \leq a < \lfloor a \rfloor + 1 \Longrightarrow \frac{a}{\lfloor a \rfloor} < 1 + \frac{1}{\lfloor a \rfloor} \leq 2.$$

Thus we have a bound on the distance between pairs of points in $af(S)$.

Our next step is to find a bound on the number of n-cubes $C(z)$ intersecting $af(S)$. We fix a subcube S and take a point $x \in af(S)$. To simplify the notation, we set $h = 2\kappa\sqrt{n-1}$. The closed ball of radius h centered on x, which we note $B(x,h)$, contains $af(S)$ and intersects a number of n-cubes bounded by $\mu = (2(h+\sqrt{n}))^n$. This last point needs an explanation. If $B(r,y)$ is a closed ball in $\mathbf{R}^n$, then

$$\text{vol } B(r,y) = \frac{\pi^{\frac{n}{2}} r^n}{\Gamma(\frac{n}{2}+1)} = \frac{(\sqrt{\pi}r)^n}{\Gamma(\frac{n}{2}+1)},$$

where Γ denotes Euler's gamma function. Now

$$\Gamma(\frac{n}{2}+1) = \begin{cases} k! & \text{if } n = 2k, \\ \frac{(2k+2)!}{(k+1)!4^{k+1}}\sqrt{\pi} & \text{if } n = 2k+1. \end{cases}$$

Thus, for $n \geq 2$ we have $\Gamma(\frac{n}{2}+1) \geq 1$, and so vol $B(r,y) \leq (\sqrt{\pi}r)^n$. Now let $C(z)$ be an n-cube intersecting $B(x,h)$. Since the distance between two points in $C(z)$ is at most $\sqrt{n}$, if $y \in C(z)$, then $\|y - x\| \leq h + \sqrt{n}$, which implies that $C(z) \subset B(x, h+\sqrt{n})$. As

$$\text{vol } B(x, h+\sqrt{n}) \leq (\sqrt{\pi}(h+\sqrt{n}))^n < (2(h+\sqrt{n}))^n,$$

the number of n-cubes intersecting $B(x,h)$ is bounded by $\mu = (2(h+\sqrt{n}))^n$, as claimed. Since $af(S) \subset B(x,h)$, the number of n-cubes intersecting $af(S)$ is also bounded by μ.

To conclude, we find a bound on the number of n-cubes intersecting the boundary $\partial(aB)$. Since there are $\lfloor a \rfloor^{n-1}$ cubes S, the boundary $\partial(aB)$ intersects at most $\mu\lfloor a \rfloor^{n-1}$ n-cubes. Given that $\lfloor a \rfloor \leq a$, the number of n-cubes intersecting $\partial(aB)$ is bounded by μa^{n-1}, i.e., $|Y|$ is bounded by μa^{n-1}. Hence we may write

$$|\mathbf{Z}^n \cap aB| - \text{vol } aB| \leq |Y| \leq \mu a^{n-1},$$

where μ is a constant which is independant of a. From this we deduce

$$|\mathbf{Z}^n \cap aB| = \text{vol } aB + (|\mathbf{Z}^n \cap aB| - \text{vol } aB) = \text{vol } aB + O(a^{n-1}).$$

Since $\det \mathbf{Z}^n = 1$ and vol $aB = a^n$vol B, we have

$$|\mathbf{Z}^n \cap aB| = \frac{\text{vol } B}{\det \mathbf{Z}^n} a^n + O(a^{n-1}),$$

as required.

We now consider the case where Λ is a general lattice in $\mathbf{R}^n$. There exists a linear automorphism L sending Λ onto $\mathbf{Z}^n$. Let $B' = L(B)$. We notice that $\partial B' = L(\partial B)$. If $f : [0,1]^{n-1} \longrightarrow \mathbf{R}^n$ is a Lipschitz mapping with constant κ, then $L \circ f$ is also Lipschitz with Lipschitz constant $\|L\|\kappa$. If ∂B is covered by the images of the Lipschitz mappings $f_1, \ldots, f_m$, then $\partial B'$ is covered by the images of the Lipschitz mappings $L \circ f_1, \ldots, L \circ f_m$. Then,

$$\mathbf{Z}^n \cap aB' = L(\Lambda) \cap aL(B) = L(\Lambda \cap aB) \Longrightarrow |\mathbf{Z}^n \cap aB'| = |\Lambda \cap aB|$$

and

$$
\begin{aligned}
|\Lambda \cap aB| &= \frac{\text{vol } B'}{\det \mathbf{Z}^n} a^n + O(a^{n-1}) \\
&= \frac{\text{vol } L(B)}{\det L(\Lambda)} a^n + O(a^{n-1}) \\
&= \frac{\text{vol } B}{\det \Lambda} a^n + O(a^{n-1}),
\end{aligned}
$$

as required. (To pass from the second line to the third, we have used Proposition G.2.) □

20.3 Proof of the ideal counting equation: first steps

From Section 20.1 we need to find a set D' of coset representatives α of V in O_K^* and determine the cardinal of those $\alpha \in D'$ which belong to J and satisfy the norm condition $|N_{K/\mathbf{Q}}(\alpha)| \leq d\|J\|$. In fact, we will 'deplace' the problem to another context.

We define the mapping $\mu : O_K^* \longrightarrow \mathbf{R}^{*r} \times \mathbf{C}^{*s}$ by

$$\mu(\alpha) = (\sigma_1(\alpha), \ldots, \sigma_r(\alpha), \tau_1(\alpha), \ldots, \tau_s(\alpha)).$$

Then μ is a semigroup homomorphism, which is also injective. Let V' be the image of V in $\mathbf{R}^{*r} \times \mathbf{C}^{*s}$ and Y a set of coset representatives of $V' = \mu(V)$ in $\mathbf{R}^r \times C^s$. By Lemma 20.1, $X = \mu^{-1}(Y)$ is a set of coset representatives of V in O_K^*. However, we have two conditions on X to take into account, namely

- 1. the norm condition $|N_{K/\mathbf{Q}}(\alpha)| \leq d\|J\|$;
- 2. the inclusion of α in J.

From Lemma 14.1, $S(y) = N_{K/\mathbf{Q}}(\alpha)$, where $y = \mu(\alpha)$, so we may take into account the norm condition by imposing that $|S(y)| \leq d\|J\|$. For the second condition we consider $\mathbf{R}^{*r} \times \mathbf{C}^{*s}$ as a subset of $\mathbf{R}^n$ and impose that $y \in \Lambda_J$, the lattice corresponding to J in $\mathbf{R}^n$. Moreover, the set of $\alpha \in X$ such that $\alpha \in J$ and $|N_{K/\mathbf{Q}}(\alpha)| \leq d\|J\|$ is in $1-1$ correspondance with the set $T = \{y \in Y : y \in \Lambda_J, |S(y)| \leq d\|J\|\}$ via the mapping $\alpha \longmapsto \mu(\alpha)$. Thus $w|B|$ is the cardinal of T.

We now determine an appropriate set of coset representatives Y of V'. To do so, we define a mapping $\mathrm{Ln} : \mathbf{R}^{*r} \times \mathbf{C}^{*s} \longrightarrow \mathbf{R}^{r+s}$ by

$$\mathrm{Ln}(x_1, \ldots, x_r, z_1, \ldots, z_s) = (\ln |x_1|, \ldots, \ln |x_r|, 2\ln |z_1|, \ldots, 2\ln |z_s|).$$

We notice that $\mathrm{Ln}(xy) = \mathrm{Ln}(x) + \mathrm{Ln}(y)$, hence Ln defines a group homomorphism into $(\mathbf{R}^{r+s}, +)$. We also observe that $\mathrm{Ln} \circ \mu$ is the mapping λ which we defined in Section 14.4. The image of λ restricted to U_K spans the hyperplane

$$H = \{(x_1, \ldots, x_{r+s}) \in \mathbf{R}^{r+s} : \sum_{i=1}^{r+s} x_i = 0\}.$$

Since V is a subgroup of U_K, $F = \lambda(V) = \mathrm{Ln}(V')$ is also an additive subgroup of H. As μ defines an isomorphism from V onto V', Ln restricted to V' can be written $\mathrm{Ln} = \lambda \circ \mu^{-1}$ and it follows that Ln defines an isomorphism from V' onto F, because $\lambda : V \longrightarrow F$ is an isomorphism.

We need to justify the last statement, namely that λ restricted to V is injective. We recall that λ is a mapping from O_K^* into $\mathbf{R}^{r+s}$, which defines a group homomorphism when restricted to U_K, the group of units in K. The kernel of λ is W, the set of roots of unity in K. Also U_K is the direct product of W and a subgroup V generated by a set of fundamental units. If $x \in V$ and $\lambda(x) = 0$, then $x \in W \cap V$, which implies that $x = 1$. It follows that λ is injective.

We now set $\mathbf{u} = (\overbrace{1, \ldots, 1}^{r}, \overbrace{2, \ldots, 2}^{s})$. As $\mathbf{u} \notin H$, we may write

$$\mathbf{R}^{r+s} = H \oplus \mathbf{Ru}.$$

To simplify the notation, let us set $v_i = \lambda(\epsilon_i)$, for $i = 1, \ldots, t$, where $\{\epsilon_1, \ldots, \epsilon_t\}$ is a fundamental system of units of V. We recall that the v_i form a basis of the hyperplane H (see Theorem 14.6). We now set

$$\Pi = \{w \in \mathbf{R}^{r+s} : w = \sum_{i=1}^{t} a_i v_i : 0 \leq a_i < 1\}.$$

Then $\Pi \oplus \mathbf{Ru}$ is a set of coset representatives Z of the subgroup F in $\mathbf{R}^{r+s}$. Using Lemma 20.1 again, if we set $Y = \mathrm{Ln}^{-1}(Z)$, then Y is a set of coset representatives of V' in $\mathbf{R}^{*r} \times \mathbf{C}^{*s}$.

We need to justify that $\Pi \oplus \mathbf{Ru}$ is in fact a set of coset representatives of the subgroup F in $\mathbf{R}^{r+s}$. If $\mathbf{x} \in \mathbf{R}^{r+s}$, then

$$\mathbf{x} = \sum_{i=1}^{t} \tilde{a}_i v_i + a\mathbf{u},$$

with $a_i, a \in \mathbf{R}$. We may write $\tilde{a}_i = \lfloor \tilde{a}_i \rfloor + a_i$, where $0 \leq a_i < 1$. Then

$$\mathbf{x} = \sum_{i=1}^{t} a_i v_i + a\mathbf{u} + \sum_{i=1}^{t} \lfloor a_i \rfloor v_i.$$

As the last term in the expression belongs to F, the elements of $\Pi \oplus \mathbf{Ru}$ form a set of coset representatives of F in $\mathbf{R}^{r+s}$, as claimed.

We now observe that Y is homogeneous, i.e., if $a \in \mathbf{R}^*$, then $aY = Y$. To see this, let $y = (x_1, \ldots, x_r, z_1, \ldots, z_s) \in Y$ and $a \in \mathbf{R}^*$. Then

$$\begin{aligned}
\mathrm{Ln}(ay) &= (\ln|ax_1|, \ldots, \ln|ax_r|, 2\ln|az_1|, \ldots, 2\ln|az_s|) \\
&= \ln|a|\mathbf{u} + (\ln|x_1|, \ldots, \ln|x_r|, 2\ln|z_1|, \ldots, 2\ln|z_s|),
\end{aligned}$$

which clearly lies in Z. So $aY \subset Y$. On the other hand, if $y \in Y$, then $\frac{1}{a}y \in Y$, which implies that $y = a \cdot \frac{1}{a}y \in aY$. Hence $Y \subset aY$ and it follows that $aY = Y$, as claimed. For $a > 0$, we define

$$Y_a = \{y \in Y : |S(y)| \leq a\}.$$

Using the homogeneity of Y, we easily obtain the equality

$$Y_a = \sqrt[n]{a}Y_1.$$

If Y_1 is bounded and has a Lipschitz boundary, then we may apply Lemma 20.2 to deduce that

$$|\Lambda_J \cap \sqrt[n]{d\|J\|}Y_1| = \frac{\text{vol } Y_1 \|J\|}{\det \Lambda_J} d + O\left((d\|J\|)^{1-\frac{1}{n}}\right) = \frac{\text{vol } Y_1}{\det \Lambda} d + O(d^{1-\frac{1}{n}}),$$

because $\|J\| = \frac{\det \Lambda_J}{\det \Lambda}$ (cf. end of Section 14.1). Our aim is to estimate the cardinal of the set $T = \{y \in Y : y \in \Lambda_J, |S(y)| \leq d\|J\|\}$. Now

$$T = \Lambda_J \cap \{y \in Y : |S(y)| \leq d\|J\|\} = \Lambda_J \cap \sqrt[n]{d\|J\|}Y_1,$$

therefore, under the conditions on Y_1, we obtain

$$|T| = |\Lambda_J \cap \sqrt[n]{d\|J\|}Y_1| = \frac{\text{vol } Y_1}{\det \Lambda} d + O(d^{1-\frac{1}{n}}).$$

Thus

$$i_C(d) = kd + O(d^{1-\frac{1}{n}}),$$

where $k = \frac{\text{vol } Y_1}{w \det \Lambda}$.

In the next section we will show that Y_1 is in fact bounded and has a Lipschitz boundary.

20.4 Properties of the set Y_1

We now show that Y_1 has the desired properties, namely that Y_1 is bounded and has a Lipschitz boundary. First we find a useful representation of Y_1. By definition, Y_1 consists of those elements $y = (x_1, \dots, x_r, z_1, \dots, z_s) \in \mathbf{R}^{*r} \times \mathbf{C}^{*s}$ such that

$$\text{Ln}(y) = (\ln |x_1|, \dots, \ln |x_r|, 2\ln |z_1|, \dots, 2\ln |z_s|) \in \Pi \oplus \mathbf{Ru},$$

with $|x_1 \cdots x_r z_1^2 \cdots z_s^2| \leq 1$. The last condition is equivalent to saying that

$$\ln |x_1| + \cdots + \ln |x_r| + 2\ln |z_1| + \cdots + 2\ln |z_s| \leq 0.$$

Writing $v_i^{(1)}, \dots, v_i^{(r+s)}$ for the coordinates of v_i, we have the system of equations

$$\begin{array}{rcl}
\ln |x_1| & = & a_1 v_1^{(1)} + \cdots + a_t v_t^{(1)} + b \\
\vdots & = & \vdots \qquad\qquad \vdots \\
\ln |x_r| & = & a_1 v_1^{(r)} + \cdots + a_t v_t^{(r)} + b \\
2\ln |z_1| & = & a_1 v_1^{(r+1)} + \cdots + a_t v_t^{(r+1)} + b2 \\
\vdots & = & \vdots \qquad\qquad \vdots \\
2\ln |z_s| & = & a_1 v_1^{(r+s)} + \cdots + a_t v_t^{(r+s)} + b2,
\end{array}$$

where the a_i and b are elements of $\mathbf{R}$. Since the v_i belong to H, the sum of their coefficients has the value 0 and it follows that b is bounded above by 0 if and only if the sum of the coefficients of $\text{Ln}(y)$ is bounded above by 0. From this we deduce Y_1 is composed of those $y \in \mathbf{R}^{*r} \times \mathbf{C}^{*s}$ such that $\text{Ln}(y) \in \Pi \oplus (-\infty, 0]\mathbf{u}$.

We now may show that Y_1 is a bounded set. For $j = 1, \cdots, r$, the sum $\sum_{i=1}^t a_i v_i^{(j)}$ is bounded, because $|\sum_{i=1}^t a_i v_i^{(j)}| \leq \sum_{i=1}^t |v_i^{(j)}|$. As $b \leq 0$, $\ln |x_i|$ is bounded above, which implies that $|x_i|$ is bounded above. In he same way, for $j = 1, \cdots, s$, $|z_j|$ is bounded above, so the set Y_1 is bounded.

We note Y_1^+ the subset of Y_1 whose real coordinates $x_1, \ldots, x_r$ are positive. We claim that Y_1 has a Lipschitz boundary, if Y_1^+ has a Lipschitz boundary. To prove this, we need a preliminary result.

Lemma 20.3 *If $A_1, \ldots, A_m$ are subsets of a topological space T, then $\partial(A_1 \cup \cdots \cup A_m) \subset \partial A_1 \cup \cdots \cup \partial A_m$, where ∂X denotes the boundary of a set X.*

PROOF We use a proof by induction. For $m = 2$ we have

$$\begin{aligned}
\partial(A_1 \cup A_2) &= \overline{A_1 \cup A_2} \cap \overline{c(A_1 \cup A_2)} \\
&= \overline{A_1 \cup A_2} \cap \overline{cA_1 \cap cA_2} \\
&= (\overline{A_1} \cup \overline{A_2}) \cap \overline{cA_1 \cap cA_2} \\
&= (\overline{A_1} \cap \overline{cA_1 \cap cA_2}) \cup (\overline{A_2} \cap \overline{cA_1 \cap cA_2}) \\
&\subset \partial A_1 \cup \partial A_2.
\end{aligned}$$

In the third line we used the fact that if A and B are subsets of a topological space, then $\overline{A \cup B} = \overline{A} \cup \overline{B}$. Here is a proof. First, $A \subset A \cup B$ implies that $\overline{A} \subset \overline{A \cup B}$. In the same way, $\overline{B} \subset \overline{A \cup B}$, so $\overline{A} \cup \overline{B} \subset \overline{A \cup B}$. Now, $\overline{A} \cup \overline{B}$ contains A and B, therefore $A \cup B \subset \overline{A} \cup \overline{B}$; as $\overline{A} \cup \overline{B}$ is closed, $\overline{A \cup B} \subset \overline{A} \cup \overline{B}$.

Suppose now that the result is true up to m and consider the case $m + 1$. We have

$$\begin{aligned}
\partial(A_1 \cup \cdots \cup A_m \cup A_{m+1}) &\subset \partial(A_1 \cup \cdots \cup A_m) \cup \partial A_{m+1} \\
&\subset \partial A_1 \cup \cdots \cup \partial A_m \cup \partial A_{m+1}.
\end{aligned}$$

Hence the result is true up to $m + 1$, so, by induction, the result is true for all $m \geq 2$. □

Lemma 20.4 *If Y_1^+ has a Lipschitz boundary, then Y_1 also has a Lipschitz boundary.*

PROOF Suppose that Y_1^+ has a Lipschitz boundary. The real coordinates of the elements of Y_1 may be positive or negative. We divide Y_1 into subsets having the same signs on the x_i, for example, $x_1 < 0, x_2 > 0, \ldots, x_r > 0$ or $x_1 > 0, x_2 > 0, x_3 < 0, x_4 > 0, \ldots, x_r > 0$. With $x_i > 0$, for all i, we have Y_1^+. There are 2^r such subsets. If S is one of these subsets, then there is a linear automorphism L of $\mathbf{R}^r \times \mathbf{C}^s$ taking Y_1^+ onto S. The isomorphism L maps the boundary of Y_1^+ onto that of S. If f is a Lipschitz function covering part of the boundary of Y_1^+, then $L \circ f$ is a Lipschitz function covering the corresponding part of the boundary of S. It follows that S has a Lipschitz boundary. From Lemma 20.3, the boundary of Y_1 is contained in the union of the boundaries of the subsets S and hence is Lipschitz. □

We now concentrate our attention on the set Y_1^+.

Proposition 20.1 *The set Y_1^+ has a Lipschitz boundary.*

PROOF We recall that we set $v_i = \lambda(\epsilon_i)$, where $\{\epsilon_1, \ldots, \epsilon_t\}$ is a system of fundamental units in O_K. As above, for each v_i, we write $v_i^{(1)}, \ldots, v_i^{(r+s)}$ for its coordinates. A point $y =$

$(x_1, \ldots, x_r, z_1, \ldots, z_s) \in Y_1^+$ is characterized by the equations

$$\begin{aligned}
\ln(x_1) &= \sum_{i=1}^t a_i v_i^{(1)} + b \\
\vdots \quad & \quad\quad \vdots \\
\ln(x_r) &= \sum_{i=1}^t a_i v_i^{(r)} + b \\
2\ln|z_1| &= \sum_{i=1}^t a_i v_i^{(r+1)} + 2b \\
\vdots \quad & \quad\quad \vdots \\
2\ln|z_s| &= \sum_{i=1}^t a_i v_i^{(r+s)} + 2b,
\end{aligned}$$

where the x_j are positive, the z_k are nonzero, the a_i belong to the interval $[0,1)$ and b is an element of $(-\infty, 0]$.

Now we set $a_{r+s} = e^b$ and write $z_k = \rho_k e^{i\theta_k}$. Then we have the relations

$$x_j = a_{r+s} \exp\big(\sum_{i=1}^t a_i v_i^{(j)}\big) \tag{20.3}$$

$$\rho_k = a_{r+s} \exp\big(\frac{1}{2}\sum_{i=1}^t a_i v_i^{(r+k)}\big) \tag{20.4}$$

$$\theta_k = 2\pi a_{r+s+k}, \tag{20.5}$$

with $a_{r+s} \in (0,1]$, because $b \in (-\infty, 0]$, and all the other $a_i \in [0,1)$. We define the "polar coordinate" transformation β by

$$\beta(x_1, \ldots, x_r, \rho_1, \cdots, \rho_s, \theta_1, \ldots, \theta_s) = (x_1, \ldots, x_r, \rho_1 e^{i\theta_1}, \ldots, \rho_s e^{i\theta_s})$$

and set $f = \beta \circ \alpha$, where

$$\begin{aligned}
\alpha(a_1, \ldots, a_n) &= \Big(a_{r+s} \exp\big(\sum_{i=1}^t a_i v_i^{(1)}\big), \ldots, a_{r+s} \exp\big(\sum_{i=1}^t a_i v_i^{(r)}\big), \\
&\quad a_{r+s} \exp\big(\frac{1}{2}\sum_{i=1}^t a_i v_i^{(r+1)}\big), \ldots, a_{r+s} \exp\big(\frac{1}{2}\sum_{i=1}^t a_i v_i^{(r+s)}\big), \\
&\quad 2\pi a_{r+s+1}, \ldots, 2\pi a_{r+2s}\Big).
\end{aligned}$$

Letting the a_i vary, we obtain a continuous injective mapping f from $C = [0,1)^t \times (0,1] \times [0,1)^s$ onto Y_1^+. Before continuing we recall a generalization of the mean value theorem:

Let E and F be normed vector spaces, O an open subset of E and $h : O \longrightarrow F$ differentiable on O. If the segment $[a,b]$ is contained in O, then

$$\|h(b) - h(a)\| \leq \sup_{x \in (a,b)} \|dh_x\| \|b - a\|.$$

If O is not only open but also convex and the norm of the differential is bounded on O, then h is Lipschitz on O. (The convexity ensures that any two points $a, b \in O$ can be joined by a segment in O.)

The function f which we defined above may be extended to $\mathbf{R}^n$ and has continuous partial deriviatives, so is of class C^1, i.e., the differential is defined and continuous on $\mathbf{R}^n$. Let $\epsilon > 0$ and $O = (-\epsilon, 1+\epsilon)^n$. Then O is a convex open subset in $\mathbf{R}^n$. On the set $\bar{O} = [-\epsilon, 1+\epsilon]^n$, the closure of O, the norm of the differential is bounded, because $\bar{O}$ is compact, hence the norm of the differential is bounded on O and so f is Lipschitz on O. It follows that f is Lipschitz on $[0,1]^n$, being a subset of O.

We claim that $f([0,1]^n)$ is $\overline{Y_1^+}$. To see this, we notice first that, as $[0,1]^n$ is compact and f continuous, $f([0,1]^n)$ is compact and therefore closed. Given that $Y_1^+ \subset f([0,1]^n)$, we have $\overline{Y_1^+} \subset f([0,1]^n) = \overline{f(C)}$. However, $Y_1^+ = f(C)$ implies that $\overline{Y_1^+} = \overline{f(C)}$, so $\overline{Y_1^+} = f([0,1]^n)$, as claimed.

We are now in a position to show that the boundary of Y_1^+ is Lipschitz. The closure $\overline{Y_1^+}$ is the disjoint union of the interior Y_1^{+0} and the boundary ∂Y_1^+. We will show that f maps the interior of the n-cube $[0,1]^n$ into the interior Y_1^{+0}, which implies that the boundary of the n-cube $[0,1]^n$ is mapped onto a set containing the boundary ∂Y_1^+. Since the boundary of $[0,1]^n$ may be considered as composed of $2n$ $(n-1)$-cubes, namely the sides of the n-cube $[0,1]^n$, the boundary ∂Y_1^+ is covered by the images of $2n$ Lipschitz mappings defined on $[0,1]^{n-1}$ (the restrictions of f to the sides of $[0,1]^n$) and so is Lipschitz. It remains to show that the interior $(0,1)^n$ of $[0,1]^n$ is in fact mapped into the interior Y_1^{+0}.

The mapping f restricted to $(0,1)^n$ is the composition of the following four mappings:

$$f_1 : (0,1)^n \longrightarrow \mathbf{R}^n, (t_1, \ldots, t_n) \longmapsto (t_1, \ldots, \ln(t_{r+s}), \ldots, t_n),$$

$$f_2 : \mathbf{R}^n \longrightarrow \mathbf{R}^n, (u_1, \ldots, u_n) \longmapsto (u_1, \ldots, u_n)M,$$

where

$$M = \begin{pmatrix} v_1^{(1)} & \ldots & v_1^{(r+s)} & \\ \vdots & & & \mathbf{0} \\ v_t^{(1)} & \ldots & v_t^{(r+s)} & \\ 1 & \ldots & 2 & \\ & \mathbf{0} & & \mathbf{I_s} \end{pmatrix},$$

$$f_3 : \mathbf{R}^n \longrightarrow \mathbf{R}^n, (a_1, \ldots, a_n) \longmapsto (e^{a_1}, \ldots, e^{\frac{1}{2}a_{r+1}}, \ldots, 2\pi a_{r+s+1}, \ldots, 2\pi a_n),$$

and

$$f_4 : \mathbf{R}^r \times (0,\infty)^s \times \mathbf{R}^s \longrightarrow \mathbf{R}^r \times \mathbf{C}^s,$$
$$(x_1, \ldots, x_r, \rho_1, \ldots, \rho_s, \theta_1, \ldots, \theta_s) \longmapsto (x_1, \ldots, x_r, \rho_1 e^{i\theta_1}, \ldots, \rho_s e^{i\theta_s}).$$

(The first r coordinates in the line $1 \ldots 2$ of the matrix M have the value 1 and the remaining s coordinates the value 2.) Of course, the mapping f_4 is just the "polar coordinate" transformation defined above.

We claim that the four mappings are open and so their composition f is also open. As the matrix M is invertible, f_2 is an automorphism, hence open. To show that the other three mappings are open, we recall another result from analysis, namely the inverse mapping theorem:

Let E and F be Banach spaces, O an open subset of E and $h : O \longrightarrow F$ of class C^1. If $x \in O$ and the differential dh_x is invertible, then there is an open neighbourhood O' of x contained in O such that $h_{|O'}$ is a C^1-diffeomorphism onto its image. This implies that $h(O')$ is an open subset of F.

If the differential dh_x is invertible at every point $x \in O$, then for every point $x \in O$ there is an open neighbourhood O'_x such that $h(O'_x)$ is an open subset of F and we have

$$O = \cup_{x\in O} O'_x \Longrightarrow h(O) = h(\cup_{x\in O} O'_x) = \cup_{x\in O} h(O'_x).$$

As the last set is a union of open subsets in F, $h(O)$ is open in F.

To see that the mappings f_1, f_3 and f_4 are open, it is sufficient to show that the differential df_{ix} is invertible on each point x of the domain of f_i. (The functions f_i have continuous partial derivatives and so are of class C^1.) To determine whether df_{ix} is invertible, we may consider the invertibility of the jacobian matrix $J_{f_i}(x)$. This is the case for all four mappings. For example, the jacobian matrix of f_1 has the form

$$J_{f_1}(t_1, \ldots, t_n) = \begin{pmatrix} \mathbf{I}_t & \mathbf{0} & \mathbf{0} \\ \mathbf{0} & t_{r+s}^{-1} & \mathbf{0} \\ \mathbf{0} & \mathbf{0} & \mathbf{I}_s \end{pmatrix},$$

which is clearly invertible. We leave the calculation of the determinant of the jacobian matrix of f_3 and f_4 to the reader. (In the case of f_4, we consider $\rho_j e^{i\theta_j}$ as the pair $(\rho_j \cos\theta_j, \rho_j \sin\theta_j)$.)

We have shown that the four mappings f_1, f_2, f_3 and f_4 are open, hence f restricted to $(0,1)^n$ is an open mapping. It follows that the image of f restricted $(0,1)^n$ is an open subset of Y_1^+ and thus is contained in Y_1^{+0}, as asserted. Hence the boundary of Y_1^+ is Lipschitz, as required. □

To sum up, we have

Theorem 20.1 *The boundary of Y_1^+ is Lipschitz and hence that of Y_1 is Lipschitz.*

20.5 The constant k

There is a point we have glossed over. We saw above that $k = \frac{\text{vol } Y_1}{w \det \Lambda}$. However, vol Y_1 could depend on the system of fundamental units which we choose. We aim to show that this choice in fact has no effect on vol Y_1 and hence no effect on k. We will calculate explicitly vol Y_1 in passing by vol Y_1^+ (vol $Y_1 = 2^r$vol Y_1^+) and show that this is independant of the choice of the set of fundamental units.

To calculate the volume vol Y_1^+ we aim to use the "change of variables" formula:

Let O be an open subset of $\mathbf{R}^n$ and $f : O \longrightarrow \mathbf{R}^n$ an injective, continuously differentiable mapping such that $J_f(x) \neq 0$, for all $x \in O$. If $g : f(O) \longrightarrow \mathbf{R}$ is integrable, then

$$\int_{f(O)} g\, dx = \int_O (g \circ f)|J_f|\, dx.$$

A proof may be found, for example, in [24].

Applying this result, with $O = (0,1)^n$, f as defined above and g the characteristic function of Y_1^+, we obtain

$$\text{vol } Y_1^+ = \int_{(0,1)^n} |J_f|\, dx,$$

so we need to determine the Jacobian matrix of f.

We recall that f is the composition of two mappings β and α, defined in the previous section, i.e., $f = \beta \circ \alpha$. The Jacobian matrix of f is the product of the Jacobian matrices of β and α, i.e., $J_f = J_\beta \circ J_\alpha$. (We draw attention to the fact that we consider $\rho_j e^{i\theta_j}$ as the pair $(\rho_j \cos\theta_j, \rho_j \sin\theta_j) \in \mathbf{R}^2$.) The Jacobian matrix J_β is easy to determine and we obtain $|\det J_\beta| = \rho_1 \cdots \rho_s$. To find the Jacobian matrix J_α we calculate the partial derivatives of x_j, ρ_j and θ_j, with respect to the a_i, using the relations (21.3), (21.4) and (21.5). We obtain

$$\frac{\partial x_j}{\partial a_i} = \begin{cases} x_j v_i^{(j)} & \text{if } 1 \leq i < r+s \\ \frac{x_j}{a_{r+s}} & \text{if } i = r+s \\ 0 & \text{if } r+s < i \leq n, \end{cases}$$

$$\frac{\partial \rho_j}{\partial a_i} = \begin{cases} \frac{1}{2}\rho_j v_i^{(r+j)} & \text{if } 1 \leq i < r+s \\ \frac{\rho_j}{a_{r+s}} & \text{if } i = r+s \\ 0 & \text{if } r+s < i \leq n \end{cases}$$

and

$$\frac{\partial \theta_j}{\partial a_i} = \begin{cases} 2\pi & \text{if } i = r+s+j \\ 0 & \text{otherwise .} \end{cases}$$

Writing this in matrix form, we have

$$J_\alpha = \begin{pmatrix} v_1^{(1)} x_1 & \dots & v_t^{(1)} x_1 & \frac{x_1}{a_{r+s}} & \\ \vdots & \vdots & \vdots & \vdots & \\ v_1^{(r)} x_r & \dots & v_t^{(r)} x_r & \frac{x_r}{a_{r+s}} & \mathbf{0} \\ \frac{1}{2} v_1^{(r+1)} \rho_1 & \dots & \frac{1}{2} v_t^{(r+1)} \rho_1 & \frac{\rho_1}{a_{r+s}} & \\ \vdots & \vdots & \vdots & \vdots & \\ \frac{1}{2} v_1^{(r+s)} \rho_s & \dots & \frac{1}{2} v_t^{(r+s)} \rho_s & \frac{\rho_s}{a_{r+s}} & \\ & & \mathbf{0} & & 2\pi \mathbf{I_s} \end{pmatrix}$$

and so

$$\det J_\alpha = \frac{x_1 \cdots x_r \rho_1 \cdots \rho_s \pi^s}{a_{r+s}} \det(M^t),$$

where M is the matrix defined in the previous section. Hence

$$|\det J_f| = \frac{x_1 \cdots x_r \rho_1^2 \cdots \rho_s^2 \pi^s}{a_{r+s}} |\det M| = |\det M| \pi^s a_{r+s}^{n-1}.$$

(The last equality needs an explanation. From the equations (21.3), (21.4) and (21.5) we have

$$\begin{aligned} x_1 \cdots x_r \rho_1^2 \cdots \rho_s^2 &= a_{r+s}^n \exp\left(\sum_{i=1}^t a_i v_i^{(1)}\right) \cdots \exp\left(\frac{1}{2}\sum_{i=1}^t a_i v_i^{(r+1)}\right)^2 \cdots \\ &= a_{r+s}^n \exp(a_1(v_1^{(1)} + \cdots + v_1^{(r+s)}) \cdots \exp(a_t(v_t^{(1)} + \cdots + v_t^{(r+s)}) \\ &= a_{r+s}^n \exp(0) \cdots \exp(0) \ = \ a_{r+s}^n, \end{aligned}$$

because the vectors v_i belong to the hyperplane H.)

Therefore

$$\begin{aligned} \mathrm{vol}\, Y_1^+ &= \int_{(0,1)^n} |J_f(a_1, \ldots, a_n)| da_1 \cdots da_n \\ &= |\det M| \pi^s \int_{(0,1)^n} a_{r+s}^{n-1} da_1 \cdots da_n \\ &= \frac{|\det M| \pi^s}{n} \end{aligned}$$

and it follows that $\mathrm{vol}\, Y_1 = 2^n \frac{|\det M| \pi^s}{n}$.

The matrix M may vary according to the choice of the fundamental system of units. We claim that this does not affect the absolute value of the determinant. Suppose that $\{\epsilon_1, \ldots, \epsilon_t\}$ and $\{\epsilon_1', \ldots, \epsilon_t'\}$ are fundamental systems of units. Then each ϵ_i' may be written

$$\epsilon_i' = \zeta_i \epsilon_1^{n_{i,1}} \cdots \epsilon_t^{n_{i,t}},$$

a where ζ_i is a root of unity and $n_{i,1}, \ldots, n_{i,t} \in \mathbf{Z}$. Thus

$$v_i' = \lambda(\epsilon_i') = n_{i,1}\lambda(\epsilon_1) + \cdots + n_{i,t}\lambda(\epsilon_t) = n_{i,1}v_1 + \cdots + n_{i,t}v_t.$$

If we note M and M' the matrices corresponding respectively to $\{\epsilon_1, \ldots, \epsilon_t\}$ and $\{\epsilon_1', \ldots, \epsilon_t'\}$, then we have

$$M' = \begin{pmatrix} n_{1,1} & \ldots & n_{1,t} & \\ \vdots & & \vdots & \mathbf{0} \\ n_{t,1} & \ldots & n_{t,t} & \\ & \mathbf{0} & & \mathbf{I_{s+1}} \end{pmatrix} M = PM.$$

In the same way, there exists a matrix Q with integer coefficients such that $M = QM'$. Therefore P is invertible, with inverse Q. As the determinants of P and Q are integers, we must have $\det P = \pm 1$ and $\det Q = \pm 1$. It follows that

$$|\det M'| = |\det M| |\det P| = |\det M|.$$

Therefore $\mathrm{vol}\, Y_1$ is independant of the fundamental system of units and so is the constant k. We call the expression $\frac{1}{n}|M|$ the *regulator* of O_K (or K) and we note it $\mathrm{reg}(O_K)$. Then

$$k = \frac{\mathrm{vol}\, Y_1}{w \det \Lambda} = \frac{2^r \pi^s \mathrm{reg}(O_K)}{w 2^{-s}\sqrt{|\mathrm{disc}(O_K)|}} = \frac{2^{r+s} \pi^s \mathrm{reg}(O_K)}{w\sqrt{|\mathrm{disc}(O_K)|}}.$$

It is interesting to determine the value of k when K is a quadratic number field. First we consider the case where $K = \mathbf{Q}(\sqrt{m})$ is imaginary. As we saw in Section 14.4, the units are the roots of unity, so we may replace w by $|U_K|$. We also saw in Section 14.4 that $s = 1$ and $r = 0$, so $t = r + s - 1 = 0$. Setting $\operatorname{reg}(O_K) = 1$, we have

$$k = \frac{2\pi}{|U_K|\sqrt{|\operatorname{disc}(O_K|}}.$$

Now we consider a real quadratic number field $K = \mathbf{Q}(\sqrt{m})$. We have two cases to consider, namely $m \equiv 2, 3 \pmod 4$ and $m \equiv 1 \pmod 4$.

Case 1: $m \equiv 2, 3 \pmod 4$ The algebraic integers are of the form $x = a + b\sqrt{m}$, with $a, b \in \mathbf{Z}$. The units are those whose norm is ± 1, i.e., $a^2 - b^2 m = \pm 1$. There are two embeddings of K into $\mathbf{R}$:

$$\sigma_1(a + b\sqrt{m}) = a + b\sqrt{m} \qquad \text{and} \qquad \sigma_2(a + b\sqrt{m}) = a - b\sqrt{m}.$$

Let $u > 0$ be a fundamental unit, with $u = a' + b'\sqrt{m}$. Then $\sigma_1(u) = u$ and $\sigma_2(u) = a' - b'\sqrt{m}$. However,

$$(a' + b'\sqrt{m})(a' - b'\sqrt{m}) = a'^2 - b'^2 m = \pm 1,$$

because u is a unit. Hence $\sigma_2(u) = \pm u^{-1}$ and it follows that $\ln|\sigma_2(u)| = \ln u^{-1} = -\ln u$. Therefore

$$M = \begin{pmatrix} \ln u & -\ln u \\ 1 & 1 \end{pmatrix},$$

therefore $\det M = 2\ln u$ and so $\operatorname{reg}(O_K) = \ln u$.

Case 2: $m \equiv 1 \pmod 4$ The algebraic integers are of the form $x = \frac{1}{2}(a+b\sqrt{m})$, where $a, b \in \mathbf{Z}$ and have the same parity. Since the norm of x is $\frac{1}{4}(a^2 - mb^2)$, x is a unit if and only if $a^2 - mb^2 = \pm 4$, with a and b both odd or both even. There are two embeddings of K into $\mathbf{R}$:

$$\sigma_1(\frac{1}{2}(a + b\sqrt{m})) = \frac{1}{2}(a + b\sqrt{m}) \qquad \text{and} \qquad \sigma_2(\frac{1}{2}(a + b\sqrt{m})) = \frac{1}{2}(a - b\sqrt{m}).$$

Let $u > 0$ be a fundamental unit, with $u = \frac{1}{2}(a' + b'\sqrt{m})$. Then $\sigma_1(u) = u$ and $\sigma_2(u) = \frac{1}{2}(a' - b'\sqrt{m})$. However,

$$\frac{1}{2}(a' + b'\sqrt{m})\frac{1}{2}(a' - b'\sqrt{m}) = \frac{1}{4}(a'^2 - b'^2 m) = \pm 1,$$

because u is a unit. Hence $\sigma_2(u) = \pm u^{-1}$ and it follows that $\ln|\sigma_2(u)| = \ln u^{-1} = -\ln u$. Therefore again we have

$$M = \begin{pmatrix} \ln u & -\ln u \\ 1 & 1 \end{pmatrix},$$

hence $\det M = 2\ln u$ and so $\operatorname{reg}(O_K) = \ln u$.

The roots of unity are ± 1, so $w = 2$, therefore in both cases we have

$$k = \frac{2^2 \ln u}{2\sqrt{|\operatorname{disc}(O_K)|}} = \frac{2\ln u}{\sqrt{|\operatorname{disc}(O_K)|}}.$$

As a fundamental unit and the discriminant $\operatorname{disc}(O_K)$ can be determined without difficulty, we may easily find k.

20.6 Dedekind's ζ function

In this section we introduce the Dedekind ζ function, which generalizes the Riemann ζ function.

We consider the *Dirichlet series*

$$S(s) = \sum_{n\geq 1} \frac{a_n}{n^s},$$

where the a_n are fixed complex numbers and s a complex variable. As usual $n^s = e^{s\ln n}$. Then we have

Lemma 20.5 *If $\sum_{n\leq t} a_n$ is $O(t^r)$, for some $r \geq 0$, then the series $S(s)$ converges for all $s = x+iy$, with $x > r$, and is analytic in the half-plane $H_r = \{s = x+iy : x > r\}$.*

PROOF It is sufficient to show that $S(s)$ converges uniformly on every compact subset of H_r.

For each $s \in H_r$ we estimate the sum $\sum_{n=m}^{M} \frac{a_n}{n^s}$. Setting $A_k = \sum_{n=1}^{k} a_n$, we have

$$\sum_{n=m}^{M} \frac{a_n}{n^s} = \sum_{n=m}^{M} \frac{A_n}{n^s} - \sum_{n=m}^{M} \frac{A_{n-1}}{n^s} = \frac{A_M}{M^s} - \frac{A_{m-1}}{m^s} + \sum_{n=m}^{M-1} A_n(\frac{1}{n^s} - \frac{1}{(n+1)^s}).$$

From the $O(t^r)$ condition there exists a constant C such that $|A_n| \leq Cn^r$, for all n. Hence

$$|\sum_{n=m}^{M} \frac{a_n}{n^s}| \leq C\left(\frac{M^r}{|M^s|} + \frac{(m-1)^r}{|m^s|} + \sum_{n=m}^{M-1} n^r|\frac{1}{n^s} - \frac{1}{(n+1)^s}|\right).$$

Now

$$\frac{1}{n^s} - \frac{1}{(n+1)^s} = s\int_n^{n+1} \frac{dt}{t^{s+1}},$$

hence

$$|\frac{1}{n^s} - \frac{1}{(n+1)^s}| \leq |s|\int_n^{n+1} \frac{dt}{t^{s+1}} = |s|\int_n^{n+1} \frac{dt}{t^{x+1}} \leq \frac{|s|}{n^{x+1}}$$

and

$$|\sum_{n=m}^{M} \frac{a_n}{n^s}| \leq C\left(M^{r-x} + m^{r-x} + |s|\sum_{n=m}^{M-1} n^{r-x-1}\right).$$

We also notice that

$$\sum_{n=m}^{M-1} n^{r-x-1} \leq \int_{m-1}^{\infty} t^{r-x-1}dt = \frac{(m-1)^{r-x}}{x-r},$$

for any $m > 1$. Therefore, letting m and M go to infinity, we find that the sum $\sum_{n=m}^{M} \frac{a_n}{n^s}$ converges to 0, for any $s \in H_r$, and it follows that the series $S(s)$ is convergent.

If A is a compact subset of H_r, then there is a constant C' such $|s| \leq C'$, for $s \in A$. In addition, $x - r \geq \epsilon$ for some $\epsilon > 0$. Hence, for $s \in A$, we have

$$|\sum_{n=m}^{\infty} \frac{a_n}{n^s}| \leq C\left(m^{-\epsilon} + C'\frac{(m-1)^{-\epsilon}}{\epsilon}\right).$$

We set

$$f_m(s) = \sum_{n=1}^{m} \frac{a_n}{n^s} \qquad \text{and} \qquad f(s) = \sum_{n=1}^{\infty} \frac{a_n}{n^s}.$$

The functions f_m are analytic and from what we have just seen they converge uniformly to f on A. It follows that f is analytic on H_r. □

If we set $a_n = 1$, for all n, then $\sum_{n\leq t} a_n = \lfloor t \rfloor$. Thus $\sum_{n\leq t} a_n$ is $O(t^1)$. From Lemma 20.5 the series $S(s)$ converges for all s in the half-plane H_1 and the function

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s}$$

is analytic on this half-plane. This is the *Riemann ζ function*.

Suppose now that K is a number field with number ring O_K. From Theorem 13.5, there is a finite number of ideals with a given norm, and a countable union of finite sets is countable, so the set of ideals in O_K is countable. If we let j_n be the number of ideals I in O_K with $\|I\| = n$, then from the ideal counting equation (20.2), we see that $\sum_{n\leq t} j_n$ is $O(t)$, so the series $S(s)$ in this case also is convergent and the function

$$\zeta_K(s) = \sum_{n=1}^{\infty} \frac{j_n}{n^s}$$

is analytic on the half-plane H_1. The function ζ_K is referred to as the *Dedekind ζ function of the number field K* .

Since the ideals in O_K form a countable set, we may index them by numbers in $\mathbf{N}^*$. Let us fix such an indexation. Then we may write

$$\zeta_K(s) = \sum_{m=1}^{\infty} \frac{1}{\|I_m\|^s}.$$

Indeed, the series $\sum_{m=1}^{\infty} \frac{1}{\|I_m\|^s}$ is absolutely convergent for $s \in H_1$: If $s = x + iy$, then $|\frac{1}{\|I_m\|^s}| = \frac{1}{\|I_m\|^x}$, and so $\sum_{m=1}^{\infty} |\frac{1}{\|I_m\|^s}| = \sum_{m=1}^{\infty} \frac{1}{\|I_m\|^x}$, which is convergent for $x > 1$. This implies that we may rearrange the terms of series as we like, always obtaining a convergent series with the same sum. We may also introduce parentheses where we like. With an appropriate rearrangement and using parentheses, we obtain the expression defining $\zeta_K(s)$.

Example At the beginning of this section we stated that the Dedekind ζ function generalizes the Riemann ζ function. If $K = \mathbf{Q}$, then $O_K = \mathbf{Z}$. The ring $\mathbf{Z}$ is a PID and the nonzero ideals have the form $I = (k)$, with $k \in \mathbf{N}^*$. The cosets of (k) are $(k), 1 + (k), \dots, k - 1 + (k)$, so $\|(k)\| = k$. It follows that for every $k \in \mathbf{N}^*$ there is a unique ideal I with norm k. Thus $\zeta_{\mathbf{Q}} = \zeta$.

We aim to extend ζ_K to a meromorphic function on the half-plane $H_{1-[K:\mathbf{Q}]^{-1}}$, having a unique simple pole. We first extend ζ to a meromorphic function on H_0. Let

$$S_0(s) = 1 - \frac{1}{2^s} + \frac{1}{3^s} - \frac{1}{4^s} + \cdots$$

Then $|\sum_{n\leq t} a_n| \leq 1 = t^0$, so, from Lemma 20.5, the series converges for all $s \in H_0$ and the function S_0 is analytic on H_0. Again using Lemma 20.5, we obtain the absolute convergence of S_0, for $s \in H_1$. We claim that, for $s \in H_1$,

$$S_0(s) = (1 - 2^{1-s})\zeta(s).$$

We show that we have the same terms in the two expressions and so, by the absolute convergence of S_0, we have equality. Indeed,

$$\zeta(s) = S_0(s) + \frac{2}{2^s} + \frac{2}{4^s} + \frac{2}{6^s} + \cdots = S_0(s) + \frac{2^{1-s}}{1^s} + \frac{2^{1-s}}{2^s} + \frac{2^{1-s}}{3^s} + \cdots = S_0(s) + 2^{1-s}\zeta(s),$$

thus the two expressions $S_0(s)$ and $(1 - 2^{1-s})\zeta(s)$ have the same terms, hence the claim. It follows that

$$\frac{S_0(s)}{1 - 2^{1-s}} = \zeta(s),$$

and we may extend ζ to a meromorphic function on the half-plane H_0, which has possible poles at points where $2^{1-s} = 1$, i.e., $s = 1 + \frac{2k\pi i}{\ln 2}$, with $k \in \mathbf{Z}$. We set $s_k = 1 + \frac{2k\pi i}{\ln 2}$. We claim that the only pole is at $s_0 = 1$. For $s_0 = 1$ we have

$$S_0(1) = 1 - \frac{1}{2} + \frac{1}{3} - \frac{1}{4} + \cdots = \ln 2 \neq 0,$$

so s_0 is a pole. This pole is in fact simple, because $h(s) = 1 - 2^{1-s}$ has a simple root at s_0. ($h'(s) = -\ln 2.2^{1-s} \Longrightarrow h'(1) = -\ln 2 \neq 0$.)

We now consider s_k, where $k \neq 0$. Let us look at the series

$$S_1(s) = 1 + \frac{1}{2^s} - \frac{2}{3^s} + \frac{1}{4^s} + \frac{1}{5^s} - \frac{2}{6^s} + \cdots$$

Then $|\sum_{n\leq t} a_n| \leq 2 = 2(t^0)$, so from Lemma 20.5, the series converges for all $s \in H_0$ and the function S_1 is analytic on H_0. A calculation similar to that for $S_0(s)$ shows that

$$S_1(s) = (1 - 3^{1-s})\zeta(s),$$

and so

$$\frac{S_1(s)}{1 - 3^{1-s}} = \zeta(s),$$

for $s \in H_1$, and we have a second possible extension of ζ to H_0, with possible poles at points where $3^{1-s} = 1$, i.e., $s = 1 + \frac{2k'\pi i}{\ln 3}$, with $k' \in \mathbf{Z}$. We set $s_{k'} = 1 + \frac{2k'\pi i}{\ln 3}$. The points s_k and $s_{k'}$ are situated on the straight line $x = 1$. In the former case the y-coordinate is the element $\frac{2\pi}{\ln 2}$ multiplied by an integer and in the latter case the y-coordinate is the element $\frac{2\pi}{\ln 3}$ multiplied by an integer. In fact, the points s_k and $s_{k'}$ are distinct, when either k or k' is nonzero. Without loss of generality, suppose that $k' \neq 0$. Then

$$s_k = s_{k'} \Longrightarrow k(\frac{2\pi}{\ln 2}) = k'(\frac{2\pi}{\ln 3}) \Longrightarrow \frac{k}{k'} = \frac{\ln 2}{\ln 3},$$

which is impossible, because $\frac{k}{k'}$ is rational and $\frac{\ln 2}{\ln 3}$ irrational.

For any $k \neq 0$, if $s \in H_1$, with $s \neq s_k$, then

$$\frac{S_0(s)}{1 - 2^{1-s}} = \zeta(s) = \frac{S_1(s)}{1 - 3^{1-s}}.$$

This implies that the limit of $\frac{S_0(s)}{1-2^{1-s}}$ as s converges to s_k from the right is finite. Consequently s_k cannot be a pole of $\frac{S_0(s)}{1-2^{1-s}}$. Also, we have seen that 1 is a simple pole of this expression. In the following we will refer to the extension $\frac{S_0(s)}{1-2^{1-s}}$ as the extension of ζ to H_0. This extension is meromorphic on H_0 and has a unique pole at 1, which is simple.

We now extend ζ_K. We have

$$\zeta_K(s) = \sum_{n=1}^{\infty} \frac{j_n}{n^s} = \sum_{n=1}^{\infty} \frac{j_n - h_K k}{n^s} + h_K k \zeta(s),$$

where h_K is the number of ideal classes in O_K and k the constant in the ideal counting equation. The Dirichlet series with coefficients $\frac{j_n - h_K k}{n^s}$ converges on the half-plane H_r, with $r = 1 - [K : \mathbf{Q}]^{-1}$, because

$$\sum_{n \leq t} (j_n - h_K k) = O(t^{1-\frac{1}{n}}) = O(t^r),$$

from the ideal counting equation. This combined with the meromorphic extension of ζ gives us a meromorphic extention of ζ_K defined on H_r, with $r = 1 - [K : \mathbf{Q}]^{-1}$, which has a unique pole at $s = 1$. Moreover, this pole is simple.

20.7 The product form of the Dedekind ζ function

As the set of prime ideals in O_K is a subset of the set of ideals, this set is countable, so we may index the prime ideals in O_K by numbers in $\mathbf{N}^*$. In this section we aim to show that, for $s \in H_1$, we may write $\zeta_K(s)$ in a particular product form, namely

$$\zeta_K(s) = \prod_{n \geq 1} \left(1 - \frac{1}{\|P_n\|^s}\right)^{-1},$$

where $\{P_n\}_{n \geq 1}$ is the set of prime ideals in O_K.

To begin with, we will show that the given product is convergent. (For the reader not familiar with infinite products, we have included an appendix on the subject.) We fix $s = x + iy \in H_1$. Now,

$$\sum_{n \geq 1} \left| \frac{1}{\|P_n\|^s} \right| = \sum_{n \geq 1} \frac{1}{\|P_n\|^x} < \sum_{m \geq 1} \frac{1}{\|I_m\|^x}, \tag{20.6}$$

which is convergent, because $s \in H_1$. It follows that $\sum_{n \geq 1} \frac{1}{\|P_n\|^s}$ is absolutely convergent. To simplify the notation we will write a_n for $\frac{1}{\|P_n\|^s}$; then $\sum_{n \geq 1} a_n$ is absolutely convergent, which implies that $\sum_{n \geq 1}(-a_n)$ is absolutely convergent. From Lemma I.2 we deduce that $\prod_{n \geq 1}(1-a_n)$ is absolutely convergent. Now, applying Theorem I.1, we obtain that the product $\prod_{n \geq 1}(1-a_n)$ converges to a nonzero number γ, which is independant of the indexation of the prime ideals. It follows that $\prod_{n \geq 1}(1-a_n)^{-1}$ converges (to $\frac{1}{\gamma}$), independently of the arrangement of the prime ideals, so we may affirm without ambiguity that $\prod_{n \geq 1}(1 - \frac{1}{\|P_n\|^s})^{-1}$ is convergent. Therefore we may write

$$\prod_{P \in \mathrm{Spec}(O_K), P \neq (0)} \left(1 - \frac{1}{\|P\|^s}\right)^{-1}$$

for this product. We aim to show that the product has the value $\zeta_K(s)$, for $s \in H_1$. First we notice that

$$(1-a_n)^{-1} = 1 + a_n + a_n^2 + \cdots ,$$

hence

$$(1-a_1)^{-1}(1-a_2)^{-1} = 1 + (a_1+a_2) + (a_1^2 + a_1a_2 + a_2^2) + \cdots = 1 + \sum a_1^{r_1}a_2^{r_2},$$

where r_1 and r_2 range over $\mathbf{N}$ and are not simultaneously 0. Now, using the multiplicativity of the norm of an ideal (Theorem 13.2), we have

$$a_1^{r_1}a_2^{r_2} = \frac{1}{\|P_1\|^{r_1 s}}\frac{1}{\|P_2\|^{r_2 s}} = \frac{1}{\|P_1^{r_1}P_2^{r_2}\|^s}.$$

For distinct values of r_1 and r_2, the ideals $P_1^{r_1}P_2^{r_2}$ are distinct, so the expression $\sum a_1^{r_1}a_2^{r_2}$ is just the sum of the values of $\frac{1}{\|I\|^s}$, where the sum is taken over all ideals whose decomposition is a product of powers of the ideals P_1 and P_2. We set $A_2 = 1 + \sum a_1^{r_1}a_2^{r_2}$.

In the same way, for the product of $(1-a_1)^{-1}$, $(1-a_2)^{-1}$ and $(1-a_3)^{-1}$, we obtain

$$(1-a_1)^{-1}(1-a_2)^{-1}(1-a_3)^{-1} = 1 + \sum a_1^{r_1}a_2^{r_2}a_3^{r_3},$$

where r_1, r_2 and r_3 range over $\mathbf{N}$ and are not simultaneously 0. The expression $\sum a_1^{r_1}a_2^{r_2}a_3^{r_3}$ is just the sum of the values of $\frac{1}{\|I\|^s}$, where the sum is taken over all ideals whose decomposition is a product of powers of the ideals P_1, P_2 and P_3. Let us set $A_3 = 1 + \sum a_1^{r_1}a_2^{r_2}a_3^{r_3}$.

Continuing in the same way, for any $n \in \mathbf{N}^*$ we obtain

$$(1-a_1)^{-1}\cdots(1-a_n)^{-1} = 1 + \sum a_1^{r_1}\cdots a_n^{r_n},$$

where $r_1, \ldots r_n$ range over $\mathbf{N}$ and are not simultaneously 0. The expression $\sum a_1^{r_1}\cdots a_n^{r_n}$ is the sum of the values of $\frac{1}{\|I\|^s}$, where the sum is taken over all ideals whose decomposition is a product of powers of the ideals $P_1, \ldots, P_n$. We set $A_0 = 1$, and for $n \geq 1$, $A_n = 1 + \sum a_1^{r_1}\cdots a_n^{r_n}$.

We are now in a position to prove the result referred to above.

Theorem 20.2 *If $s \in H_1$, then*

$$\zeta_K(s) = \prod_{P \in Spec(O_K), P \neq (0)} \left(1 - \frac{1}{\|P\|^s}\right)^{-1},$$

where Spec(O_K) denotes the collection of prime ideals in O_K.

PROOF As the series $\zeta_K(s) = \sum_{m=1}^{\infty} \frac{1}{\|I_m\|^s}$, with $s \in H_1$, is absolutely convergent, any rearrangement of the terms gives us another series converging to $\zeta_K(s)$. We now construct a useful rearrangement.

Let T_0 be composed of the single ideal O_K. We give O_K some index, say 0. Every nontrivial ideal I in O_K which is not equal to O_K can be written in a unique way as a product of prime ideals: $I = P_1^{r_1}\cdots P_u^{r_u}$, where at least one r_i is nonzero. We index the ideals in O_K in the following way: First we index the set T_1 composed of the powers of P_1 with indices not equal to 0. (We could use the powers of P_1 as indices.)

Next we consider the set T_2 composed of products of P_1 and P_2, which do not belong to $T_0 \cup T_1$. We index these elements with indices which we have not already used.

Now we consider the set T_3 composed of products of powers of P_1, P_2 and P_3, which do not belong to $T_0 \cup T_1 \cup T_2$. We index the elements of T_3 once again with indices which we have not previously used.

Continuing in the same way we obtain an indexation of all nontrivial ideals. From this indexation we obtain a rearrangement of the terms in the series for $\zeta_K(s)$.

We recall that

$$\zeta_K(s) = \sum_{m=1}^{\infty} \frac{1}{\|I_m\|^s},$$

where the I_m are the ideals in O_K, indexed in some arbitrary way. As the series is absolutely convergent, we may group the terms into 'packets', choosing a permutation allowing us to sum the 'packets' in the order we desire. Thus

$$\zeta_K(s) = \sum_{n \geq 0} \left(\sum_{I \in T_n} \frac{1}{\|I\|^s} \right).$$

If

$$B_n = \sum_{I \in T_0 \cup \cdots \cup T_n} \frac{1}{\|I\|^s},$$

then $\lim_{n\to\infty} B_n = \zeta_K(s)$. However, $B_n = A_n$ and $\lim_{n\to\infty} A_n = \prod_{i=1}^{\infty} \left(1 - \frac{1}{\|P_i\|^s}\right)^{-1}$. Hence we have the equality

$$\zeta_K(s) = \prod_{P \in \mathrm{Spec}(O_K), P \neq (0)} \left(1 - \frac{1}{\|P\|^s}\right)^{-1},$$

as claimed. □

Corollary 20.1 *For $s \in H_1$, we have $\zeta_K(s) \neq 0$.*

PROOF Since the expression of $\zeta_K(s)$ as a product is nonzero, we have the result. □

Remark From what we have just seen, we may find a multiplicative expression for the Riemann ζ function. Setting $K = \mathbf{Q}$, for $s \in H_1$ we obtain

$$\zeta(s) = \zeta_{\mathbf{Q}}(s) = \prod (1 - \frac{1}{p^s})^{-1},$$

where the product is taken over all prime numbers in $\mathbf{N}^*$.

20.8 The class number formula

In this section we bring together the ideal counting equation and the Dedekind ζ function to obtain a relation involving the class number of a number ring. This is known as the *class number formula*. We begin with a preliminary result concerning the Riemann ζ function.

Proposition 20.2 *For the Riemann ζ function, we have*

$$\lim_{s\to 1+}(s-1)\zeta(s) = 1.$$

PROOF We have seen that the series

$$S_0(s) = \sum_{n=1}^{\infty} \frac{(-1)^{n-1}}{n^s},$$

is convergent and holomorphic on the open half-plane H_0; also, for s in the half-plane H_1,

$$\zeta(s) = \frac{S_0(s)}{1-2^{1-s}}.$$

As S_0 is continuous at 1, $\lim_{s\to 1+} S_0(s) = \ln 2$. On the other hand, we have

$$2^{1-s} - 1 = (-\ln 2)2^{1-s'}(s-1),$$

where $s' \in (1, s)$. It follows that

$$\frac{2^{1-s}-1}{s-1} = (-\ln 2)2^{1-s'} \Longrightarrow \lim_{s\to 1+} \frac{2^{1-s}-1}{s-1} = -\ln 2.$$

Hence

$$\lim_{s\to 1+}(s-1)\zeta(s) = 1,$$

as required. □

This result may be written in the form: $\lim_{s\to 1+}(s-1)\zeta_{\mathbf{Q}}(s) = 1$. We now replace $\mathbf{Q}$ by any number field K and consider the limit $\lim_{s\to 1+}(s-1)\zeta_K(s)$. We set $b_l = j_l - h_K k$, where h_K is the class number of O_K (or of K) and k the constant whose value is given by

$$k = \frac{2^{r+s}\pi^s \mathrm{reg}(O_K)}{w\sqrt{|\mathrm{disc}(O_K)|}},$$

where $\mathrm{reg}(O_K)$ is the regulator of O_K as defined above, r (resp. s) the number of real (resp. complex) embeddings of K in $\mathbf{C}$ and w the number of roots of unity in O_K. We have seen above that the Dirichlet series $S_2(s)$ with coefficients $\frac{b_l}{l^s}$ converges and is analytic on the half-plane H_r, with $r = 1 - [K : \mathbf{Q}]^{-1}$. In particular, $S_2(1)$ is finite. Now,

$$S_2(s) = \zeta_K(s) - h_K k\zeta(s) \Longrightarrow \lim_{s\to 1+}(s-1)S_2(s) = \lim_{s\to 1+}(s-1)\zeta_K(s) - h_K k \lim_{s\to 1+}(s-1)\zeta(s)$$

and, from Proposition 20.2, it follows that

$$\lim_{s\to 1+}(s-1)\zeta_K(s) = \frac{2^{r+s}\pi^s \mathrm{reg}(O_K)}{w\sqrt{|\mathrm{disc}(O_K)|}} h_K.$$

This expression is referred to the *class number formula.*

Remark It should be noticed that in general the class number h_K is difficult to determine, hence the expression $\lim_{s\to 1+}(s-1)\zeta_K(s)$ is difficult to evaluate from the formula. On the other hand, using the formula to calculate the class number is also difficult, because the expression $\lim_{s\to 1+}(s-1)\zeta_K(s)$ is not easy to determine directly.

Appendix A

Formal power series, polynomials and polynomial functions

In this appendix we summarize the main results on polynomials which we use in the text. We make a clear distinction between polynomials and polynomial functions, something which is often neglected. Also, we present polynomials in the context of formal power series, which seems to us quite natural. We do not give any proofs. These can be found elsewhere in standard algebra texts, for example [1] or [14].

Formal power series

Let R be a commutative ring with identity. A sequence $A = (a_i)_{i=0}^{\infty}$ of elements of R is called a formal power series over R. We will write $\mathcal{S}_R$ for the set of all such power series. We define an addition $\oplus$ pointwise on $\mathcal{S}_R$: If $A = (a_i)$ and $B = (b_i)$, then we set $A \oplus B = (a_i + b_i)$. With this operation $\mathcal{S}_R$ is a group, with identity $O = (o_i)$, where $o_i = 0$ for all i. The inverse of $A = (a_i)$ is $-A = (-a_i)$.

We also define a multiplication $\odot$ on $\mathcal{S}_R$: for $A, B \in \mathcal{S}_R$, we set $C = (c_i) \in \mathcal{S}_R$, where $c_i = \sum_{k+l=i} a_k b_l$. We write $C = A \odot B$. With this operation and the addition, $\mathcal{S}_R$ is a ring with identity $U = (u_i)$, where $u_0 = 1$ and $u_i = 0$ for $i \neq 0$. An element A is invertible (for the multiplication) if and only if a_0 is invertible in R. An element $X \in \mathcal{S}_R$ plays a special role. We define $X = (x_i)$ by $x_1 = 1$ and $x_i = 0$ for $i \neq 1$. Then it easy to check that, if $X^k = (y_i)$, then $y_k = 1$ and $y_i = 0$ for $i \neq k$. If we set $X^0 = U$, then we can write the power series $A = \sum_{i=1}^{\infty} a_i \cdot X^i$. By convention we usually write $R[[X]]$ for $\mathcal{S}_R$ and call the ring we have just defined the ring of formal power series over R.

We also define a scalar multiplication $\cdot$ on $\mathcal{S}_R$: for $\lambda \in R$, $\lambda \cdot (a_i) = (\lambda a_i)$. With the addition, $\mathcal{S}_R$ is an R-module (an R-vector space, if R is a field) and with the three operations an algebra.

We make certain simplifications in the notation: we write $A + B$ for $A \oplus B$, AB for $A \otimes B$ and λA for $\lambda \cdot A$.

Polynomials

It may be so that a power series has only a finite number of nonzero coordinates. We call such power series polynomials over R. We note the set of polynomials $R[X]$, which is a subring of $R[[X]]$, when $R[[X]]$ is considered as a ring, and a submodule (resp. vector subspace), when $R[[X]]$ is considered as an R-module (resp. R-vector space).

If $A \in R[X]$ and $A \neq O$, then we define the *degree* of A, written $\deg A$, to be $\max\{i : a_i \neq 0\}$. The coefficient a_i, where $i = \deg A$ is called the *leading coefficient* of A. If the leading coefficient has the value 1, then we say that the polynomial is *monic*. We define the degree of the zero polynomial O to be $-\infty$. If $A = (a_i)$ is a nonzero polynomial and $\deg A = n$, then we may write $A = \sum_{i=0}^{n} a_i X^i$.The degree has the following properties:

- $\deg(-A) = \deg A$;
- $\deg(A + B) \leq \max\{\deg A, \deg B\}$;
- $\deg AB = \deg A + \deg B$, if R is an integral domain.

From the third property we easily derive that, if R is an integral domain, then $R[X]$ is an integral domain and the set of invertible elements $R[X]^\times$ is composed of the constant polynomials $A = a$, where $a \in R^\times$.

We may consider division of one polynomial by another. We have the following result:

Theorem A.1 *Let B be a nonzero polynomial in $R[X]$, with leading coefficient invertible in R. For any $A \in R[X]$, there exist unique polynomials $Q, S \in R[X]$ such that*

$$A = QB + S,$$

where $\deg S < \deg B$.

The polynomial Q (resp. R) is called the quotient (resp. *remainder*) of A divided by B. Clearly, if R is a field, then the polynomial B can be any nonzero polynomial. The polynomial B divides A if and only if $S = O$.

Polynomial functions

For a commutative ring R with identity, we note $\mathcal{F}(R)$ the collection of functions from R into itself. We define three operations on $\mathcal{F}(R)$:

$$(f \oplus g)(x) = f(x) + g(x) \qquad (f \odot g)(x) = f(x)g(x) \qquad (z \cdot f)(x) = zf(x),$$

for all $x, z \in R$ and $f, g \in \mathcal{F}(R)$. With the first two operations $\mathcal{F}(R)$ is a ring with identity, and with the first and third operations $\mathcal{F}(R)$ is an R-module. We may define a mapping

$$\Phi : R[X] \longrightarrow \mathcal{F}(R), A \longmapsto \bar{A}$$

in the following way. Let $x \in R$ and $A \in R[X]$. If $A \neq O$ and $A = \sum_{i=0}^{n} a_i X^i$, then we set $\bar{A}(x) = \sum_{i=0}^{n} a_i x^i$ and if $A = O$, then we set $\bar{O}(x) = 0$. The mapping Φ is a ring homomorphism and also an R-module homomorphism. The image of Φ, which we will write $\mathcal{P}(R)$, is a subring of $\mathcal{F}(R)$ and also an R-submodule. The image $\bar{A}$ of A is called the *polynomial function* associated to A. We should notice that there is a clear distinction between polynomials and polynomial functions. When there is no confusion possible, we often write A for $\bar{A}$.

If $\alpha \in R$ and $\bar{A}(\alpha) = 0$, then we say that α is a root of A. The following result is fundamental. It is an easy consequence of Theorem A.1.

Proposition A.1 *Let $A \in R[X]$. Then $\alpha \in R$ is a root of A if and only if $-\alpha + X$ divides A.*

It may be so that a power of $-\alpha + X$ greater than 1 divides A. If $(-\alpha + X)^k$ divides A, but $(-\alpha + X)^{k+1}$ does not, then we say that the root α has *multiplicity* k. We will write $\nu(\alpha)$ for the multiplicity of the root α. Roots with multiplicity 1 are said to be *simple*; on the other hand, roots with multiplicity $k > 1$ are called *multiple roots*. We must be careful with the number of roots: in general, this number is bounded, however there are polynomials with an infinite number of roots. In the case where A is an integral domain we have the following important result.

Theorem A.2 *Let R be an integral domain and A a nonzero polynomial in $R[X]$. Then the number of roots of A, counted with multiplicity, is bounded by the degree of A. If R is an algebraically closed field, then we have equality.*

If R is an infinite integral domain and A is a nonzero polynomial in $R[X]$, then, from the theorem, $\bar{A} \neq 0$ and so the mapping Φ defined above is injective. This means that $R[X]$ is isomorphic as a ring, or as an R-module, to $\mathcal{P}(R)$.

Remark If R is not an integral domain, then Theorem A.2 may not be true. For example, if $f \in \mathbf{Z}_8[X]$, with $f(X) = 4X$, then $\deg f = 1$, but f has four roots, namely $0, 2, 4, 6$.

Differentiation of polynomials

Let $A \in R[X]$ of degree n. We define the derivative $A' \in R[X]$ of A in the following way. If $\deg A \leq 0$, i.e., if A is a constant polynomial, then $A = O$; if $\deg A \geq 1$ and $A = \sum_{i=0}^{n} a_i X^i$, then

$$A' = \sum_{i=1}^{n} i a_i X^{i-1} = \sum_{i=0}^{n-1} (i+1) a_{i+1} X^i.$$

Clearly $\deg A' \leq \deg A - 1$; however, the inequality may be strict. The following result is not difficult to prove.

Theorem A.3 *If $A, B \in R[X]$ and $z \in R$, then*

- $(A + B)' = A' + B'$;
- $(zA)' = zA'$;
- $(AB)' = AB' + A'B$.

Corollary A.1 *The mapping*

$$D : R[X] \longrightarrow R[X], A \longmapsto A'$$

is a an R-module homomorphism.

The derivative is useful in finding multiple roots:

Proposition A.2 *If $\alpha \in R$ and $A \in R[X]$, then α is a multiple root of A if and only if α is a root of both A an A'.*

Remark We may extend the notion of root in the following way. If R is an integral domain and $A \in R[X]$, then any α in an extension of the field of fractions of R is called a root of A if $\bar{A}(\alpha) = 0$.

Irreducible polynomials

We recall that an element a in a ring R is irreducible if it is neither 0 nor invertible and, if there are elements $b, c \in R$ such that $a = bc$, then either b or c is invertible. Also, two elements a and b are associates, if there exists an invertible element c such that $a = cb$. If R is an integral domain and every element $a \in R$, which is neither 0 nor invertible can be written as a product of a unit and irreducible elements and, given two complete factorizations of a

$$a = ub_1 \cdots b_r = vc_1 \cdots c_s,$$

where u and v are units and the b_i and c_j are irreducible, then we have r=s and the b_i can be renumbered so that each c_j is associated to b_j, then we say that R is a unique factorization domain (UFD). A basic property of UFDs is that any two elements a and b have a highest common factor (HCF) d and a lowest common multiple (LCM) m. In addition, dm is an associate of ab (see [5]).

If R is a unique factorization domain and $A \in R[X]$, with $A \neq 0$, then the *content* of A, which we write $c(A)$, is the HCF of the coefficients of A. We say that a polynomial is *primitive* if its content is 1. Clearly, we may write $A = c(A)B$, where $c(B) = 1$. The following result is known as *Gauss's lemma.*

Theorem A.4 *If R is a UFD and $A, B \in R[X]$ are nonzero, then $c(AB) = c(A)c(B)$, up to association. Thus the product of two primitive polynomials is primitive.*

This apparently simple result enables us to prove several other important results. Proofs may be found, for example, in [1].

Theorem A.5 *Let R be a unique factorization domain, with quotient field F, and $A \in R[X]$. Then, if A is nonconstant and irreducible in $R[X]$, then A is irreducible in $F[X]$. On the other hand, if A is primitive and irreducible in $F[X]$, then A is irreducible in $R[X]$.*

Theorem A.6 *If R is a UFD, then so is $R[X]$.*

Theorem A.7 *(Eisenstein's irreducibility criterion) Let R be a UFD, with quotient field F, and $A \in R[X]$, with $\deg A = n \geq 1$. If there is an irreducible element $p \in R$ such that p divides a_i, for $i = 0, \ldots, n-1$, p does not divide a_n and p^2 does not divide a_0, then A is irreducible in $F[X]$. If, in addition, A is primitive, then A is irreducible in $R[X]$.*

Multivariate polynomials

We may define polynomials in an alternative way. We let X be a symbol and define $\tilde{R}[X]$ to be the collection of expressions of the form

$$A = \sum_{i=0}^{m} a_i X^i,$$

where the $a_i \in R$, $m \in \mathbf{N}$, $X^0 = 1$. We call the terms $a_i X^i$ monomials. For $A, B \in R[X]$, we define their sum $A \oplus B$ by adding the coefficients of terms having the same power of X. If

$A = aX^i$ and $B = bX^j$, then we define $A \odot B = abX^{i+j}$. We may extend this multiplication: if $A = \sum_{i=0}^{m} a_i X^i$ and $B = \sum_{j=0}^{n} a_j X^j$, then we multiply pairs of elements (aX^i, bX^j) and then add resulting monomials having the same power; this gives us $A \odot B$. Finally, we define a scalar multiplication: if $\lambda \in R$ and $A = \sum_{i=0}^{m} a_i X^i$ then we set $\lambda \cdot A = \sum_{i=0}^{m} \lambda a_i X^i$. With the three operations so defined $\tilde{R}[X]$ is an R-algebra isomorphic to $R[X]$. As above, we write $A + B$ for $A \oplus B$, AB for $A \odot B$ and λA for $\lambda \cdot A$ and we identify $R[X]$ and $\tilde{R}[X]$.

The alternative way of defining polynomials enables us to extend the definition to polynomials in several variables over a commutative ring R with identity. We let $X_1, \ldots, X_n$ be n commuting symbols, often referred to as variables or indeterminates, and we define $R[X_1, \ldots, X_n]$ to be the collection of expressions of the form

$$A = \sum a_{s_1,\ldots,s_n} X_1^{s_1} \cdots X_n^{s_n},$$

where $a_{s_1,\ldots,s_n} \in R$ and the sum is finite. Each term $a_{s_1,\ldots,s_n} X_1^{s_1} \cdots X_n^{s_n}$ is said to be a monomial. We call the elements of $R[X_1, \ldots, X_n]$ polynomials in n variables or indeterminates. We define an addition $\oplus$ on elements of $R[X_1, \ldots, X_n]$ by adding like monomials in the expressions of polynomials and scalar multiplication $\cdot$ by an element $\lambda \in R$ by multiplying the coefficients of all the monomials by λ. We define a multiplication $\odot$ first on monomials. If $A = aX_1^{s_1} \cdots X^{s_n}$ and $B = bX_1^{t_1} \cdots x_{t_n}$, then we set $A \odot B = abX_1^{s_1+t_1} \ldots X_n^{s_n+t_n}$. We extend this multiplication to any pair of polynomials A and B by first multiplying all pairs of monomials (m_A, m_B), with m_A a monomial of A and m_B a monomial of B, and then adding the monomials obtained with the same powers of each X_i. With the three operations so defined $R[X_1, \ldots, X_n]$ is an R-algebra. As above, we write $A + B$ for $A \oplus B$, AB for $A \odot B$ and λA for $\lambda \cdot A$. We call the maximum value of $s_1 + \cdots + s_n$ the *total degree* of the polynomial A, which we note $\deg A$.

Exercise A.1 *Show that $R[X_1, \ldots, X_n]$ is an integral domain if and only if R is an integral domain.*

If F is a field and $f \in F[X]$ has an infinite number of roots, then f is the zero polynomial. The situation with multivariate polynomials is not the same. For example, if $f(X, Y) = -X + Y^2 \in \mathbf{R}[X, Y]$, then f has an infinite number of roots, but f is not the zero polynomial. However, if the infinite set on which f vanishes has a certain form, then we can assert that f is the zero polynomial.

Theorem A.8 *Let F be a field and $A_1, \ldots, A_n$ infinite subsets of F. If $f \in F[X_1, \ldots, X_n]$ vanishes on the cartesian product $A_1 \times \cdots \times A_n$, then f is the zero polynomial.*

PROOF We use an induction on n, the number of indeterminates. If $n = 1$, then there is nothing to prove. Suppose now that $n > 1$ and the result is true up to $n - 1$. Let $f \in F[X_1, \ldots, X_n]$ and $A_1, \ldots, A_n$ infinite subsets of F such that f vanishes on $A_1 \times \cdots \times A_n$. Fixing $a \in A_n$, we obtain a polynomial $g_a(X_1, \ldots, X_{n-1}) = f(X_1, \ldots X_{n-1}, a)$ in $n - 1$ indeterminates. By the induction hypothesis, g_a has the value 0 on all members of F^{n-1}. We may consider f as an element of $F(X_1, \ldots, X_{n-1})[X_n]$, which has the value 0 on all values of A_n. As this is a polynomial in one indeterminate, it vanishes on F. We have shown that f is the zero polynomial on F^n. This completes the induction step and hence the proof. □

Partial fraction decomposition

Let K be a field and $K[X]$ the integral domain of polynomials with coefficients in K. We note $K(X)$ the field of fractions of $K[X]$. The following theorem generalizes a well-known result of elementary analysis.

Theorem A.9 *Let K be a field and $\phi_1, \ldots, \phi_l$ distinct polynomials in $K[X]$ with positive degrees $d_1, \ldots, d_l$. We suppose that $n_1, \ldots, n_l$ are fixed positive integers and define $g = \prod_{k=1}^{l} \phi_k^{n_k}$ and set $N = \deg g$. Then the following conditions are equivalent:*

- **a.** *The polynomials $\phi_1, \ldots, \phi_l$ are pairwise coprime.*
- **b.** *For every $f \in K[X]$ with $\deg f < N$, there exist unique polynomials $\{p_{kj}\}_{\substack{1\le k\le l\\ 1\le j\le n_k}}$ in $K[X]$, with $\deg p_{kj} \le d_k - 1$ such that $\frac{f}{g}$ may be written in the form*

$$\frac{f}{g} = \sum_{k=1}^{l} \sum_{j=1}^{n_k} \frac{p_{kj}}{\phi_k^j}.$$

- **c.** *Statement* **b.** *without the uniqueness condition.*

PROOF see [2] □

We refer to this result as the partial fraction decomposition theorem.

Appendix B

Symmetric polynomials

If A is a polynomial in n indeterminates, then we obtain another polynomial σA if we permutate the indeterminates X_i by the permutation σ: the monomial $aX_1 \cdots X_n$ becomes $aX_{\sigma(1)} \cdots X_{\sigma(n)}$. The polynomial $A \in R[X_1, \dots, X_n]$ is *symmetric* if, for all permutations $\sigma \in S_n$, $\sigma A = A$. We write $R[X_1, \dots, X_n]^{S_n}$ for the collection of symmetric polynomials over R. These form a subalgebra of $R[X_1, \dots, X_n]$.

We define the polynomials $\Sigma_1, \dots, \Sigma_n$ as follows:

$$\Sigma_1 = \sum_{i=1}^{n} X_i,\ \Sigma_2 = \sum_{i<j} X_i X_j, \dots, \Sigma_k = \sum_{1 \le i_1 < \cdots < i_k \le n} X_{i_1} \cdots X_{i_k}, \dots, \Sigma_n = X_1 \cdots X_n.$$

These polynomials are symmetric and are called the *elementary symmetric polynomials* in $R[X_1, \dots, X_n]$. Each Σ_k is the sum of $\binom{n}{k}$ monomials of degree k. We will sometimes write $\Sigma_k^{(n)}$, instead of Σ_k, to indicate the number of indeterminates. A symmetric polynomial can be expressed in terms of these polynomials, as we will soon see. First we need to generalize the notion of degree in a particular way.

We have seen the notion of total degree, which generalizes that of degree for a polynomial in one variable. However, we may generalize the notion of degree in another way. First we define an order $<$ on $\mathbf{N}^n$: if $I = (i_1, \dots, i_n)$ and $J = (j_1, \dots, j_n)$ and there exists k such that $a_i = b_i$, for $i < k$, and $a_k < b_k$, then we write $I < J$. Clearly $<$ defines a total order on $\mathbf{N}^n$, said to be a *lexicographic* order. It is easy to see that, if $I, J, K \in \mathbf{N}^n$, then

$$I < J \Longrightarrow I + K < J + K.$$

We now consider a polynomial

$$A = \sum_{i_1, \dots, i_n} a_{i_1, \dots, i_n} X_1^{i_1} \cdots X_n^{i_n},$$

which we often abbreviate to $\sum_I a_I X^I$. We notice that $X^I X^J = X^{I+J}$. For a nonzero polynomial A we call the multidegree of A

$$\text{mdeg } A = \max\{I : a_I \neq 0\}.$$

If mdeg $A = I$, then we call $a_I X^I$ the *leading term* of A and a_I the *leading coefficient* of A, which we note lead A. For the elementary symmetric polynomials we have

$$\text{mdeg } \Sigma_1 = (1, 0, \dots, 0), \text{mdeg } \Sigma_2 = (1, 1, 0, \dots, 0), \dots, \text{mdeg } \Sigma_n = (1, 1, \dots, 1).$$

The multidegree has properties similar to those of the degree.

Proposition B.1 *If $A, B \in R[X_1, \ldots, X_n]$ are nonzero, then*

- *mdeg* $AB =$ *mdeg* $A +$ *mdeg* B, *if R is an integral domain;*
- *mdeg* $(A+B) \leq \max($*mdeg* a, *mdeg* $B)$;
- *mdeg* $(A+B) =$ *mdeg* B, *if mdeg* $A <$ *mdeg* B.

PROOF Let

$$A = \sum_{I<K} a_I X^I + a_K X^K \qquad \text{and} \qquad B = \sum_{J<L} b_J X^J + b_L X^L.$$

Then AB has the nonzero term $a_K b_L X^{K+L}$ and the other terms have multidegrees stricly less than $K+L$. Hence

$$\text{mdeg } AB = \text{mdeg } A + \text{mdeg } B.$$

The multidegrees of the monomials of $A+B$ are those of A and B, with the exception of those eliminated when the coefficients of a monomial in A and a monomial in B have opposite signs. It follows that

$$\text{mdeg } (A+B) \leq \max(\text{mdeg } a, \text{mdeg } B).$$

If mdeg $A <$ mdeg B, then the leading term of $A+B$ is that of B, hence

$$\text{mdeg } (A+B) = \text{mdeg } B.$$

This ends the proof. □

We now prove a fundamental result relating symmetric and elementary symmetric polynomials.

Theorem B.1 *Let R be a commutative ring with identity. If $A \in R[X_1, \ldots, X_n]^{S_n}$, then there exists a unique polynomial $S \in R[X_1, \ldots, X_n]$ such that*

$$A = S(\Sigma_1, \ldots, \Sigma_n),$$

where $S(\Sigma_1, \ldots, \Sigma_n)$ is the polynomial S with X_i replaced by Σ_i.

PROOF Existence If A is the zero polynomial, then there is nothing to prove, so let us suppose that this is not the case. We use an argument by induction on the multidegree. If mdeg $A = (0, \ldots, 0)$, then A is constant and we may take $S = A$.

Now suppose that mdeg $A = K = (k_1, \ldots, k_n)$, with $K \neq (0, \ldots, 0)$. We have

$$A = \sum_{I<K} a_I X^I + a_K X^K,$$

with $a_K \neq 0$. We claim that $k_1 \geq k_2 \cdots \geq k_n$. As $(k_1, \ldots, k_n)$ is the multidegree of a nonzero monomial in A and A is symmetric, all permutations of the k_i appear as multidegrees of monomials of A and K is greater than any of these permutations. If, for some i, $k_i < k_{i+1}$, then the sequence obtained by permutation of k_i and k_{i+1} is greater than K and so mdeg $A \neq K$, a contradiction, thus $k_i \geq k_{i+1}$, for all i. We now set

$$a_1 = k_1 - k_2,\ a_2 = k_2 - k_3, \ldots, a_{n-1} = k_{n-1} - k_n, a_n = k_n.$$

As $k_i \geq k_{i+1}$, for all i, the elements a_i are all positive and $B = a_K \Sigma_1^{a_1} \cdots \Sigma_n^{a_n}$ is a polynomial. Since the elementary symmetric polynomials are monic, we have

$$
\begin{aligned}
\text{mdeg } B &= a_1\text{mdeg } \Sigma_1 + a_2\text{mdeg } \Sigma_2 + \cdots + a_n\Sigma_n \\
&= (a_1, 0, \ldots, 0) + (a_2, a_2, 0, \ldots, 0) + \ldots (a_n, \ldots, a_n) \\
&= (a_1 + a_2 + \ldots + a_n, a_2 + \ldots + a_n, \ldots, a_n) \\
&= (k_1, k_2, \ldots, k_n) \;=\; \text{mdeg } A.
\end{aligned}
$$

It follows that A and B have the same leading term, namely $a_K X^K$. If $A = B$, then we are done. If this is not the case and we set $C = A - B$, then mdeg $C < K$. As C is symmetric, there is a polynomial $S' \in R[X_1, \ldots, X_n]$ such that $C = S'[\Sigma_1, \ldots, \Sigma_n]$ and

$$A = B + C = a_K \Sigma_1^{a_1} \cdots \Sigma_n^{a_n} + S'[\Sigma_1, \ldots, \Sigma_n] = S''[\Sigma_1, \ldots, \Sigma_n].$$

This finishes the induction step.

Uniqueness In order to prove the uniqueness of the polynomial S, we will prove, by induction on n, the number of variables, that, if $Q \in R[X_1, \ldots, X_n]$ and $Q[\Sigma_1, \ldots, \Sigma_n] = 0$, then $Q = 0$. First, if $n = 1$, then $\Sigma_1 = X$ and the only possibility is clearly $Q = 0$. Suppose now that $n \geq 2$. We may write

$$Q = \sum_{k=0}^{N} Q_k X_n^k,$$

where $Q_k \in R[X_1, \ldots, X_{n-1}]$. If $Q \neq 0$, then there is a $Q_i \neq 0$. We set $p = \min\{i : Q_i \neq 0\}$. Then

$$0 = Q(\Sigma_1, \ldots, \Sigma_n) = \Sigma_n^p \sum_{k=p}^{N} Q_k(\Sigma_1, \ldots, \Sigma_{n-1}) \Sigma_n^{k-p}.$$

Using the fact that Σ_n^p is monic, we obtain

$$Q_p(\Sigma_1, \ldots, \Sigma_{n-1}) + Q_{p+1}(\Sigma_1, \ldots, \Sigma_{n-1})\Sigma_n + Q_{p+2}(\Sigma_1, \ldots, \Sigma_{n-1})\Sigma_n^2 + \cdots = 0.$$

We define a mapping from $R[X_1, \ldots, X_n]$ into $R[X_1, \ldots, X_{n-1}]$ by setting $X_n = 0$. (We discard all monomials with a power of X_n.) The mapping ψ is a surjective ring homomorphism and

$$\text{Ker}\, \psi = \{A \in R[X_1, \ldots, X_n] : A = aX^n, a \in R\}.$$

Then

$$\psi(Q_p(\Sigma_1^{(n)}, \ldots, \Sigma_{n-1}^{(n)}) = Q_p(\Sigma_1^{(n-1)}, \ldots, \Sigma_{n-1}^{(n_1)}) \qquad \text{and} \qquad \psi(\Sigma_n^{(n)}) = 0,$$

hence

$$Q_p(\Sigma_1^{(n-1)}, \ldots, \Sigma_{n-1}^{(n_1)}) = 0.$$

From the induction hypothesis, $Q_p = 0$, a contradiction. It follows that $Q = 0$, which is what we set out to prove. □

Corollary B.1 *Let R and S be commutative rings with identity such that $R \subset S$. We suppose that $f \in R[X]$, with leading term invertible and roots $\alpha_1, \ldots, \alpha_n$ in S. If $A \in R[X_1, \ldots, X_n]$ is symmetric, then $A(\alpha_1, \ldots, \alpha_n) \in R$.*

PROOF As A is symmetric, there exists a polynomial $T \in R[X_1, \dots, X_n]$ such that $A(X_1, \dots, X_n) = T(\Sigma_1, \dots, \Sigma_n)$. For $i = 1, \dots, n$, let us note $s_i = \Sigma_i(\alpha_1, \dots, \alpha_n)$. Thus $A(\alpha_1, \dots, \alpha_n) = T(s_1, \dots, s_n)$. If $f(X) = \sum_{i=0}^n a_i X^i$, then

$$a_{n-i} = a_n(-1)^i \Sigma_i(\alpha_1, \dots, \alpha_n) = a_n(-1)^i s_i \Longrightarrow s_i = (-1)^i a_n^{-1} a_{n-i}$$

Therefore

$$A(\alpha_1, \dots, \alpha_n) = T(-a_n^{-1} a_{n-1}, a_n^{-1} a_{n-2}, \dots, (-1)^n a_0) \in R,$$

as required. □

Exercise B.1 *Let f be a monic polynomial in $\mathbf{Z}[X]$, with roots $\alpha_1, \dots, \alpha_n \in \mathbf{C}$. We take $e \in \mathbf{N}^*$ and let g be the monic polynomial in $\mathbf{C}[X]$ with roots $\alpha_1^e, \dots, \alpha_n^e$. Show that g has its coefficients in $\mathbf{Z}$.*

Appendix C

Semidirect products

In this appendix we introduce the notion of the *semidirect product* of two groups, which generalizes that of the direct product. This is not usually handled in depth in elementary algebra courses.

If H is a normal subgroup of a group G, then K is said to be a *complement* of H if

$$G = HK \qquad \text{and} \qquad H \cap K = \{e\}.$$

It is easy to see that any $g \in G$ has a unique representation as a product hk, with $h \in H$ and $k \in K$. Also, $G = KH$ and so g has a unique representation $k'h'$, with $k' \in K$ and $h' \in H$. (It is not necessarily the case that $h' = h$ or $k' = k$.) If K is a proper normal subgroup of the group G and H has a complement H, then we say that G is the *semidirect product* of H and K (the order is important).

Proposition C.1 *If G is the semidirect product of H and K, then K is isomorphic to the quotient group G/H.*

PROOF The kernel of the quotient mapping $\phi : G \longrightarrow G/H$ restricted to K is $H \cap K = \{e\}$, so $\phi_{|K}$ is injective. To see that $\phi_{|K}$ is surjective, we take any element $gH \in G/H$. As $g = kh$, we have

$$gH = khH = kH = \phi_{|K}(k),$$

hence $\phi_{|K}$ is surjective. □

If G is the semidirect product of H and K, then there is a natural bijection from the cartesian product $H \times K$ into G, namely

$$\psi(h, k) = hk,$$

for all $(h, k) \in H \times K$. However, this mapping is not necessarily a group homomorphism. If ψ is a homomorphism, then we say that the indirect product is an *internal direct product.*

Proposition C.2 *The mapping ψ is a homomorphism if and only if the elements of H commute with those of K.*

PROOF If ψ is a homomorphism, then, for $h \in H$ and $k \in K$,

$$\psi((e, k)(h, e)) = \psi(e, k)\psi(h, e), \qquad \text{i.e.,} \qquad hk = kh,$$

so elements of H commute with elements of K.

Now suppose that the elements of H commute with those of K and let $(h,k),(h',k') \in H \times K$. Then

$$\psi((h,k)(h',k')) = hh'kk' = hkh'k' = \psi(h,k)\psi(h'k'),$$

so ψ is a homomorphism. $\square$

Corollary C.1 *The mapping ψ is a homomorphism if and only if K is a normal subgroup of G.*

PROOF If ψ is a homomorphism and $k \in K$ and $g = k'h' \in G$, then

$$gkg^{-1} = (k'h')k(k'h')^{-1} = k'(h'kh'^{-1})k'^{-1} = k'kk'^{-1} \in K,$$

so $K \lhd G$.

Now let us suppose that $K \lhd G$ and let $h \in H$ and $k \in K$. We set $z = hkh^{-1}k^{-1}$, the commutator of h and k. As $K \lhd G$, $z = (hkh^{-1})k^{-1} \in K$. In the same way, $z \in H$. However, $H \cap K = \{e\}$, which implies that $z = e$ and hence that h and k commute. As elements of H and K commute, ψ is a homomorphism. $\square$

Examples - If $G = \mathbf{Z}_6$, then there exist subgroups H and K, isomorphic respectively to $\mathbf{Z}_3$ and $\mathbf{Z}_2$, which satisfy the conditions, so we may say that G is the semidirect product of H and K.
- Now let us consider S_3, with $H = A_3$, which is a normal subgroup of S_3, and $K = \{e, (1\ 2)\}$. This subgroup is not normal: for example,

$$(1\ 2\ 3)(1\ 2)(1\ 3\ 2) = (2\ 3) \notin H.$$

However,

$$H \cap K = \{e\} \qquad HK = G.$$

So S_3 is the semidirect product of H and K (and $H \simeq \mathbf{Z}_3$, $K \simeq \mathbf{Z}_2$).

- The dihedral group D_{2n}, $n \geq 3$ is generated by elements a and b such that $o(a) = n$, $o(b) = 2$ and $bab = a^{-1}$. Using the relation $bab = a^{-1}$, we see that, if $H = \langle a \rangle$ and $K = \langle b \rangle$, then $D_{2n} = HK$. If $a^s = b$, with $1 \leq s < n$, then $a^{2s} = e$ and $n|2s$. As $2s < n$, we have $n = 2s$. This is clearly impossible if n is odd. If n is even, then $s = \frac{n}{2}$ and

$$bab = a^{\frac{n}{2}} a a^{\frac{n}{2}} = a = a^{-1} \Longrightarrow n = 2,$$

a contradiction. Hence $H \cap K = \{e\}$. We have shown that D_{2n} is the semidirect product of H and K.

The first two examples show clearly that groups G_1 and G_2 may be nonisomorphic, but at the same time the semidirect product of pairs of subgroups (H_1, K_1) (resp. (H_2, K_2)), with $H_1 \simeq H_2$ and $K_1 \simeq K_2$.

Exercise C.1 *Let H be the subgroup V_4 of A_4, i.e.,*

$$V_4 = \{e, (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)\}.$$

Show that H is normal in S_4 and hence in A_4 and then that A_4 is the semidirect product of H and the subgroup K generated by the 3-cycle $(1\ 2\ 3)$. Is A_4 a direct product of H and K?

If G is the semidirect product of H and K, then any $g \in G$ may be written in a unique form as $g = hk$, with $h \in H$ and $k \in K$. We may write the product of two elements g and g' as follows

$$gg' = (hk)(h'k') = hkh'k^{-1}kk' = h\phi_k(h')kk',$$

where ϕ_k is the automorphism of H defined by k, i.e.,

$$\phi_k(h) = khk^{-1},$$

for all $h \in H$. (As $H \lhd G$, $\phi_k(h) \in H$, so ϕ_k is a mapping from H into H; checking that ϕ_k is an automorphism is easy.) This means that the bijection ψ from $H \times K$ into G defined above is a homomorphism, if we define the product on $H \times K$ by

$$(h,k)(h',k') = (h\phi_k(h), kk').$$

Exercise C.2 *Show that the mapping*

$$\phi : K \longrightarrow Aut(H), k \longmapsto \phi_k$$

is a group homomorphism, where $Aut(H)$ is the group of automorphisms defined on H.

A natural question now arises. Given groups H and K, together with a homomorphism $\phi : K \longrightarrow Aut(H)$, can we construct a semidirect product based on this information? The answer is affirmative and is based on our previous analysis of the semidirect product.

Theorem C.1 *If H and K are groups and $G = H \times K$, their cartesian product, then from a homomorphism $\phi : K \longrightarrow Aut(H)$, we may define a multiplication on G such that G is the semidirect product of H and K. (We identify H with $H' = H \times \{e_K\}$ and K with $K' = \{e_H\} \times K$).*

PROOF We define a multiplication on G by

$$(h,k)(h',k') = (h\phi_k(h'), kk').$$

We need to show first that G, with this multiplication, is indeed a group. The associativity is the most difficult part. We have

$$\begin{aligned}
((h,k)(h',k'))\,(h'',k'') &= \big(h\phi_k(h'), kk'\big)(h'',k'') \\
&= \big(h\phi_k(h')\phi_{kk'}(h''), kk'k''\big) \\
&= \big(h\phi_k(h')\phi_k\phi_{k'}(h''), kk'k''\big) \\
&= \big(\phi_k(h')\phi_k(\phi'_k(h'')), kk'k''\big) \\
&= \big(h\phi_k(h'\phi_{k'}(h''), kk'k''\big) \\
&= (h,k)\big(h'\phi_{k'}(h''), k'k''\big) \\
&= (h,k)\big((h',k')(h'',k'')\big).
\end{aligned}$$

For (e_H, e_K) we write (e,e). Then

$$(h,k)(e,e) = (h\phi_k(e), ke) = (h,k)$$

and

$$(h,k)(\phi_{k^{-1}}(h^{-1}), k^{-1}) = (h\phi_k(\phi_{k^{-1}}(h^{-1}), kk^{-1}) = (hh^{-1}, kk^{-1}) = (e,e),$$

hence G is a group.

We must now show that G is the desired semidirect product of H and K (or of H' and K'). Clearly, $H \cap K = \{(e,e)\}$ and $HK = G$, so we only need to show that H is a normal subgroup of G. First, we consider an element of H conjugated with an element of K:

$$\begin{aligned}
(e,k)(h,e)(e,k)^{-1} &= (e,k)(h,e)(\phi_{k^{-1}}(e^{-1}), k^{-1}) \\
&= (e,k)(h,e)(e,k^{-1}) \\
&= (\phi_k(h), k)(e,k^{-1}) \\
&= (\phi_k(h)\phi_k(e), kk^{-1}) \;=\; (\phi_k(h), e) \in H.
\end{aligned}$$

Now, for the general case, we have:

$$\begin{aligned}(h,k)(h',e)(h,k)^{-1} &= (h,e)(e,k)(h',e)(e,k)^{-1}(h,e)^{-1} \\ &= (h,e)(\phi_k(h'),e)(h,e)^{-1} \\ &= (h,e)(\phi_k(h'),e)(\phi_{e^{-1}}(h^{-1}),e^{-1}) \\ &= (h\phi_k(h')h^{-1},e) \in H.\end{aligned}$$

Therefore H is normal in G and G is the semidirect product of H and K. □

We write $H \rtimes_\phi K$ for this semidirect product of H and K, or simply $H \rtimes K$. We often refer to it as an *external semidirect product.*

It is natural to ask under what circumstances an external semidirect product is a direct product. We give a simple criterion.

Proposition C.3 *An external semidirect product is direct if and only if ϕ is trivial, i.e., $\phi_k = \mathrm{id}_H$, for all $k \in K$.*

PROOF We must show that K is normal in G if and only if ϕ is trivial. If ϕ is trivial, then

$$(h,e)(e,k)(h,e)^{-1} = (h,k)(\phi_{e^{-1}}(h^{-1}),e^{-1}) = (h,k)(h^{-1},e) = (h\phi_k(h^{-1}),k) = (e,k) \in K,$$

because $\phi_k = \mathrm{id}_H$. Therefore K is normal in G.

On the other hand, if ϕ is not trivial, then there exist h and k such that $\phi_k(h) \neq h$ and

$$(h,e)(e,k)(h,e)^{-1} = (h,k)(\phi_{e^{-1}}(h^{-1}),e^{-1}) = (h,k)(h^{-1},e) = (h\phi_k(h^{-1}),k) \notin K,$$

because

$$h\phi_k(h^{-1})k = e \Longrightarrow h\phi_k(h)^{-1} = e \Longrightarrow h = \phi_k(h),$$

a contradiction. It follows that K is not normal in G. □

In general, external semidirect products are not abelian. In fact, this is always so if mapping ϕ is nontrivial. In this case there exist h and k such that $\phi_k(h) \neq h$ and

$$(h,e)(e,k) = (h,k) \neq (\phi_k(h),k) = (e,k)(h,e).$$

Consequently, if the external semidirect product is abelian, then it is a direct product. This enables us to construct a large variety of nonabelian groups.

Remarks

- If the external semidirect product is abelian, then it is a direct product.
- Not all groups can be written as semidirect products. For example, for $n \geq 5$, A_n is simple, i.e., it has no nontrivial proper normal subgroup, and so cannot be written as a semidirect product.

Application: Groups of order pq, with p, q prime and $q < p$

We first consider the case where $q = 2$.

Proposition C.4 *If G is a group of order $2p$, with $p > 2$ prime, the G is cyclic or dihedral.*

PROOF From Cauchy's theorem there exist $a, b \in G$ such that $o(a) = p$ and $o(b) = 2$. Let us set $H = \langle a \rangle$ and $K = \langle b \rangle$. As H has index 2, H is normal in G, hence

$$bab = bab^{-1} = a^r,$$

for $1 \leq r < p$. ($r = 0$ is impossible, because in this case we would have $a = e$.) If $a^s = b$, with $1 \leq s < p$, then $a^{2s} = e$, then $p|2s$. However, $s < p$, we have $p = 2s$, which implies that p is even, a contradiction. It follows that $H \cap K = \{e\}$ and $|HK| = 2p$. This in turn implies that $HK = G$ and so $G = \langle a, b \rangle$.

In addition,

$$a^{r^2} = ba^r b = b(bab)b = a \Longrightarrow a^{r^2-1} = e \Longrightarrow p|r^2 - 1.$$

This implies that $p|r-1$ or $p|r+1$.
Case 1: $p|r-1$: Here $r = 1$, because

$$1 \leq r < p \Longrightarrow 0 \leq r - 1 < p - 1 \Longrightarrow r = 1 \Longrightarrow ab = ba.$$

Therefore G is abelian and the order of ab is $2p$. It follows that G is cyclic.
Case 2: $p|r+1$: Here $r = p-1$, because

$$1 \leq r < p \Longrightarrow 2 \leq r + 1 < p + 1 \Longrightarrow r + 1 = p \Longrightarrow r = p - 1.$$

This implies that

$$G = \langle a, b \rangle \qquad a^p = b^2 = e \qquad bab = a^{-1},$$

ce qui implique que $G \simeq D_{2p}$. □

We now consider the general case. We need a preliminary result.

Lemma C.1 *Suppose that the group G is generated by the elements a and b, whose orders are respectively m and n. We also assume that $bab^{-1} = a^r$, for some $r \in \mathbf{Z}$. Then, for $i, j, k, l \in \mathbf{N}$,*

$$(a^i b^k)(a^j b^l) = a^{i + jr^k} b^{k+l}. \tag{C.1}$$

Therefore, every element $g \in G$ can be written $g = a^s b^t$, with $0 \leq s < m$ and $0 \leq t < n$. This expression is unique if $\langle a \rangle \cap \langle b \rangle = \{e\}$.

PROOF We first prove by induction that, for all $k \in \mathbf{N}$,

$$b^k a b^{-k} = a^{r^k}, \tag{C.2}$$

For $k = 0, 1$, this is evident. Suppose now that the property is true for $k-1$, for some $k \geq 2$. Then

$$b^k a b^{-k} = b(b^{k-1} a b^{-(k-1)}) b^{-1} = b(a^{r^{k-1}}) b^{-1} = (bab^{-1})^{r^{k-1}}.$$

From this last expression we obtain

$$b^k a b^{-k} = (a^r)^{r^{k-1}} = a^{r r^{k-1}} = a^{r^k}.$$

This finishes the induction.

Now, using this relation, we have

$$b^k a^j b^{-k} = (b^k a b^{-k})^j = a^{jr^k} \Longrightarrow b^k a^j = a^{jr^k} b^k$$

and

$$(a^i b^k)(a^j b^l) = a^i a^{jr^k} b^k b^l = a^{i+jr^k} b^{k+l}.$$

Using the orders of the elements a and b, we obtain the expressions that, for all $g \in G$, $g = a^s b^t$, with $0 \leq s < m$ and $0 \leq t < n$.

If $\langle a \rangle \cap \langle b \rangle = \{e\}$, then, for $0 \leq i, j < m$ and $0 \leq k, l < n$,

$$a^i b^k = a^j b^l \Longrightarrow a^{i-j} = b^{l-k} = e \Longrightarrow m|i-j, n|l-k \Longrightarrow i-j = k-l = 0.$$

Therefore the expression $g = a^s b^t$ is unique, if $0 \leq s < m$ and $0 \leq t < n$. □

We will now establish an elementary result, which is useful here (and elsewhere).

Lemma C.2 *If $n \geq 2$, then*

$$Aut(\mathbf{Z}_n) \simeq \mathbf{Z}_n^{\times}.$$

PROOF If $r \in \mathbf{Z}_n^{\times}$, then the mapping $\phi_r : x \longmapsto rx$ is an automorphism of $\mathbf{Z}_n$, so there are at least $\phi(n)$ automorphisms of $\mathbf{Z}_n$. Notice that r is in fact $\phi_r(1)$, so we have $\phi_r(x) = x\phi_r(1)$, where $\phi_r(1)$ is inversible.

On the other hand, if ϕ is an automorphism of $\mathbf{Z}_n$, then $\phi(x) = x\phi(1)$, for all $x \in \mathbf{Z}_n$. If $\phi(1)$ is not inversible, then $\phi(1) = 0$ or $\phi(1)$ is a zero divisor. The first alternative is false, because this would imply that the mapping ϕ takes every $x \in \mathbf{Z}_n$ to 0. In the second case, there exists $v \neq 0$ in $\mathbf{Z}_n$ such that $v\phi(1) = 0$. This implies that $\phi(v) = 0$ and, as $\phi(0) = 0$, ϕ is not injective. It follows that $\phi(1)$ is inversible and the result now follows. □

Proposition C.5 *Let p and q be prime numbers with $q < p$. There exists a nonabelian group of order pq if and only if $p \equiv 1(mod\, q)$.*

PROOF Let us first suppose that $p \equiv 1(\text{mod } q)$. From Lemma C.2, we know that $|Aut(\mathbf{Z}_p)| = p-1$. Given that $q|p-1$, from Cauchy's theorem, there exists $\alpha \in Aut(\mathbf{Z}_p)$ with order q. We may now define a homomorphism $\phi : \mathbf{Z}_q \longrightarrow Aut(\mathbf{Z}_p)$ by associating $1 \in \mathbf{Z}_q$ to α. The homomorphism ϕ is not trivial, because α is not the identity on $\mathbf{Z}_p$. Therefore, from Proposition C.3, the external semidirect product $\mathbf{Z}_p \rtimes_\phi \mathbf{Z}_q$ is not direct, hence not abelian; its order is clearly pq.

Now let us suppose that $p \not\equiv 1(\text{mod } q)$ and that G is a group of order pq. Let P (resp. Q) be a Sylow p-subgroup (resp. q-subgroup) of G. We note s_p (resp. s_q) the number of such subgroups. From the Sylow theorems we know that $s_p|q$ and $s_p \equiv 1(\text{mod } p)$. As $q < p$, we must have $s_p = 1$. As every conjugate gPg^{-1}, for $g \in G$, is a Sylow p-subgroup, $gPg^{-1} = P$, hence P is a normal subgroup of G. Also, $s_q|p$ and $s_q \equiv 1(\text{mod } q)$. From the first property $s_q = 1$ or $s_q = p$. However, if $s_q = p$, then, from the second property, $q|p-1$, which is false by hypothesis. Hence, $s_q = 1$ and it follows, as in the case of P, that Q is normal in G. This means that G is the direct product of the cyclic subgroups P and Q and so is abelian. □

There is a natural question which now arises: Can there be nonisomorphic nonabelian groups of order pq? In fact, this is not possible, as we will now see.

Proposition C.6 *If p, q are prime numbers with $q < p$ and G, G' are nonabelian groups of order pq, then G is isomorphic to G'.*

PROOF Let P (resp. Q) a Sylow p-subgroup (resp. q-subgroup) of G and P', Q' the corresponding subgroups of G'. These four subgroups are cyclic, so we may write

$$P = \langle a\rangle \qquad Q = \langle b\rangle \qquad P' = \langle \alpha\rangle \qquad Q' = \langle \beta\rangle.$$

The relation $\langle a\rangle \cap \langle b\rangle = \{e\}$ implies that the cardinal of $\langle a\rangle\langle b\rangle$ is pq. Consequently $G = \langle a\rangle\langle b\rangle$. In the same way, $G' = \langle \alpha\rangle\langle \beta\rangle$.

From the proof of Proposition C.5 we have $P \lhd G$ (resp. $P' \lhd G'$) and there exists $r \in \mathbf{Z}$ such that $bab^{-1} = a^r$ (resp. $s \in \mathbf{Z}$ such that $\beta\alpha\beta^{-1} = \alpha^s$). Now, using Lemma C.1, we have

$$b^q = e \Longrightarrow b^q ab^{-q} = a^{r^q} \Longrightarrow a = a^{r^q} \Longrightarrow e = a^{r^q - 1} \Longrightarrow r^q \equiv 1(\text{mod } p).$$

An analogous calculation shows that $s^q \equiv 1(\text{mod } p)$. The order of s (mod p) cannot be 1, because G' are not abelian. It follows that the order of s is q. (A similar argument shows that the order of r (mod p) is q. Now let us consider the equation

$$X^q \equiv 1 \ (\text{mod } p). \tag{C.3}$$

The solutions are of the form s^j, with $j = 1, \dots, q-1$. (If $s^k \equiv s^l$ (mod p), with $k < l$, then $s^{l-k} \equiv 1$ (mod p), which implies that $k - l = 0$, so the solutions are distinctes.) As r is a solution of the equation (C.3), there is a $j \in \{1, \dots, q-1\}$ such that $r \equiv s^i$ (mod p). We notice that $j \neq 1$, because G is not abelian. We have

$$\beta^j \alpha \beta^{-j} = \alpha^{s^j} = \alpha^r,$$

because $\alpha^p = e$. If $\bar{\beta} = \beta^j$, then $\bar{\beta}$ is a generator of Q'. Finally, we have $G = \langle a, b\rangle$, with $bab^{-1} = a^r$ and $G' = \langle \alpha, \bar{\beta}\rangle$, with $\bar{\beta}\alpha\bar{\beta}^{-1} = \alpha^r$. We define a mapping ϕ from G into G' by

$$\phi(a) = \alpha \qquad \text{and} \qquad \phi(b) = \bar{\beta}$$

and extending it in a natural way to G. Using Lemma C.1, we see that ϕ is an isomorphism. □

We can now summarize the preceding work:

Theorem C.2 *If p and q are prime numbers, with $q < p$, and G is a group of order pq, then either*

- *$p \not\equiv 1$ (mod q) and G is cyclic, or*
- *$p \equiv 1$ (mod q) and G is either cyclic or nonabelian and isomorphic to the semidirect product $\mathbf{Z}_p \rtimes_\phi \mathbf{Z}_q$ defined in Proposition C.5.*

PROOF From Proposition C.5, if $p \not\equiv 1$ (mod q), then G is abelian and it follows that G has an element of order pq and so is cyclic. On the other hand, if $p \equiv 1$ (mod q), then G may be abelian or nonabelian. In the first case G has an element of order pq and so is cyclic. In the second case, from Proposition C.5, we know that there exists a nonabelian group of order pq. However, from Proposition C.6, all groups of order pq are isomorphic, hence G is isomorphic to the semidirect product $\mathbf{Z}_p \rtimes_\phi \mathbf{Z}_q$ defined in Proposition C.5. □

Remark Given that all nonabelian groups of order pq, with $q < p$, are isomorphic, we often write $\mathbf{Z}_p \rtimes \mathbf{Z}_q$ for $\mathbf{Z}_p \rtimes_\phi \mathbf{Z}_q$.

Appendix D

Nonabelian groups of order 8

We aim to identify the nonabelian groups with order 8. If G is such a group and has an element x of order 8, then G is cyclic, so abelian. On the other hand, if all elements other than the identity e have order 2, then $x^{-1} = x$, for all $x \in G$ and it follows that G is abelian. Now suppose that G has an element x with order 4 and let

$$H = \langle x \rangle = \{e, x, x^2, x^3\}.$$

We take $y \notin H$. Then $Hy \neq H$ and $G = H \cup Hy$. Suppose that there is an element $y' \in G \setminus H$ with $o(y') = 2$. To simplify the notation, let us write y for y'. We claim that $yx \neq x^2y$. If so, then

$$yx^2y = yxxy = x^2yxy = x^2x^2yy = x^4y^2 = ee = e,$$

then

$$x = ex = y^2x = yyx = yx^2y = e,$$

which is impossible. Hence $yx \neq x^2y$, as claimed. There are two other possibilities, namely $yx = xy$ or $yx = x^3y$. In the first case G is abelian, so let us consider the second. Then we have $G = \langle x, y \rangle$, $o(x) = 4$, $o(y) = 2$ and

$$yxy = x^3yy = x^3 = x^{-1}.$$

Therefore G is isomorphic to D_8 (and nonabelian).

Now let us suppose that every element of $G \setminus H$ has order 4 and let $y \in G \setminus H$. As $o(y) = 4$, we have $o(y^2) = 2$ and so $y^2 \in H$. The only element of order 2 in H is x^2, so $y^2 = x^2$. We claim that $yx \neq xy$. If this is the case, then

$$(x^3y)^2 = x^3yx^3y = x^6y^2 = x^2y^2 = x^2x^2 = x^4 = e,$$

which implies that $o(x^3y) \neq 4$, because $x^3y \notin H$. This is a contradiction and the claim is established.

If $yx = x^2y$, then

$$yx = x^2yy^2y = y^3 \Longrightarrow x = y^2,$$

which is impossible, because $o(x) = 4$ and $o(y^2) = 2$. The remaining possibility is $yx = x^3y$:

$$yx = x^3y \Longrightarrow yxy^{-1} = x^3 = x^{-1}.$$

Thus G is isomorphic to the quatornian group Q_8. To this more clearly, if we set

$$\mathbf{i} = x \qquad \mathbf{j} = y \qquad \mathbf{k} = xy,$$

then we obtain

$$\mathbf{i}^2 = \mathbf{j}^2 = \mathbf{k}^2.$$

Writing $-\mathbf{1}$ for this common value and then abbreviating $(-\mathbf{1})\mathbf{u}$ to $-\mathbf{u}$, then we have

$$\mathbf{ij} = -\mathbf{ji} = \mathbf{k} \qquad \mathbf{jk} = -\mathbf{kj} = \mathbf{i} \qquad \mathbf{ki} = -\mathbf{ik} = \mathbf{j}.$$

We have a nonabelian group of 8 elements with the required relations. This is called the quatornian group and we note it Q_8.

D_8 as a Galois group

Let

$$f(X) = -2 + X^4 \in \mathbf{Z}[X].$$

Using the Eisenstein criterion it is easy to see that f is irreducible over $\mathbf{Q}$. The roots of f in $\mathbf{C}$ are $\pm\sqrt[4]{2}$, $\pm i\sqrt[4]{2}$ and the splitting field of f in $\mathbf{C}$ may be written $E = \mathbf{Q}(i, \sqrt[4]{2})$. As $[E : \mathbf{Q}] = 8$, the cardinal of the Galois group of f is 8. Consider the automorphism $\rho \in G = Gal(E/\mathbf{Q})$ such that $\rho(i) = i$ and $\rho(\sqrt[4]{2}) = i\sqrt[4]{2}$. The existence of such an automorphism is assured by Proposition 2.3 and Theorem 2.2. Now $\rho(i)^2 = i$ and

$$\rho^2(\sqrt[4]{2}) = \rho(i\sqrt[4]{2}) = i(i\sqrt[4]{2}) = -\sqrt[4]{2},$$

therefore $\rho^4(\sqrt[4]{2}) = \sqrt[4]{2}$. Hence $o(\rho) = 4$.

Now let $\sigma \in G$ be complex conjugation. Then

$$\sigma \circ \rho(\sqrt[4]{2}) = \sigma(i\sqrt[4]{2}) = -i\sqrt[4]{2} \qquad \text{and} \qquad \rho \circ \sigma(\sqrt[4]{2}) = \rho(\sqrt[4]{2}) = i\sqrt[4]{2},$$

so ρ and σ do not commute. Thus G is not abelian. As $o(\rho^2) = 2$, G has at least two elements with order 2. This means that G is not isomorphic to Q_8, which has a unique element of order 2. Hence G is isomorphic to D_8.

Appendix E

Free abelian groups and free modules

Free abelian groups

In this appendix, as is usual for abelian groups, we will use the additive notation. A group G is a *free abelian group* if $G = \{0\}$ or G is isomorphic to a direct sum, not necessarily finite, of additive groups $\mathbf{Z}$, i.e.,

$$G \simeq \oplus_{i \in I} \mathbf{Z}.$$

(We recall that $\oplus_{i \in I} \mathbf{Z}$ is the collection of sets $(n_i)_{i \in I}$, with $n_i \in \mathbf{Z}$, and only a finite number of n_i nonzero.)

If G is a nontrivial abelian group, i.e., $G \neq \{0\}$, then we say that a subset $\mathcal{B}$ of G is a *basis*, if

- $\mathcal{B}$ generates G, i.e., any element $x \in G$ can be written $x = n_1 x_1 + \ldots + n_k x_k$, where the $x_i \in \mathcal{B}$ and the $n_i \in \mathbf{Z}$;
- if, for $x_1, \ldots, x_k \in \mathcal{B}$ and $n_1, \ldots, n_k \in \mathbf{Z}$, we have $n_1 x_1 + \ldots + n_k x_k = 0$, then $n_1 = \cdots = n_k = 0$.

(We often refer to a basis as an *integral basis*).

Free abelian groups are precisely those abelian groups having a basis. More precisely, we have:

Theorem E.1 *A nontrivial abelian group G has a basis if and only if G is a free abelian group.*

PROOF Suppose that G has a basis $\mathcal{B}$. Then the mapping

$$f : \oplus_{x \in \mathcal{B}} \mathbf{Z} \longrightarrow G, (n_x)_{x \in \mathcal{B}} \longmapsto \sum_{x \in \mathcal{B}} n_x x$$

is an isomorphism.

Now suppose that we have an isomorphism $f : \oplus_{i \in I} \mathbf{Z} \longrightarrow G$. For $j \in I$, let us set $\delta_j = (n_i)_{i \in I} \in \oplus_{i \in I} \mathbf{Z}$, where

$$n_i = \begin{cases} 1 & \text{if } i = j, \\ 0 & \text{otherwise.} \end{cases}$$

Then $\{f(\delta_j)\}_{j\in I}$ is a basis of G. $\square$

We now consider bases of free abelian groups in more detail. We begin with an elementary lemma.

Lemma E.1 *Let $\{G_i\}_{i\in I}$ be a collection of abelian groups and H_i a subgroup of G_i, for each $i \in I$. Then*

$$\oplus_{i\in I} G_i / \oplus_{i\in I} H_i \simeq \oplus_{i\in I}(G_i/H_i).$$

PROOF For $x = (x_i)_{i\in I} + \oplus_{i\in i} H_i$, let us set

$$f(x) = (x_i + H_i)_{i\in I}.$$

Then $f(x) \in \oplus_{i\in I}(G_i/H_i)$ and f is an isomorphism. $\square$

In order to prove the next theorem we will need the following elementary result from set theory.

Proposition E.1 *If X is an infinite set and $P_{fin}(X)$ the collection of finite sets in X, then the cardinal of X and that of $P_{fin}(X)$ are equal.*

Theorem E.2 *If G is a nontrivial free abelian group, then all bases of G have the same cardinal.*

PROOF Let $\mathcal{B}$ and $\mathcal{B}'$ be two bases of the free abelian group G. Then we have isomorphisms

$$f : G \longrightarrow \oplus_{x\in\mathcal{B}} \mathbf{Z} \qquad \text{and} \qquad f : G \longrightarrow \oplus_{y\in\mathcal{B}'} \mathbf{Z}.$$

Let us consider $2G = \{2a : a \in G\}$. $2G$ is a subgroup of G. From Lemma E.1,

$$G/2G \simeq (\oplus_{x\in\mathcal{B}} \mathbf{Z})/2(\oplus_{x\in\mathcal{B}} \mathbf{Z}) \simeq \oplus_{x\in\mathcal{B}} \mathbf{Z}/2\mathbf{Z}.$$

In the same way

$$G/2G \simeq \oplus_{y\in\mathcal{B}'} \mathbf{Z}/2\mathbf{Z},$$

so we have the relation

$$\oplus_{x\in\mathcal{B}} \mathbf{Z}/2\mathbf{Z} \simeq \oplus_{y\in\mathcal{B}'} \mathbf{Z}/2\mathbf{Z}. \tag{E.1}$$

<u>Case 1</u> : $|\mathcal{B}| = m < \infty$, $|\mathcal{B}'| = n < \infty$.
Using equation (E.1), we have

$$2^m = |\oplus_{x\in\mathcal{B}} \mathbf{Z}/2\mathbf{Z}| = |\oplus_{y\in\mathcal{B}'} \mathbf{Z}/2\mathbf{Z}| = 2^n,$$

therefore $m = n$.

<u>Case 2</u> : $|\mathcal{B}| < \infty$, $|\mathcal{B}'| = \infty$.

As in the first case, we have

$$\oplus_{x\in\mathcal{B}} \mathbf{Z}/2\mathbf{Z} \simeq \oplus_{x\in\mathcal{B}'} \mathbf{Z}/2\mathbf{Z},$$

which is impossible, because $\oplus_{x\in\mathcal{B}} \mathbf{Z}/2\mathbf{Z}$ is finite and $\oplus_{x\in\mathcal{B}'} \mathbf{Z}/2\mathbf{Z}$ infinite.

<u>Case 3</u> : $|\mathcal{B}| = \infty$, $|\mathcal{B}'| = \infty$.

The mapping ϕ of $P_{fin}(\mathcal{B})$ into $\oplus_{x\in\mathcal{B}}\mathbf{Z}/2\mathbf{Z}$, where $\phi(S) = (n_x)_{x\in\mathcal{B}}$, with $n_x = 1$ if and only if $x \in S$, is a bijection. We define a bijection ϕ' of $P_{fin}(\mathcal{B}')$ onto $\oplus_{y\in\mathcal{B}'}\mathbf{Z}/2\mathbf{Z}$ in the same way. From equation $(E.1)$, we obtain a bijection ψ from $P_{fin}(\mathcal{B})$ onto $P_{fin}(\mathcal{B}')$, so these two sets have the same cardinality. Applying Proposition E.1, we obtain $|\mathcal{B}| = |\mathcal{B}'|$. □

If G is a nontrivial free abelian group, then the *rank* of G is the cardinal of a basis of G; if $G = \{0\}$, then the rank is 0. For this rank we write $\operatorname{rk} G$.

We now consider subgroups of free abelian groups. We need to some preliminary work.

Lemma E.2 *If G and H are groups and $f : G \longrightarrow H$, $g : H \longrightarrow G$ homomorphisms such that $fg = \mathrm{id}_H$, then*

$$G \simeq H \oplus Ker\, f.$$

PROOF Let $G' = g(H)$. If $g(x_1) = g(x_2)$, then $fg(x_1) = fg(x_2)$, which implies that $x_1 = x_2$, because $fg = \mathrm{id}_H$. Hence H is isomorphic to G'. Suppose now that $y \in G' \cap \operatorname{Ker} f$. There exists $x \in H$ such that $g(x) = y$, because $y \in G'$. As $y \in \operatorname{Ker} f$, $f(y) = e_H$, the identity of H, hence $fg(x) = e_H$. As $fg = \mathrm{id}_H$, $x = e_H$ and it follows that $y = g(e_H) = e_G$, the identity of G. Thus $G' \cap \operatorname{Ker} f = e_G$. We now show that $G = G' + \operatorname{Ker} f$. Let $y \in G$ and set $y' = gf(y)$. Then

$$f(y'^{-1}y) = f(y')^{-1}f(y) = fgf(y)^{-1}f(y) = e_H$$

and so $y'^{-1}y \in \operatorname{Ker} f$. Thus y is the product of an element in G' and an element in $\operatorname{Ker} f$. We have

$$G \simeq G' \oplus \operatorname{Ker} f \simeq H \oplus \operatorname{Ker} f,$$

as stated. □

Proposition E.2 *If G and H are abelian groups, with H free, and $f : G \longrightarrow H$ an epimorphism, then*

$$G \simeq H \oplus Ker\, f.$$

PROOF We take a basis $\mathcal{B}$ of H. As f is surjective, for every $x \in \mathcal{B}$, there exists an element $y_x \in G$ such that $f(y_x) = x$. We define a homomorphism $g : H \longrightarrow G$ by setting $g(x) = y_x$, for all $x \in \mathcal{B}$. Then $fg(x) = x$, for all $x \in \mathcal{B}$ and so $fg = \mathrm{id}_H$. From Lemma E.2, $G \simeq H \oplus \operatorname{Ker} f$. □

Now we are in a position to prove an important result concerning subgroups of free abelian groups of finite rank.

Theorem E.3 *Let G be a free abelian group of finite rank n and H a subgroup of G. Then H is a free abelian group and*

$$rk\, H \leq rk\, G.$$

We may suppose that $G = \mathbf{Z}^n$. We will prove the result by induction on n. If $n = 1$ and $H \subset \mathbf{Z}$, then $H = k\mathbf{Z}$, for some $k \in \mathbf{N}$. Therefore $H = 0$ or $H \simeq \mathbf{Z}$, so the statement is true for $n = 1$.

Now suppose that the result is true for n and let $H \subset \mathbf{Z}^{n+1}$. The mapping

$$f : \mathbf{Z}^{n+1} \longrightarrow \mathbf{Z}, (m_1, \ldots, m_{n+1}) \longmapsto m_{n+1}$$

is a homomorphism and

$$\operatorname{Ker} f = \{(m_1, \ldots, m_n, 0) : m_i \in \mathbf{Z}\} \simeq \mathbf{Z}^n.$$

Clearly f restricted to H is an epimorphism onto its image. As $\mathrm{Im}\, f_{|_H} \subset \mathbf{Z}$, from what we have seen for $n = 1$, $\mathrm{Im}\, f_{|_H}$ is a free abelian group, therefore, from Proposition E.2,

$$H \simeq \mathrm{Im}\, f_{|_H} \oplus \mathrm{Ker}\, f_{|_H}.$$

We notice that $\mathrm{Ker}\, f_{|_H}$ is a subgroup of $\mathrm{Ker}\, f$ and recall that $\mathrm{Ker}\, f \simeq \mathbf{Z}^n$, hence, from the induction hypothesis, $\mathrm{Ker}\, f_{|_H}$ is a free abelian group and rk $\leq n$. It follows that H is a free abelian group and $\mathrm{rk}\, H \leq 1 + n$. By induction the result is true for all $n \in \mathbf{N}$. □

Exercise E.1 *Show that a free abelian group G may have a subgroup H strictly included in G with the same rank.*

If G is a nontrivial free abelian group and H a nontrivial subgroup, then G and H have bases. We may find bases of G and H, which have a special relation to each other.

Theorem E.4 *If H is a nontrivial subgroup of rank r of a free abelian group G of rank n, then G has a basis $(e_1, \dots, e_n)$ for which there exist integers $d_1, \dots, d_r \in \mathbf{N}^*$ such that $d_i | d_{i+1}$, for $1 \leq i < r$, and $(d_1 e_1, \dots, d_r e_r)$ is a basis of H.*

PROOF We will prove the result by an induction on n. For $n = 1$, the statement is evident. Now take $n > 1$ and suppose that the result is true for $m < n$. If $(u_i)_{i=1}^n$ is a basis of G, then the elements $u \in H$ are expressions of the form $\sum_{i=1}^n n_i u_i$, with the $n_i \in \mathbf{Z}$. If we consider all such expressions, then there is a coefficient of minimal value in $\mathbf{N}^*$. For different bases this minimal value could be different. We take a basis $(v_i)_{i=1}^n$ for which this minimal value is a minimum. We may suppose that this is the coefficient of v_1 in some expression and we write l_1 for this coefficient. We fix $v \in H$ with

$$v = l_1 v_1 + \sum_{i=2}^n a_i v_i.$$

We now divide each a_i by l_1 to obtain

$$a_i = q_i l_1 + r_i, \quad 0 \leq r_i < l_1.$$

We have

$$v = l_1(v_1 + \sum_{i=2}^n q_i v_i) + \sum_{i=2}^n r_i v_i.$$

There is no difficulty in seeing that $(v_1 + \sum_{i=2}^n q_i v_i, v_2, \dots, v_n)$ is a basis of G. As l_1 is minimal, $r_i = 0$, for all i. Noting $w_1 = v_1 + \sum_{i=2}^n q_i v_i$, we have $v = l_1 w_1 \in H$.

Now let us note H_0 the collection of elements of H whose coefficient of w_1 in the basis $(w_1, v_2, \dots, v_n)$ is 0. H_0 is a subgroup of H and $H_0 \cap \mathbf{Z}v = \{0\}$. In fact, $H = H_0 \oplus \mathbf{Z}v$. To show this it remains to prove that $H = H_0 + \mathbf{Z}v$. Let $h = b_1 w_1 + \sum_{i=2}^n b_i v_i \in H$. Dividing b_1 by l_1, we obtain

$$b_1 = m_1 l_1 + s_1, \quad 0 \leq s_1 < l_1,$$

and

$$\begin{aligned} h - m_1 v &= (b_1 w_1 + \sum_{i=2}^n b_i v_i) - (m_1 l_1 w_1) \\ &= (b_1 - m_1 l_1) w_1 + \sum_{i=2}^n b_i v_i \\ &= s_1 w_1 + \sum_{i=2}^n b_i v_i \ \in \ H. \end{aligned}$$

As l_1 is minimal, $s_1 = 0$, which implies that $h - m_1 v \in H_0$. It follows that $H = H_0 + \mathbf{Z}v$. We have shown that $H = H_0 \oplus \mathbf{Z}v$.

Now, H_0 is included in the subgroup $G_0 = \oplus_{i=2}^n \mathbf{Z}v_i$ of G. From the induction hypothesis, G_0 has a basis $(w_2, \ldots, w_n)$ and there are integers $d_2, \ldots, d_r \in \mathbf{N}^*$ such that $d_i | d_{i+1}$, for $2 \leq i < r$ and $(d_2 w_2, \ldots, d_r w_r)$ is a basis of H_0. It is clear that $(l_1 w_1, d_2 w_2, \ldots, d_r w_r)$ is a basis of H and $(w_1, \ldots, w_n)$ a basis of G. . To finish, we only need to show that $l_1 | d_2$. We divide d_2 by l_1:

$$d_2 = a l_1 + t, \quad 0 \leq t < l_1,$$

and

$$l_1 w_1 + d_2 w_2 = l_1(w_1 + a w_2) + t w_2 \ \in \ H.$$

As $(w_1 + a w_2, w_2, \ldots, w_n)$ is a basis of G, from the minimality of l_1, we must have $t = 0$, which implies that $l_1 | d_2$. □

Free modules

Although we have already seen free modules, we first recall the definition. We define free modules over rings in much the same way as we define free groups. Indeed, a free group may be considered as a free $\mathbf{Z}$-module.

Let R be a commutative ring and M an R-module. We say that a module M over R is free if it has a basis, i.e., a subset U with the following properties:

- U is a generating set: every element $m \in M$ can be expressed in the form

  $$m = r_1 u_1 + \cdots + r_s u_s,$$

  with $r_i \in R$ and $u_i \in U$;

- U is an independant set:

  $$r_1 u_1 + \cdots + r_s u_s = 0 \Longrightarrow r_i = 0 \ \ \forall i.$$

Theorem E.5 *Any two bases of a free module M over a commutative ring R have the same cardinality.*

PROOF Let M be a free module over the ring R and I a maximal ideal of R. Then $F = R/I$ is a field. We note IM the collection of all finite sums of the form $\sum_{i=1}^m a_i x_i$, with $a_i \in I$ and $x_i \in M$. IM is a submodule of M. We now set $V = M/IM$ and define an addition on V by

$$(a + IM) + (b + IM) = (a + b) + IM.$$

We also define a scalar multiplication by

$$(r + I)(a + IM) = ra + IM.$$

Both these operations are well-defined and it is easy to check that V, with these operations, is a vector space over F.

Suppose that $\mathcal{B} = \{x_i\}$ is a basis of M and let us note $\bar{\mathcal{B}} = \{\bar{x}_i\}$, where $\bar{x}_i = x_i + IM$. We claim that $\bar{\mathcal{B}}$ is a basis of V. As $\mathcal{B}$ is a generating set of M, $\bar{\mathcal{B}}$ is a generating set of V. If $\sum_{i=1}^m \bar{a}_i \bar{x}_i = \bar{0}$, with $\bar{a}_i = a_i + I$ and $a_i \in R$, then $\sum_{i=1}^m a_i x_i \in IM$. Hence there exist

$b_1, \dots, b_n \in I$ such that $\sum_{i=1}^m a_i x_i = \sum_{i=1}^n b_i x_i$. As $\mathcal{B}$ is a basis of M, for each i, there is a b_j with $a_i = b_j$, so $a_i \in I$ and it follows that $\bar{a}_i = \bar{0}$ in F. We have shown that the $\bar{x}_i$ form an independant set and therefore a basis of V over F. As all bases of a vector space have the same cardinality, all bases of the free module M have the same cardinality. □

The common cardinality of bases of a free R-module M is referred to as to as its *rank* .

Remark It is well-known that all bases of a finite-dimensional vector space have the same cardinality. This is also the case for an infinite-dimensional vector space. Let $\mathcal{B} = \{u_i\}_{i \in I}$ and $\mathcal{B}' = \{v_j\}_{j \in J}$ be bases of the infinite-dimensional vector space V over the field F. Each x_i lies in the span of a finite set $\{y_j\}_{j \in J_i}$ of $\mathcal{B}'$. We claim that $J = \cup_{i \in I} J_i$. Clearly $\cup_{i \in I} J_i \subset J$. If $\cup_{i \in I} J_i \neq J$, then the span of the x_i is contained in the span of the y_j such that j is contained in at least one J_i. However, the span of the x_i is V, so a subset of $\mathcal{B}'$ spans V, which is impossible, because $\mathcal{B}'$ is a basis of V and hence a minimal spanning set. It follows that $J = \cup_{i \in I} J_i$, as claimed. Therefore

$$|J| = | \cup_{i \in I} J_i| \leq \sum_{i \in I} |J_i| \leq |I| \aleph_0 = |I|,$$

because the product of a pair of cardinals is equal to their maximum, if one of them is infinite. To show that $|I| \leq |J|$, we use an analogous argument. Hence all bases of an infinite-dimensional vector space have the same cardinality.

We know that if V is a vector space over a field F and the dimension of V is $n < \infty$, then there can be no independant subset of V with more than n elements. We have an analogous result for free modules.

Theorem E.6 *If M is a free module of rank $n < \infty$ over a commutative ring R, then any independant subset of M is composed of at most n elements.*

PROOF Let $\{b_1, \dots, b_m\}$ be an independant subset of M. The mapping

$$\phi : R^m \longrightarrow M, (r_1, \dots, r_m) \longmapsto \sum_{i=1}^m r_i b_i$$

is a monomorphism of R-modules. Hence there exists a monomorphism of R-modules ψ from R^m into R^n. Now let I be a maximal ideal of R and IR^n the collection of sums of the form $\sum_{i=1}^k a_i x_i$, with $a_i \in I$ and $x_i \in R^n$. The set IR^n is a submodule of R^n. We define IR^m in an analogous fashion. The mapping

$$\Psi : R^m/(IR^m) \longrightarrow R^n/(IR^n), x + IR^m \longmapsto \psi(x) + IR^n$$

is a well-defined monomorphism of R-modules. In addition, the mapping

$$\Gamma : (R/I)^m \longrightarrow R^m/(IR^m), (r_1 + I, \dots, r_m + I) \longrightarrow (r_1, \dots, r_m) + IR^m$$

is a well-defined isomorphism of R-modules. In the same way, $(R/I)^n$ is isomorphic, as an R-module, to $R^n/(IR^n)$. Therefore we have an R-module monomorphism α from $(R/I)^m$ into $(R/I)^n$. However, $(R/I)^m$ and $(R/I)^n$ are vector spaces over the field R/I. We claim that α is an R/I-linear mapping. We notice that, for $x \in (R/I)^m$ (or $x \in (R/I)^n$), $(r + I)x = rx$ and so $\alpha((r + I)x)$ is defined. Then

$$\alpha\left((r + I)x\right) = \alpha(rx) = r\alpha(x) = (r + I)\alpha(x)$$

and it follows that α is R/I-linear. As α is a linear monomorphism, we have $m \leq n$. □

Exercise E.2 *In the proof of Theorem E.6 we stated that the mapping Ψ is a monomorphism. Show that this is indeed the case.*

We may extend this result to R-modules of infinite rank.

Theorem E.7 *If M is a free module, with infinite basis $\mathcal{B}$, over a commutative ring R, and A an independant subset of M, then $|A| \leq |\mathcal{B}|$.*

PROOF The elements of A are finite linear combinations of elements of $\mathcal{B}$. For $x \in A$, we let $f(x)$ be the finite subset of $\mathcal{B}$ composed of the elements of $\mathcal{B}$ in the linear combination of x. We thus obtain a mapping of A into $\mathcal{P}_{fin}(\mathcal{B})$, the collection of finite subsets of $\mathcal{B}$. If $E \in \mathcal{P}_{fin}(\mathcal{B})$ has n elements and $\langle E \rangle$ be the R-module generated by E, then, from Theorem E.6, any independant subset of $\langle E \rangle$ has at most n elements. As $f^{-1}(E) \subset \langle E \rangle$ and is a set composed of independant elements, we have $|f^{-1}(E)| \leq n$. Thus

$$|A| = \sum_{n>0} \sum_{\substack{E \in \mathcal{P}_{fin}(\mathcal{B}) \\ |E|=n}} |f^{-1}(E)| \leq \sum_{n>0} n|\mathcal{B}|,$$

because the cardinal of the collection of finite subsets of a given infinite set is the cardinal of the set itself. We obtain

$$|A| \leq |\mathcal{B}| \sum_{n>0} n = |\mathcal{B}||\mathbf{N}^*|,$$

where we have again used the result concerning finite subsets of a given infinite set. To finish, we observe that, for two infinite cardinals X and Y, we have

$$|X||Y| = \max(|X|, |Y|)$$

and so we obtain

$$|A| \leq |\mathcal{B}|,$$

as required. □

We may use Theorem E.6 to prove another result concerning free modules.

Theorem E.8 *Let $R \subset S$ be integral domains, with respective fraction fields K and L. If S is a free R-module of rank $n < \infty$, then $[K : L] = n$.*

PROOF Let $X = \{x_1, \dots, x_m\}$ be an independant subset of the K-vector space L. Each x_i can be written in the form $\frac{u_i}{v_i}$, with $(u_i, v_i) \in S \times S^*$. If we set $v = v_1 \cdots v_m$, then the set $\{sx_1, \dots, sx_m\}$ is independant in the R-module S. From Theorem E.6, we have $m \leq n$. It follows that L is a finite extension of K and $[K : L] \leq n$.

Now let $\mathcal{B}$ be a basis of the R-module S. Clearly $\mathcal{B}$ is an independant subset of the K-vector space L, so $n \leq [K : L]$. Therefore $[K : L] = n$. □

Corollary E.1 *Under the conditions of Theorem E.8, if $\mathcal{B}$ is a basis of the free R-module S, then $\mathcal{B}$ is a basis of the K-vector space L.*

PROOF If $\mathcal{B}$ is a basis of the free R-module S, then $\mathcal{B}$ is an independant subset of the K-vector space L. From Theorem E.8, we have $\operatorname{rk} S = [K : L]$, so $\mathcal{B}$ is a basis of L. □

Torsion and free modules

Our aim here is to prove a result giving us a condition for a module to be free. However, before turning to modules, we will recall the Smith normal form of a matrix. For a ring R we will write $\mathcal{M}_{m,n}(R)$ for the collection of $m \times n$ matrices with coefficients in R. If $m = n$, i.e., in the case where the matrices are square matrices, we will use the notation $\mathcal{M}_m(R)$. We have the following result:

If R is a principal ideal domain and $A \in \mathcal{M}_{m,n}(R)$, then there exist invertible matrices $P \in \mathcal{M}_m(R)$ and $Q \in \mathcal{M}_n(R)$ such that

$$PAQ = B = \begin{bmatrix} D & X \\ Y & Z \end{bmatrix},$$

where $D = \operatorname{diag}(d_1, \ldots, d_r)$ is a diagonal matrix, with nonzero entries d_i such that $d_i | d_{i+1}$, for $i = 1, \ldots, r-1$, and X, Y and Z are matrices of zeros of respective dimensions $r \times (n-r)$, $(m-r) \times r$ and $r \times (n-r)$. The d_i are unique up to multiplication by an invertible element of R. Such a matrix B is called a *Smith normal form* of the matrix A. (A good introduction to the Smith normal form may be found in [5].)

We say that a module M over a ring R is *finitely generated* if there are $m_1, \ldots, m_s \in M$ such that every element $m \in M$ can be expressed in at least one way as

$$m = r_1 m_1 + \cdots + r_s m_s,$$

with the $r_i \in R$. The module M is *free* if it has a *basis*, i.e., a set U which has the properties:

- U is a generating set: every element $m \in M$ can be expressed as

  $$m = r_1 u_1 + \cdots + r_s u_s,$$

  with the $u_i \in U$ and the $r_i \in R$;

- U is an independant set:

  $$r_1 u_1 + \ldots + r_s u_s = 0 \Longrightarrow r_i = 0, \quad \text{for all } i.$$

We now consider modules over integral domains. If R is an integral domain and M an R-module, then an element $u \in M$ is a *torsion element* if there exists $r \in R^{\times}$ such that $ru = 0$. The torsion elements form a submodule of M, which we note tM. If $tM = 0$, then we say that M is *torsion-free*. The following result relates finitely generated, torsion-free and free modules.

Proposition E.3 *Let R be principal ideal domain and M a finitely generated R-module. Then M has a finite basis if and only if M is torsion-free.*

PROOF Suppose that M has a finite basis $U = (u_1, \ldots, u_s)$. If $m = r_1 u_1 + \cdots + r_s u_s \neq 0$, then there is at least one r_i which is nonzero. If $d \in R^*$ and $dm = 0$, then

$$(dr_1)u_1 + \cdots + (dr_i)u_i + \cdots + (dr_s)u_s = 0 \Longrightarrow dr_1 = \cdots = dr_i = \cdots = dr_s = 0,$$

because U is a basis. As R is an integral domain and $r_i \neq 0$, $d = 0$, which is a contradiction. Hence, M is torsion-free.

We now begin with the hypothesis that M is torsion-free. Let $U = (u_1, \ldots, u_s)$ be a generating set of M. We use an induction on s to show that M is free. If $s = 1$, then $M = Ru$, so $\{u\}$ is a generating set. If $ru = 0$ and $r \neq 0$, then $u \in tM$. As M is torsion-free, this si impossible, hence $U = (u)$ is a basis. Now suppose that $s > 1$ and that the result is true for up to $s - 1$ elements in a generating set. Let $r_1, \ldots, r_s \in R$, not all 0, be such that $\sum_{i=1}^{s} r_i u_i = 0$. Let C be the $1 \times s$ matrix $[r_i]$. From our discussion of the Smith normal form, we know that there are invertible matrices, $P \in \mathcal{M}_1(R)$ and $Q \in \mathcal{M}_s(R)$, such that

$$P[r_1 \ldots r_s]Q = [d\,0 \ldots 0].$$

If $P = [p]$, then p is invertible and we obtain

$$[r_1 \ldots r_s]Q = [d'\,0 \ldots 0],$$

where $d' = p^{-1}d$. If we set $V = Q^{-1}U$, then $V = (v_1, \ldots, v_s)$ clearly generates M. Also,

$$0 = [r_1 \ldots r_s]U = [r_1 \ldots r_s]QV = [d'\,0 \ldots 0]V \Longrightarrow d'v_1 = 0.$$

As $d' \neq 0$ and M is torsion-free, $v_1 = 0$. Hence, the set $(v_1, \ldots, v_s)$ generates M. By the induction hypothesis, M has a finite basis. This finishes the proof. $\square$

Appendix F

The Chinese remainder theorem

We give two versions of the Chinese remainder theorem, one as a corollary of the other. We recall that two ideals I and J in a commutative ring R are said to be coprime if $I + J = R$.

Theorem F.1 *Let $I_1, \ldots, I_n$ be ideals in a commutative ring A which are coprime in pairs, i.e., $I_i + I_j = R$ if $i \neq j$. If $a_1, \ldots, a_n \in R$, then there exists a solution $\alpha \in R$ to the system of congruences*

$$\begin{aligned} x &\equiv a_1 \; (mod\, I_1) \\ \vdots \quad &\quad \vdots \qquad \vdots \\ x &\equiv a_n \; (mod\, I_n). \end{aligned}$$

Any two solutions are congruent modulo $I_1 \cap \cdots \cap I_n$.

PROOF We fix i and take $j \neq i$. As $I_i + I_j = R$, there exist $b_j \in I_i$, $c_j \in I_j$ such that $b_j + c_j = 1$. Then

$$\prod_{j \neq i} (b_j + c_j) = 1.$$

We now expand the left hand side of the equation to obtain $x_i + y_i = 1$, where x_i is the sum of the terms containing a b_j and $y_i = \prod_{j \neq i} c_j$. Then

$$y_i \equiv 1 \text{ (mod } I_i) \qquad \text{and} \qquad y_i \equiv 0 \text{ (mod } I_j), j \neq i.$$

We now set

$$\alpha = a_1 y_1 + a_2 y_2 + \cdots + a_n y_n.$$

Clearly α has the required properties.

If β is another solution to the system of congruences, then $\beta \equiv a_i(\text{mod } I_i)$, for all i. This is equivalent to saying that $\beta - \alpha \equiv 0(\text{mod } I_i)$, for all i, which in turn is equivalent to the statement $\beta - \alpha \in \cap_{i=1}^n I_i$, i.e., $\beta \equiv \alpha(\text{mod } \cap_{i=1}^n I_i)$. □

Corollary F.1 *Under the conditions of the theorem*

$$R/(\cap_{i=1}^n I_i) \simeq R/I_1 \times \cdots \times R/I_n.$$

PROOF We define a mapping ϕ from R into $\prod_{i=1}^{n} R/I_i$ by setting

$$\phi(x) = (x + I_1, \ldots, x + I_n).$$

It is not difficult to see that ϕ is a ring homomorphism. From Theorem F.1, we know that, if $(a_1, \ldots, a_n) \in R^n$, then there exists an $a \in R$ such that $a \equiv a_i (\text{mod } I_i)$, for all i. It follows that the mapping ϕ is surjective. As $\operatorname{Ker} \phi = \cap_{i=1}^{n} I_i$, we have

$$R/(\cap_{i=1}^{n} I_i) \simeq R/I_1 \times \cdots \times R/I_n,$$

from the first isomorphism theorem for rings. □

Appendix G

Lattices in euclidian space

A subgroup Λ of the additive group of $\mathbf{R}^n$ is said to be *discrete* if there exists an open ball of radius $\epsilon > 0$, centered on the origin, $B(0, \epsilon)$, such that $B(0, \epsilon) \cap \Lambda = \{0\}$. If, in addition, the span of Λ is $\mathbf{R}^n$, then we say that Λ is a *lattice in* $\mathbf{R}^n$, or, more briefly, a lattice.

Example If $V = \{v_1, \ldots, v_n\}$ is an independant set in $\mathbf{R}^n$, then the set

$$\Lambda = \{v \in \mathbf{R}^n : v = \sum_{i=1}^{n} a_i v_i, a_i \in \mathbf{Z}\} \tag{G.1}$$

is a lattice. In the case where $v_i = e_i$, where $(e_i)_{i=1}^n$ is the standard basis of $\mathbf{R}^n$, then we call this lattice the *standard integer lattice in* $\mathbf{R}^n$.

<u>Bases of lattices</u>

If $\{v_1, \ldots, v_k\}$ is an independant set in $\mathbf{R}^n$ such that the lattice Λ can be written

$$\Lambda = \{v \in \mathbf{R}^n : v = \sum_{i=1}^{n} a_i v_i, a_i \in \mathbf{Z}\},$$

then we say that $(v_i)_{i=1}^n$ is a *basis of* Λ. Our first task is to show that all lattices have a basis, hence they are of the form $(G.1)$.

Lemma G.1 *Let $\Lambda \subset \mathbf{R}^n$ be a lattice and $b_1, \ldots, b_k$, with $k < n$, be linearly independant. We set $L = span(b_1, \ldots, b_k)$. Then there exists a point $v \in \Lambda \setminus L$ which minimizes the distance to L.*

PROOF Let A be the closed parallelepiped generated by $b_1, \ldots, b_k$:

$$A = \{u \in \mathbf{R}^n : u = \sum_{i=1}^{k} \alpha_i b_i,\ 0 \leq \alpha_i \leq 1\}.$$

A is a compact subset of $\mathbf{R}^n$. We claim that there there is a point $v \in \Lambda \setminus L$ which minimizes the distance to A. To see this, we first choose $a \in \Lambda \setminus L$ and set $\rho = \mathrm{dist}\,(a, A)$. We note

$$A_\rho = \{u \in \mathbf{R}^n : \mathrm{dist}\,(u, A) \leq \rho\}.$$

As A_ρ is closed and bounded, it is compact. If $A_\rho \cap \Lambda$ is infinite, then it contains a convergent subsequence (x_n) composed of distinct elements. By hypothesis, there is an open ball $B(0,\epsilon)$ such $B(0,\epsilon) \cap \Lambda = \{0\}$. As Λ is a subgroup of the additive group of $\mathbf{R}^n$, $x_s - x_t \in \Lambda$, when $s \neq t$, so $\|x_s - x_t\| \geq \epsilon$. This implies that the sequence (x_n) is not convergent and it follows that the set $A_\rho \cap \Lambda$ is finite. Also, as $a \in A_\rho \cap \Lambda$, there are points in this set which are not in L. Hence $A_\rho \cap \Lambda \setminus L \neq \emptyset$ and this set is finite. We may thus choose $v \in A_\rho \cap \Lambda \setminus L$ which minimizes the distance to A. Clearly, v minimizes the distance from $\Lambda \setminus L$ to A, which establishes the claim.

Let $w \in \Lambda \setminus L$ and $y \in L$. Then

$$y = \sum_{i=1}^{k} \gamma_i b_i,$$

with $\gamma_i \in \mathbf{R}$. If we set

$$z = \sum_{i=1}^{k} \lfloor \gamma_i \rfloor b_i,$$

then $z \in \Lambda$, hence $w - z \in \Lambda$. Also, $w - z \notin L$. (If $w - z \in L$, then $w = (w-z) + z \in L$, a contradiction.) Therefore $w - z \in \Lambda \setminus L$. In addition,

$$y - z = \sum_{i=1}^{k} (\gamma_i - \lfloor \gamma_i \rfloor) b_i \in A,$$

therefore

$$\operatorname{dist}(w,y) = \operatorname{dist}(w-z, y-z) \geq \operatorname{dist}(w-z, A) \geq \operatorname{dist}(v, A) = \operatorname{dist}(v, L)$$

and so v minimizes the distance from $\Lambda \setminus L$ to L. □

We need another preliminary result.

Lemma G.2 *Let $\Lambda \subset \mathbf{R}^n$ be a lattice and $b_1, \ldots, b_n \in \Lambda$ independant. We set $L_0 = \{0\}$ and $L_k = span(b_1, \ldots, b_k)$, for $k = 1, \ldots, n$. Then , for $k = 1, \ldots, n$, there exists $u_k \in (L_k \cap \Lambda) \setminus L_{k-1}$ which minimizes the distance from $(L_k \cap \Lambda) \setminus L_{k-1}$ to L_{k-1}.*

PROOF Let ϕ be the linear isomorphism from L_k onto $\mathbf{R}^k$ defined by

$$\phi(\alpha_1 b_1 + \cdots + \alpha_k b_k) = (\alpha_1, \ldots, \alpha_k).$$

It is not difficult to see that $\phi(L_k \cap \Lambda)$ is a lattice in $\mathbf{R}^k$. From Lemma G.1 we know that there is a point $u \in \phi(L_k \cap \Lambda) \setminus \phi(L_{k-1})$ which minimizes the distance to $\phi(L_{k-1})$. It follows that $\phi^{-1}(u)$ minimizes the distance from $(L_k \cap \Lambda) \setminus L_{k-1}$ to L_{k-1}. □

We may now show that every lattice has a basis. We remark that any lattice Λ in $\mathbf{R}^n$, from the definition of a lattice, must contain a set of n independant vectors. We may see this in the following way: Each vector e_i of the standard basis is a linear combination of a finite number of elements of Λ. Taking all the elements of Λ in these linear combinations, we obtain a finite generating set of $\mathbf{R}^n$, from which we may extract a minimum generating set of $\mathbf{R}^n$, i.e., a basis.

Notation We will write $\{x\}$ for the fractional part of the number $x \in \mathbf{R}$, i.e., $\{x\} = x - \lfloor x \rfloor$.

Theorem G.1 *Let $\Lambda \subset \mathbf{R}^n$ be a lattice and $b_1, \ldots, b_n \subset \Lambda$ independant. We define $L_0, L_1, \ldots, L_n$ an in Lemma G.2. From the same lemma, we know that there exists $u_k \in (L_k \cap \Lambda) \setminus L_{k-1}$ minimizing the distance to L_{k-1}. Then the vecteurs $u_1, \ldots, u_n$ form a basis of the lattice Λ.*

PROOF Let us set $\Lambda_k = \Lambda \cap L_k$. We will show by induction that the set $\{u_1, \ldots, u_k\}$ is a **Z**-basis of Λ_k, i.e., an independant set such that

$$\Lambda_k = \{v \in \mathbf{R}^n : v = \sum_{i=1}^{k} a_i u_i,\ a_i \in \mathbf{Z}\}.$$

As $\Lambda = \Lambda_n$, this will be sufficient to prove the theorem.

For $k = 1$ we have

$$u_1 = \alpha_1 b_1,$$

for some $\alpha_1 \neq 0$ in **R**. If $v \in \Lambda_1$, then

$$v = \beta b_1,$$

for some $\beta \in \mathbf{R}$. We claim that $\mu = \frac{\beta}{\alpha_1}$ is an integer. If not, then $0 < \{\mu\} < 1$. Setting $u_1' = v - \lfloor \mu \rfloor u_1$, we have, since $v = \mu u_1$,

$$u_1' = \mu u_1 - \lfloor \mu \rfloor u_1 = \{\mu\} u_1.$$

However, $u_1' \in \Lambda_1 \setminus \{0\}$ and is closer to the origin than u_1, a contradiction. Thus $\frac{\beta}{\alpha_1} \in \mathbf{Z}$. It now follows that

$$v = \beta b_1 = \frac{\beta}{\alpha_1} u_1,$$

with $\frac{\beta}{\alpha_1} \in \mathbf{Z}$. So $\{u_1\}$ is a **Z**-basis of Λ_1.

We now suppose that the result is true for $k-1$ and consider the case k. If

$$x = \sum_{i=1}^{k} \gamma_i b_i \in L_k,$$

then, since L_{k-1} is a vector space,

$$\operatorname{dist}(x, L_{k-1}) = \operatorname{dist}(\gamma_k b_k, L_{k-1}) = |\gamma_k| \operatorname{dist}(b_k, L_{k_1}).$$

Also,

$$u_k = \sum_{i=1}^{k} \alpha_i b_i,$$

with $\alpha_1, \ldots, \alpha_k \in \mathbf{R}$ and $\alpha_k \neq 0$. If $v \in \Lambda_k$, then

$$v = \sum_{i=1}^{k} \beta_i b_i,$$

with $\beta_1, \ldots, \beta_k \in \mathbf{R}$. We claim that $\mu = \frac{\beta_k}{\alpha_k}$ is an integer. If this is not the case, then $0 < \{\mu\} < 1$. We set $u_k' = v - \lfloor \mu \rfloor u_k$. Then

$$\begin{aligned}
u_k' &= v - \mu u_k + \{\mu\} u_k \\
&= \sum_{i=1}^{k} \beta_i b_i + \beta_k b_k - \frac{\beta_k}{\alpha_k}\left(\sum_{i=1}^{k-1} \alpha_i b_i + \alpha_k b_k\right) + \{\mu\}\left(\sum_{i=1}^{k-1} \alpha_i b_i + \alpha_k b_k\right) \\
&= \sum_{i=1}^{k-1} \beta_i b_i - \lfloor \mu \rfloor \sum_{i=1}^{k-1} \alpha_i b_i + \{\mu\} \alpha_k b_k \\
&= \sum_{i=1}^{k-1} (\beta_i - \lfloor \mu \rfloor \alpha_i) b_i + \{\mu\} \alpha_k b_k.
\end{aligned}$$

The element u'_k belongs to $\Lambda_k \setminus L_{k-1}$ and the distance from u'_k to L_{k-1} is that of $\{\mu\}\alpha_k b_k$. However, the distance of $\{\mu\}\alpha_k b_k$ to L_{k-1} is that of $\{\mu\}u_k$, which is strictly less than that of u_k, a contradiction. Hence $\mu = \frac{\beta_k}{\alpha_k} \in \mathbf{Z}$, as claimed. Therefore $v - \mu u_k \in \Lambda_{k-1}$. Applyinging the induction hypothesis we obtain that $v - \mu u_k$ is an integer linear combination of $u_1, \ldots, u_{k-1}$ and it follows that v is an integer linear combination of $u_1, \ldots, u_k$. This finishes the induction step and hence the proof. □

Corollary G.1 *A lattice in $\mathbf{R}^n$ is a free abelian group of rank n.*

Parallelepipeds

If $\Lambda \subset \mathbf{R}^n$ is a lattice and $u = (u_i)_{i=1}^n$ a basis of Λ, then the set

$$\Pi_u = \left\{ v = \sum_{i=1}^n \alpha_i u_i : 0 \leq \alpha_i < 1, \right\}$$

is called the *fundamental parallelepiped of the basis u*. If the basis u is understood, then we usually write Π in place of Π_u.

Proposition G.1 *If Π is a fundamental parallelepiped of the lattice Λ, then, for each element $x \in \mathbf{R}^n$, there exist unique elements $y \in \Lambda$ and $z \in \Pi$ such that $x = y + z$.*

PROOF Let us consider the fundamental parallelepiped $\Pi = \Pi_u$ of the basis u. As u is a basis of $\mathbf{R}^n$, we can write $x = \sum_{i=1}^n \alpha_i u_i$, with $\alpha_i \in \mathbf{R}$. If we set

$$y = \sum_{i=1}^n \lfloor \alpha_i \rfloor u_i \qquad \text{and} \qquad z = \sum_{i=1}^n \{\alpha_i\} u_i,$$

then $y \in \Lambda$, $z \in \Pi$ and $x = y + z$.

Suppose now that there two decompositions: $x = y_1 + z_1 = y_2 + z_2$. Then

$$z_1 = \sum_{i=1}^n \alpha_i u_i \qquad \text{and} \qquad z_2 = \sum_{i=1}^n \beta_i u_i,$$

with $0 \leq \alpha_i < 1$ and $0 \leq \beta_i < 1$, for all α_i, β_i. We obtain

$$y_1 - y_2 = z_2 - z_1 = \sum_{i=1}^n \gamma_i u_i,$$

with $\gamma_i = \beta_i - \alpha_i$. Clearly, $|\gamma_i| < 1$. As $y_1 - y_2 \in \Lambda$, we must have $\gamma_i = 0$, for all γ_i, which implies that $y_1 = y_2$ and $z_1 = z_2$. □

Corollary G.2 *Let $\Lambda \subset \mathbf{R}^n$ be a lattice and Π a fundamental parallelepiped of Λ. Then the translates $\{y + \Pi : y \in \Lambda\}$ cover $\mathbf{R}^n$ without overlapping.*

PROOF From Proposition G.1, if $x \in \mathbf{R}^n$, then $x = y + z$, with $y \in \Lambda$ and $z \in \Pi$; hence x belongs to the translate $y + \Pi$. Therefore the translates cover $\mathbf{R}^n$. If $x \in (y_1 + \Pi) \cap (y_2 + \Pi)$, then $x = y_1 + z_1 = y_2 + z_2$, with $z_1, z_2 \in \Pi$. From the uniqueness of the decomposition of x, we have $y_1 = y_2$ (and $z_1 = z_2$), so there can be no overlapping of translates. □

We recall that the volume of a Lebesgue measurable set A in $\mathbf{R}^n$ is defined by

$$\text{vol } A = \int_{\mathbf{R}^n} \chi_A(x)dx,$$

where χ_A is the characteristic function of A. The next elementary result is important for what follows.

Proposition G.2 *Let A be a Lebesgue measurable set in $\mathbf{R}^n$ and T a linear automorphism of $\mathbf{R}^n$. Then*

$$\text{vol } T(A) = |\det T| \text{vol } A.$$

PROOF Using the "change of variable" formula (see for example [20]), we have

$$\int_{\mathbf{R}^n} \chi_A(x)dx = \int_{\mathbf{R}^n} \chi_A \circ T(x)|\det T|dx = |\det T| \int_{\mathbf{R}^n} \chi_{T^{-1}(A)}(x)dx.$$

Hence

$$\text{vol } A = |\det T| \text{vol } T^{-1}(A) \Longrightarrow \text{vol } T(A) = |\det T| \text{vol } A,$$

as required. □

Corollary G.3 *If $X \subset R^n$ is Lebesgue measurable and $r > 0$, then*

$$\text{vol } rX = r^n \text{vol } X.$$

We now introduce a result which will enable us to define an important invariant of a lattice.

Theorem G.2 *Let $u = (u_i)_{i=1}^n$ and $v = (v_i)_{i=1}^n$ be bases of the lattice $\Lambda \subset \mathbf{R}^n$ and Π_u, Π_v the corresponding fundamental parallelepipeds. Then*

$$\text{vol } \Pi_u = \text{vol } \Pi_v.$$

PROOF Let T be the linear automorphism of $\mathbf{R}^n$ defined by

$$T(u_i) = v_i,$$

for $i = 1, \ldots, n$. The matrix of T in the basis u is the matrix representation A of the basis v in terms of the basis u. The coefficients are integers, since each $v_i \in \Lambda$ and u is a basis of Λ. Similarly, the matrix representation B of the basis u in terms of the basis v has only integer coefficients. As $AB = BA = I_n$, we have $|\det T| = 1$. Therefore, from Proposition G.2,

$$\text{vol } T(\Pi_u) = \text{vol } \Pi_u.$$

As $T(\Pi_u) = \Pi_v$, we have the result. □

The volume of a fundamental parallelepiped of a lattice is called the *determinant of the lattice*. For the determinant of the lattice Λ, we write $\det \Lambda$. If $u = (u_i)_{i=1}^n$ is a basis of Λ, $e = (e_i)_{i=1}^n$ the standard basis of $\mathbf{R}^n$ and T the linear automorphism defined by

$$T(e_i) = u_i,$$

for $i = 1, \ldots, n$, then from Proposition G.2 we have

$$\text{vol } \Pi_u = \text{vol } T(\Pi_e) = |\det T| \text{vol } \Pi_e.$$

As vol $\Pi_e = 1$ and $\det T$ is the determinant of the matrix U whose columns are the vectors $u_1, \ldots, u_n$, we have

$$\det \Lambda = |\det U|.$$

This justifies the use of the term $\det \Lambda$ for the volume of a fundamental parallelepiped Π_u.

Minkowski's convex body theorem

In order to prove Minkowski's theorem we will prove another result, namely Blichfeldt's theorem.

Theorem G.3 *(Blichfeldt) Let Λ be a lattice in $\mathbf{R}^n$ and X a Lebesgue measurable set in $\mathbf{R}^n$ such that* vol $X > \det \Lambda$. *Then there are distinct points $x_1, x_2 \in X$ such that $x_1 - x_2 \in \Lambda$.*

PROOF Let Π be a fundamental parallelepiped of Λ. For each $y \in \Lambda$, we set

$$X_y = ((\Pi + y) \cap X) - y.$$

Then $X_y + y = (\Pi + y) \cap X$. From Corollary G.2 these sets form a partition of X. Therefore

$$\sum_{y \in \Lambda} \text{vol } (X_y + y) = \text{vol } X > \det \Lambda = \text{vol } \Pi.$$

We now set

$$f(x) = \sum_{y \in \Lambda} \chi_{X_y}(x),$$

for all $x \in \mathbf{R}^n$. Then

$$\sum_{y \in \Lambda} \int_{\Pi} \chi_{X_y}(x) dx = \sum_{y \in \Lambda} \text{vol } (X_y \cap \Pi) = \sum_{y \in \Lambda} \text{vol } (X_y \cap \Pi + y),$$

by the invariance of Lebesgue measure with repect to translation. Consequently,

$$\int_{\Pi} f(x) dx = \sum_{y \in \Lambda} \text{vol } \big((X_y + y) \cap (\Pi + y)\big) = \sum_{y \in \Lambda} \text{vol } (X_y + y) > \text{vol } \Pi.$$

From this we deduce that

$$\int_{\Pi} (f(x) - 1) dx > 0$$

and so $f(x) > 1$ for some $x \in \Pi$. As $f(x) \in \mathbf{N} \cup \{+\infty\}$, we must have $f(x) \geq 2$, which implies that there exist distinct values elements $y_1, y_2 \in \Lambda$ such that $X_{y_1} \cap X_{y_2} \neq \emptyset$. Let $z \in X_{y_1} \cap X_{y_2}$. Then

$$z + y_1 = x_1 \in X \qquad \text{and} \qquad z + y_2 = x_2 \in X,$$

which implies that $x_1 - x_2 = y_1 - y_2 \in \Lambda$. □

We may now prove Minkowski's convex body theorem.

Theorem G.4 *(Minkowski) Let $\Lambda \subset \mathbf{R}^n$ be a lattice and A a convex subset of $\mathbf{R}^n$, with* vol $A > 2^n \det \Lambda$. *In addition suppose that A is centrally symmetric. Then A contains a nonzero lattice point. If A is compact, then it is sufficient to suppose that* vol $A \geq 2^n \det \Lambda$.

PROOF We set $X = \frac{1}{2}A$. From Corollary G.3,

$$\text{vol } X = \frac{1}{2^n}\text{vol } A > \det \Lambda.$$

By Theorem G.4 there exist distinct elements $x_1, x_2 \in X$ such that $x = x_1 - x_2 \in \Lambda$. Now, $2x_1, 2x_2 \in A$ and, as A is symmetric about the origin, $-2x_2 \in A$. Since A is convex, we have

$$x = x_1 - x_2 = \frac{1}{2}(2x_1) + \frac{1}{2}(-2x_2) \in A.$$

Now we consider the case where A is compact and vol $A = 2^n \det \Lambda$. Let $\rho > 1$. Then, by Corollary G.3,

$$\text{vol } \rho A = \rho^n \text{vol } A > 2^n \det \Lambda,$$

so there is a nonzero lattice point x_ρ in ρA. Now let (ρ_n) be a sequence in $(1, +\infty)$ converging to 1. Then $(\frac{x_{\rho_n}}{\rho_n})$ is a sequence in A. As A is compact, the sequence has a convergent subsequence $(\frac{x_{\rho_m}}{\rho_m})$. If $x = \lim \frac{x_{\rho_m}}{\rho_m}$, then $x = \lim x_{\rho_m}$. For m, n sufficiently large, $x_{\rho_m} - x_{\rho_n} = 0$, because Λ is a discrete group. This implies that $x = x_{\rho_m}$ for some m, hence $x \in \Lambda$. Also, as $x_{\rho_m} \neq 0$, $x \neq 0$. □

Sublattices

If $\Lambda, \Lambda_0 \subset \mathbf{R}^n$ are lattices and $\Lambda_0 \subset \Lambda$, then we say that Λ_0 is a *sublattice* of Λ. As Λ_0 is a subgroup of Λ, we may consider the index of Λ_0 in Λ.

Proposition G.3 *The index of Λ_0 in Λ, $[\Lambda : \Lambda_0]$, is finite.*

PROOF We fix the fundamental parallelepipeds Π and Π_0 of Λ and Λ_0 respectively. Let $x + \Lambda_0$ be a coset in the quotient group Λ/Λ_0. From Proposition G.1 there is a unique decomposition $x = y + z$, with $y \in \Lambda_0$ and $z \in \Pi_0$. As $x, y \in \Lambda$, we have $z \in \Lambda$. It follows that z is a representative of the coset $x + \Lambda_0$: each coset has a representative in $\Lambda \cap \Pi_0$. As Λ is a discrete group and Π_0 a compact set, the set $\Lambda \cap \Pi_0$ is finite, there can only be a finite number of cosets.□

In fact, we can determine $[\Lambda : \Lambda_0]$ from the determinants of the two lattices. We claim that, if $x_1 + \Lambda_0 = x_2 + \Lambda_0$, with $x_1, x_2 \in \Lambda \cap \Pi_0$, then $x_1 = x_2$. First we notice that $x_1 - x_2 \in \Lambda$, because both $x_1, x_2 \in \Lambda$. If $v = (v_1, \ldots, v_n)$ is a basis of Λ_0, then the coefficients of x_1 and x_2 in this basis have values in the interval $[0, 1)$, which implies that the coefficients of $x_1 - x_2$ have values in the interval $(-1, 1)$. Since $x_1 - x_2 \in \Lambda_0$, these coefficients are integers, hence the only possible value is 0 and so $x_1 = x_2$, as claimed. It follows that there are exactly $|\Lambda \cap \Pi_0|$ cosets in Λ/Λ_0.

The lattice Λ is a free abelian group of rank n and the sublattice Λ_0 is also a free abelian group of the same rank. From Theorem E.4, there exists a basis $(u_1, \ldots, u_n)$ of Λ for which there exist integers $d_1, \ldots, d_n \in \mathbf{N}^*$ such that $(d_1u_1, \ldots, d_nu_n)$ is a basis of Λ_0. If $x \in \Lambda \cap \Pi_0$, then

$$x = a_1u_1 + \cdots + a_nu_n = b_1d_1u_1 + \cdots + b_nd_nu_n,$$

where $a_i \in \mathbf{Z}$ and $0 \leq b_i < 1$. As $a_i, d_i \in \mathbf{Z}$, we have $b_i = \frac{a_i}{d_i} \in \mathbf{Q}$. Given that $0 \leq b_i < 1$, we have d_i possibilities for b_i, namely $0, \frac{1}{d_i}, \ldots, \frac{d_i-1}{d_i}$. It follows that $0, 1, \ldots, d_i - 1$ are the only possibilities for a_i. Therefore for x there are $d_1 \cdots d_n$ possibilities, i.e., $|\Lambda/\Lambda_0| = d_1 \cdots d_n$.

We now consider the automorphism T of $\mathbf{R}^n$ defined by

$$T(u_i) = d_iu_i,$$

for $i = 1, \dots, n$. We now suppose that Π is the fundamental parallalepiped of Λ corresponding to the basis (u_i) and Π_0 that of Λ_0 corresponding to the basis $(d_i u_i)$. As $|\det T| = d_1 \cdots d_n$, from Proposition G.2 we have

$$\mathrm{vol}\, \Pi_0 = d_1 \cdots d_n \mathrm{vol}\, \Pi.$$

We have shown that

Theorem G.5

$$[\Lambda : \Lambda_0] = \frac{\det \Lambda_0}{\det \Lambda}.$$

We defined a lattice in $\mathbf{R}^n$ at the beginning of this appendix as a discrete subgroup whose span is $\mathbf{R}^n$. We now consider the case where we do not have a condition on the span.

Theorem G.6 *If H is a discrete, nontrivial subgroup of $\mathbf{R}^n$, then H is isomorphic to a lattice in $\mathbf{R}^r$, where r is the dimension of the vector subspace generated by H.*

PROOF Let $e_1, \dots, e_r \in H$ be a maximal linearly independant subset in H and T the fundamental domain defined by the e_i, i.e.,

$$T = \{x \in \mathbf{R}^n : x = \sum_{i=1}^r a_i e_i,\ 0 \le a_i < 1\}.$$

The closure of T is

$$\bar{T} = \{x \in \mathbf{R}^n : x = \sum_{i=1}^r a_i e_i,\ 0 \le a_i \le 1\}.$$

If $x \in H$, then $x = \sum_{i=1}^r b_i e_i$, with $b_i \in \mathbf{R}$. For an integer j we set $x_j = jx - \sum_{i=1}^r \lfloor jb_i \rfloor e_i$. We claim that $x_j \in H \cap T$. As $x_j = \sum_{i=1}^r (jb_i - \lfloor jb_i \rfloor) e_i$ and $0 \le jb_i - \lfloor jb_i \rfloor < 1$, we have $x_j \in T$. Also, H is a subgroup of $\mathbf{R}^n$, so $\lfloor jb_i \rfloor e_i \in H$, for all i, and so their sum is also in H. Clearly $jx \in H$, hence $x_j \in H$. This proves the claim.

If we take $j = 1$, then we have $x_1 = x - \sum_{i=1}^r \lfloor b_i \rfloor e_i \in H \cap T$. As H is discrete $H \cap \bar{T}$ is a finite set, because $\bar{T}$ is compact. It follows that $H \cap T$ is also finite, so there exist only a finite number of choices for x_1 and it follows that H is generated by the distinct values of the x_1 and the e_i. (Any element $y \in H$ is the translation of an element $x \in H \cap T$ by a sum of the form $u = \sum_{i=1}^r a_i e_i$, with $a_i \in \mathbf{Z}$, which belongs to H.)

Our next step is to show that the b_i are rational. As there are only a finite number of distinct elements in $H \cap T$ and all the x_j belong to this set, there must be $x_j = x_k$, with $j \ne k$. Then, using the linear independance of the e_i, we obtain

$$(j - k) b_i = \lfloor jb_i \rfloor - \lfloor kb_i \rfloor,$$

for all i, and it follows that the b_i are rational.

Since the distinct values of x_1 are linear combinations of the e_i with rational coefficients, H is generated by a finite number of linear combinations of the e_i with rational coefficients. If d is the *lcm* of the denominators of these coefficients, then $d \ne 0$ and $dH \subset \sum_{i=1}^r \mathbf{Z} e_i$. Thus dH is a subgroup of a free abelian group of rank r, hence is free of rank at most r. Given that $dH \simeq H$, H is free, and since $H \supset \sum_{i=1}^r \mathbf{Z} e_i$, the rank of H is at least r, and hence exactly r. Since H is a free abelian group of rank r, it is isomorphic to the standard integer lattice $\mathbf{Z}^r$ of $\mathbf{R}^r$.

To conclude we need to show that r is equal to the dimension of the vector subspace generated by H. Let us write S for this subspace and A for the subspace generated by the e_i. It is sufficient to show that $S = A$. In the previous part of the proof we showed that H is generated by a finite number of linear combinations of the e_i with rational coefficients, thus $S \subset A$. However, S must contain all linear combinations of the e_i, hence $A \subset S$. Therefore $S = A$, as required. □

Appendix H

Kronecker products of matrices

Let A be an $m \times n$ matrix and B a $p \times q$ matrix over a commutative ring R. The *Kronecker* (or tensor) *product* of A and B, written $A \otimes B$, is the $mp \times nq$ matrix defined as follows:

$$A \otimes B = \begin{bmatrix} a_{11}B & \dots & a_{1n}B \\ \vdots & & \vdots \\ a_{m1}B & \dots & a_{mn}B \end{bmatrix}$$

In general, $A \otimes B \neq B \otimes A$, because we do not have $mp = nq$. However, even if this is the case, for example when both A and B are square matrices of the same dimension, it is not in general true that $A \otimes B = B \otimes A$. For example,

$$\begin{bmatrix} 1 & 2 \\ 3 & 4 \end{bmatrix} \otimes \begin{bmatrix} 1 & 0 \\ 2 & 3 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 2 & 0 \\ 2 & 3 & 4 & 6 \\ 3 & 0 & 4 & 0 \\ 6 & 9 & 8 & 12 \end{bmatrix}$$

and

$$\begin{bmatrix} 1 & 0 \\ 2 & 3 \end{bmatrix} \otimes \begin{bmatrix} 1 & 2 \\ 3 & 4 \end{bmatrix} = \begin{bmatrix} 1 & 2 & 0 & 0 \\ 3 & 4 & 0 & 0 \\ 2 & 4 & 3 & 6 \\ 6 & 8 & 9 & 12 \end{bmatrix}.$$

We are particularly interested in the case where R is a field F and A and B square matrices. Then $A \otimes B$ is an $mn \times mn$ matrix, with coefficients in F.

It is interesting to notice what happens when $A = I_m$. We have

$$I_m \otimes B = \mathrm{diag}\,(B \dots B),$$

i.e., $I_m \otimes B$ is a matrix with m blocks B on the diagonal and 0 elsewhere. We leave it to the reader to determine the form of the matrix $A \otimes I_n$.

Let us write c_{ij} for the column vector

$$(a_{1i}b_{1j} \dots a_{1i}b_{nj}\ a_{2i}b_{ij} \dots a_{2i}b_{nj} \dots a_{mi}b_{1j} \dots a_{mi}b_{1j} \dots a_{m_i}b_{nj})^t.$$

We notice that the pairs of indices (k, l) in $a_{ki}b_{lj}$ follow the order

$$(1,1),(1,2),\ldots,(1,n),(2,1),\ldots,(2,n),\ldots,(m,1),\ldots,(m,n).$$

We define a mapping

$$\mathcal{B} : F^m \times F^n \longrightarrow F^{mn}, (uv) \longmapsto u \otimes v,$$

where

$$u \otimes v = (u_1v_1, \ldots, u_1v_n, u_2v_1, \ldots, u_2v_n, \ldots, u_mv_1, \ldots, u_mv_n).$$

The mapping $\mathcal{B}$ is clearly bilinear. Also, if $(e_i)_{i=1}^m$ (resp. $(f_j)_{j=1}^n$) is the standard basis of F^m (resp. F^n), then the products $e_i \otimes f_j$, for $1 \leq i \leq m$ and $1 \leq j \leq n$, form the standard basis of F^{mn}. It is not difficult to see that

$$(A \otimes B)(e_i \otimes f_j) = c_{ij} = Ae_i \otimes Bf_j.$$

Using the bilinearity of $\mathcal{B}$ we obtain

$$(A \otimes B)(u \otimes v) = Au \otimes Bv,$$

for every pair $(u, v) \in F^m \times F^n$.

We have seen that in general $A \otimes B \neq B \otimes A$. However, if the matrices A and B are square matrices, then $A \otimes B$ and $B \otimes A$ are conjugate, i.e., there exists an invertible $mn \times mn$ matrix P such that

$$P(A \otimes B)P^{-1} = B \otimes A.$$

To see this, let ϕ be the linear endomorphism defined on F^{mn} by the matrix $A \otimes B$ and the ordered basis

$$B_1 = (e_1 \otimes f_I, \ldots, e_1 \otimes f_n, \ldots, e_m \otimes f_1, \ldots, e_m \otimes f_n).$$

The coordinates of $\phi(e_i \otimes f_j)$ in this basis are the elements of the column vector c_ij. Suppose now that we order the basis elements differently to obtain the new ordered basis

$$B_2 = (e_1 \otimes f_1, \ldots, e_m \otimes f_1, e_1 \otimes f_2, \ldots, e_m \otimes f_2, \ldots, e_1 \otimes f_n, \ldots, e_m \otimes f_n).$$

Then the coordinate vector of $\phi(e_i \otimes f_j)$ in this ordered basis is

$$(a_{1i}b_{1j} \; a_{2i}b_{1j} \ldots a_{mi}b_{1j} \; a_{1i}b_{2j} \ldots a_{mi}b_{2j} \ldots a_{1i}b_{nj} \ldots a_{mi}b_{nj})^t$$

However, this is the column c'_{ij} of the matrix $B \otimes A$. Hence the representation of the linear endomorphism ϕ in the bases B_1 and B_2 is $B \otimes A$ and it follows that $A \otimes B$ and $B \otimes A$ are conjugate.

We can now prove the main result of this appendix.

Theorem H.1 *Let $A \in \mathcal{M}_m(F)$ and $B \in \mathcal{M}_n(F)$. Then*

$$tr(A \otimes B) = tr(A)tr(B) \quad \textit{and} \quad \det(A \otimes B) = \det(A)^n \det(B)^m.$$

PROOF For the trace we have

$$\mathrm{tr}\,(A \otimes B) = \sum_{i=1}^m \sum_{j=1}^n a_{ii}b_{jj} = \sum_{i=1}^m a_{ii} \sum_{j=1}^n b_{jj} = \mathrm{tr}\,(A)\mathrm{tr}\,(B).$$

The determinant is more subtle. We claim that

$$A \otimes B = (A \otimes I_n)(I_m \otimes B).$$

In fact, for $u \in F^m$ and $v \in F^n$,

$$(A \otimes I_n)(I_m \otimes B)(u \otimes v) = (A \otimes I_n)(u \otimes Bv) = Au \otimes Bv = (A \otimes B)(u \otimes v),$$

which proves the claim. Now, using the fact that $A \otimes I_n$ and $I_n \otimes A$ are conjugate, we obtain

$$\det(A \otimes B) = \det(A \otimes I_n)\det(I_m \otimes B) = \det(I_n \otimes A)\det(I_m \otimes B) = \det(A)^n \det(B)^m,$$

as given in the statement of the theorem. $\square$

Corollary H.1 *$A \otimes B$ is invertible if and only if both A and B are invertible.*

Appendix I

Infinite products

Let $a_1, a_2, \ldots$ be an infinite sequence of nonzero complex numbers. We say that the infinite product $\prod_{n\geq 1} a_n$ converges if there is a number γ such that the sequence $(\prod_{i=1}^{n} a_i)$ converges to γ. An infinite product may converge to 0, even if all the elements a_n are nonzero. For example, it is sufficient to take $a_n = \frac{1}{2}$, for all n. However, we are interested in the case where γ is nonzero.

Lemma I.1 *The infinite product $\prod_{n\geq 1} a_n$ converges to a nonzero element γ if and only if, for all $\epsilon > 0$, there is an $n(\epsilon)$ such that*

$$|a_n a_{n+1} \cdots a_{n+k} - 1| < \epsilon$$

for all $n \geq n(\epsilon)$ and $k \geq 0$.

PROOF Suppose that $\prod_{n\geq 1} a_n$ converges to $\gamma \neq 0$ and let $\epsilon > 0$. Choose a positive number $\delta < |\gamma|$ such that $\frac{2\delta}{|\gamma|-\delta} < \epsilon$. There exists n_1 with the property

$$|a_1 \cdots a_i - \gamma| < \delta,$$

for all $i \geq n_1$. In particular,

$$|a_1 \cdots a_{1+i+k'} - a_1 \cdots a_{1+i}| \leq |a_1 \cdots a_{1+i+k'} - \gamma| + |\gamma - a_1 \cdots a_{1+i}| < 2\delta,$$

for all $i \geq n_1$ and $k' \geq 1$. Also,

$$\begin{aligned}
|a_1 \cdots a_{1+i+k'} - a_1 \cdots a_{1+i}| &= |a_1 \cdots a_{1+i}||a_{1+i+1} \cdots a_{1+i+k'} - 1| \\
&= |a_1 \cdots a_{1+i} - \gamma + \gamma||a_{1+i+1} \cdots a_{1+i+k'} - 1| \\
&\geq (|\gamma| - |a_1 \cdots a_{1+i} - \gamma|)|a_{1+i+1} \cdots a_{1+i+k'} - 1| \\
&> (|\gamma| - \delta)|a_{2+i} \cdots a_{1+i+k'} - 1|,
\end{aligned}$$

and so, setting $n = 2 + i$ and $k = k' - 1$, we obtain

$$|a_n \cdots a_{n+k} - 1| < \frac{2\delta}{|\gamma| - \delta} < \epsilon,$$

for all $n \geq 2 + n_1 = n(\epsilon)$ and $k \geq 0$.

We now consider the converse. Taking $\epsilon = \frac{1}{2}$, we see that there exists $n(\frac{1}{2}) \geq 1$ such that

$$\frac{3}{2} \geq |a_n \cdots a_{n+k}| \geq \frac{1}{2}, \tag{I.1}$$

for all $n \geq n(\frac{1}{2})$ and $k \geq 0$. To simplify the notation, we set $n(\frac{1}{2}) = n_2$. We consider the sequence of partial products

$$p_n = \prod_{i=n_2}^{n_2+n-1} a_i$$

and let $\epsilon > 0$. Let n be sufficiently large so that $n_2 + n \geq n(\frac{2\epsilon}{3})$. Then we have

$$\begin{aligned} |p_n - p_{n+k}| &= |a_{n_2} \cdots a_{n_2+n-1} - a_{n_2} \cdots a_{n_2+n+k-1}| \\ &= |a_{n_2} \cdots a_{n_2+n-1}||1 - a_{n_2+n} \cdots a_{n_2+n+k-1}| \leq \frac{3}{2} \cdot \frac{2\epsilon}{3} = \epsilon, \end{aligned}$$

where we have used the inequality (I.1). Thus the p_n form a Cauchy sequence and hence converge. The condition (I.1) shows that the limit is nonzero. □

Remark By Lemma I.1, if we take $\epsilon > 0$ and n is sufficiently large, then $|a_n - 1| \leq \epsilon$. Hence if the infinite product converges to a nonzero element, then $\lim a_n = 1$. Therefore, if the infinite product $\prod_{n\geq 1}(1 + a_n)$ converges, then we have $\lim a_n = 0$.

Definition The infinite product $\prod_{n\geq 1}(1 + a_n)$ is said to be absolutely convergent if the product $\prod_{n\geq 1}(1 + |a_n|)$ converges (necessarily to a nonzero element).

Lemma I.2 *The infinite product $\prod_{n\geq 1}(1+a_n)$ is absolutely convergent if and only if the infinite sum $\sum_{n\geq 1} a_n$ is absolutely convergent.*

PROOF First we notice that the function $f(x) = e^x - x - 1$ is nonnegative for $x \geq 0$: $f(0) = 0$ and $f'(x) = e^x - 1 > 0$, for $x > 0$. Then

$$\begin{aligned} |a_1| + \cdots + |a_n| &< (1 + |a_1|) \cdots (1 + |a_n|) \\ &\leq e^{|a_1|} \cdots e^{|a_n|} \\ &= e^{|a_1|+\cdots+|a_n|}. \end{aligned}$$

Therefore the sums $\sum_{i=1}^n |a_i|$ are bounded if and only if the products $\prod_{i=1}^n (1+|a_i|)$ are bounded and the result follows. □

We conclude this appendix with a fundamental theorem.

Theorem I.1 *Suppose that the infinite product $\prod_{n\geq 1}(1 + a_n)$ is absolutely convergent. Then*

- **a.** *the infinite product $\prod_{n\geq 1}(1 + a_n)$ converges to a nonzero element;*
- **b.** *the infinite product $\prod_{n\geq 1}(1 + a_n)$ is convergent after any rearrangement of the terms;*
- **c.** *all such rearrangements yield the same limit.*

PROOF **a.** From Lemma I.2 the absolute convergence of the sum $\sum_{n\geq 1} a_n$ is equivalent to the absolute convergence of the product $\prod_{n\geq 1}(1+a_n)$. Let $\epsilon > 0$. By Lemma I.1, for all n sufficiently large and all $k \geq 0$, we have

$$|(1 + |a_n|) \cdots (1 + |a_{n+k}|) - 1| < \epsilon.$$

But

$$\begin{aligned}|(1+a_n)\cdots(1+a_{n+k})-1| &\leq (1+|a_n|)\cdots(1+|a_{n+k}|)-1\\ &= |(1+|a_n|)\cdots(1+|a_{n+k}|)-1|<\epsilon,\end{aligned}$$

and so, from Lemma I.1, the product $\prod_{n\geq 1}(1+a_n)$ converges to a nonzero element.

(The first inequality merits an explanation. The expression $(1+a_n)\cdots(1+a_{n+k})-1$ is a sum of monomials in $a_n,\ldots,a_{n+k}$, whose absolute value is bounded by the sum of the corresponding monomials in $|a_n|,\ldots,|a_{n+k}|$, the value of which is $(1+|a_n|)\cdots(1+|a_{n+k}|)-1$.)

b. Let $\sigma:\mathbf{N}\longrightarrow\mathbf{N}$ be a bijection, which is not the identity. The convergence of $\sum_{n\geq 1}|a_n|$ implies that of $\sum_{n\geq 1}|a_{\sigma(n)}|$ so, by Lemma I.2, $\prod_{n\geq 1}(1+|a_{\sigma(n)}|)$ is convergent. From part **a.** we deduce that $\prod_{n\geq 1}(1+a_{\sigma(n)})$ is convergent.

c. For $n\geq 1$ we set $p_n=(1+a_1)\cdots(1+a_n)$ and $p'_n=(1+\sigma(a_1))\cdots(1+\sigma(a_n))$. Let $k_1<\cdots<k_m$ denote the elements of $\{1,\ldots,n\}\setminus\{\sigma(1),\ldots,\sigma(n)\}$ and $k'_1<\cdots<k'_l$ the elements of $\{\sigma(1),\ldots,\sigma(n)\}\setminus\{1,\ldots,n\}$. Then

$$\frac{p_n}{p'_n}=\frac{(1+a_{k_1})\cdots(1+a_{k_m})}{(1+a_{k'_1})\cdots(1+a_{k'_l})}.$$

Considering the numerator we have

$$\begin{aligned}|(1+a_{k_1})\cdots(1+a_{k_m})-1| &\leq (1+|a_{k_1}|)\cdots(1+|a_{k_m}|)-1\\ &\leq \exp(|a_{k_1}|+\cdots+|a_{k_m}|)-1\\ &< \exp\left(\sum_{i=k_1}^{\infty}|a_i|\right)-1.\end{aligned}$$

As $n\to\infty$, we have $k_1\to\infty$, so, from Lemma I.2, we have $\sum_{i\geq k_1}|a_i|\to 0$. This shows that the numerator tends to 1 as $n\to\infty$. An analogous argument shows that this is also the case for the denominator. This proves part **c.** □

Bibliography

[1] R.B. Ash, *Basic abstract algebra*, Dover, 2013.

[2] B.A. Bailey, *A general partial fraction decomposition*, www.benjamin-bailey.com

[3] R. Chapman, *Dirichlet's theorem, a real variable approach*, empslocal.ex.ac.uk, 2008.

[4] L.N. Childs, *A concrete introduction to higher algebra*, Springer, 2013.

[5] P.M. Cohn, *Introduction to ring theory*, Springer, 2000.

[6] K. Conrad, *Recognizing Galois groups S_n and A_n*, www.math.uconn.edu.

[7] G. Dresden, *On the middle coefficient of a cyclotomic polynomial*, Amer. Math. Monthly **111** (2004), 531-533.

[8] K. Ford, *The number of solutions of $\phi(x) = m$*, Ann. Math. **150** (1999), 283-311.

[9] M.-N. Gras and F. Tenoé, *Corps biquadratiques monogènes*, Manuscripta Math. **86** (1995), 63-67.

[10] M.J. Greenberg, *An elementary proof of the Kronecker-Weber theorem*, Amer. Math. Monthly **81** (1974), 601-607.

[11] K. Györy, *Sur les polynômes à coefficients entiers et de discriminant donné*, Publ. Math. Debrecen 23 (1976), 141-165.

[12] P. Henrici, *Applied and computational complex analysis, Vol 1*, Wiley, 1974.

[13] C.U. Jensen, A. Ledet, N. Yui, *Generic polynomials Constructive aspects of the Inverse Galois Problem*, Cambridge, 2002.

[14] N. Lauritzen, *Concrete abstract algebra*, Cambridge, 2003.

[15] D.A. Marcus, *Number fields*, Springer, 1977.

[16] Y. Motada, *On integral bases of certain real monogenic biquadratic fields*, Rep. Fac. Sci. Engrg. Saga Univ. Math. **33** Vol. No.1 (2004), 9-22.

[17] V. Prasolov, *Polynomials*, Springer, 2001.

[18] P. Ribenboim, *Classical theory of algebraic numbers*, Springer, 2001.

[19] J.J. Rotman, *An introduction to the theory of groups*, Springer, 1999.

[20] W.Rudin, *Real and complex analysis*, McGraw-Hill, 1987.

[21] H.N. Shapiro, *Introduction to the theory of numbers*, John Wiley and Sons, 1983.

[22] L. Soicher and J. McKay, *Computing Galois groups over the rationals*, Journal of Number Theory **20**, 273-281 (1985).

[23] K. Spindler, *Abstract algebra with applications vol 2*, Marcel Dekker, 1994.

[24] M. Spivak, *Calculus on manifolds*, W.A. Benjamin,Inc., 1965.

Index