12. Let $\mathbf{Z}$ be a $\mathbf{Z}$-module with the obvious action. Find all the submodules.

13. Let R be a ring, and let M be a finitely generated R-module. Is it true that M necessarily has only finitely many distinct R-submodules? If not, is there an extra condition on R which will lead to this conclusion?

14. An abelian group G is said to be *torsion-free* if $g \in G$, $g \neq 0$ and $kg = 0$ for $k \in \mathbf{Z}$ implies $k = 0$. Prove that a finitely generated torsion-free abelian group is a finitely generated free group.

15. By examining the proof of Theorem 1.16 carefully, or by other means, prove that if H is a subgroup of a free group G of rank n then there exists a basis $u_1, \ldots, u_n$ for G and a basis $v_1, \ldots, v_s$ for H where $s \leq n$ and $v_i = \alpha_i u_i$ $(1 \leq i \leq s)$ where the α_i are positive integers and α_i divides α_{i+1} $(1 \leq i \leq s-1)$.

2

Algebraic Numbers

In this chapter we introduce the algebraic numbers as solutions of polynomial equations with integer coefficients. Among these numbers, the major players are the solutions of equations with integer coefficients whose leading coefficient is 1. These are the algebraic integers. We shall develop a theory of factorization of algebraic integers, analogous to factorization of whole numbers. In many ways the theories are alike, but in at least one essential way—uniqueness of factorization—there are important differences. Factorization into irreducible elements depends on the ring in which the factorization is performed. In $\mathbf{Z}$ the number 5 is irreducible. The only ways to write it as a product are trivial: multiply ± 5 and ± 1. However, in $\mathbf{Z}[\sqrt{5}]$ it can be written as the non-trivial product $5 = \sqrt{5} \cdot \sqrt{5}$; moreover, it turns out that $\sqrt{5}$ cannot be further factorized in this ring. Thus 5 is irreducible in $\mathbf{Z}$, yet reducible in $\mathbf{Z}[\sqrt{5}]$.

To clarify these issues it is therefore essential to specify in which ring the factorization is to be carried out. The natural context is a ring of algebraic integers, contained in its associated algebraic number field. We begin with algebraic number fields that obey a finiteness condition: they are finite-dimensional as vector spaces over the rationals. It will follow that such a field is of the form $\mathbf{Q}[\theta]$ for a single algebraic number θ.

We introduce the conjugates of an algebraic number and the discriminant of a basis for $\mathbf{Q}[\theta]$ over $\mathbf{Q}$, using the conjugates of θ to show that the discriminant is always a non-zero rational number. Algebraic integers are defined and shown to form a ring. The ring of algebraic integers in a number field is shown to have an integral basis whose discriminant is an integer. This integer is independent of the choice of integral basis and is called the discriminant of the number field.

Finally, we introduce the norm and trace of an algebraic number, which prove to be ordinary integers when the algebraic number is an algebraic integer. Using the norm and trace in later chapters we shall be able to translate statements about algebraic integers into statements about ordinary integers which are easier to handle.

2.1 Algebraic Numbers

A complex number α will be called *algebraic* if it is algebraic over $\mathbf{Q}$, that is, it satisfies a non-zero polynomial equation with coefficients in $\mathbf{Q}$. Equivalently (clearing out denominators) we may assume the coefficients to be in $\mathbf{Z}$. We let $\mathbf{A}$ denote the set of algebraic numbers. In fact $\mathbf{A}$ is a field, by virtue of:

Theorem 2.1. *The set* $\mathbf{A}$ *of algebraic numbers is a subfield of the complex field* $\mathbf{C}$.

Proof: We use Theorem 1.11, which in this case says that α is algebraic if and only if $[\mathbf{Q}(\alpha) : \mathbf{Q}]$ is finite. Suppose that α, β are algebraic. Then

$$[\mathbf{Q}(\alpha, \beta) : \mathbf{Q}] = [\mathbf{Q}(\alpha, \beta) : \mathbf{Q}(\alpha)]\,[\mathbf{Q}(\alpha) : \mathbf{Q}]$$

Now since β is algebraic over $\mathbf{Q}$ it is certainly algebraic over $\mathbf{Q}(\alpha)$, so the first factor on the right is finite; and the second factor is also finite. Hence $[\mathbf{Q}(\alpha, \beta) : \mathbf{Q}]$ is finite. But each of $\alpha + \beta$, $\alpha - \beta$, $\alpha\beta$, and (for $\beta \neq 0$) α/β belongs to $\mathbf{Q}(\alpha, \beta)$. So all of these are in $\mathbf{A}$, and the theorem is proved. □

The whole field $\mathbf{A}$ is not as interesting, for us, as certain of its subfields. We define a *number field* to be a subfield K of $\mathbf{C}$ such that $[K : \mathbf{Q}]$ is finite. This implies that every element of K is algebraic, and hence $K \subseteq \mathbf{A}$. The trouble with $\mathbf{A}$ is that $[\mathbf{A} : \mathbf{Q}]$ is not finite (see Chapter 1, Exercise 7, or Stewart [71], Exercise 4.8, p. 55). If K is a number field then $K = \mathbf{Q}(\alpha_i, \ldots, \alpha_n)$ for finitely many algebraic numbers $\alpha_1, \ldots, \alpha_n$ (for instance, a basis for K as vector space over $\mathbf{Q}$). We can strengthen this observation considerably:

Theorem 2.2. *If* K *is a number field then* $K = \mathbf{Q}(\theta)$ *for some algebraic number* θ.

Proof: Arguing by induction, it is sufficient to prove that if $K = K_1(\alpha, \beta)$ then $K = K_1(\theta)$ for some θ, (where K_1 is a sub-field of K). Let p and

q respectively be the minimum polynomials of α, β over K_1, and suppose that over $\mathbf{C}$ these factorize as

$$\begin{aligned} p(t) &= (t - \alpha_1) \ldots (t - \alpha_n), \\ q(t) &= (t - \beta_1) \ldots (t - \beta_m), \end{aligned}$$

where we choose the numbering so that $\alpha_1 = \alpha$, $\beta_1 = \beta$. By Corollary 1.6 the α_i are distinct, as are the β_j. Hence for each i and each $k \neq 1$ there is at most one element $x \in K_1$ such that

$$\alpha_i + x\beta_k = \alpha_1 + x\beta_1.$$

Since there are only finitely many such equations, we may choose $c \neq 0$ in K_1, not equal to any of these x's, and then

$$\alpha_i + c\beta_k \neq \alpha_1 + c\beta_1$$

for $1 \leq i \leq n$, $2 \leq k \leq m$. Define

$$\theta = \alpha + c\beta.$$

We shall prove that $K_1(\theta) = K_1(\alpha, \beta)$. Obviously $K_1(\theta) \subseteq K_1(\alpha, \beta)$, and it suffices to prove that $\beta \in K_1(\theta)$ since $\alpha = \theta - c\beta$.

Now

$$p(\theta - c\beta) = p(\alpha) = 0.$$

We define the polynomial

$$r(t) = p(\theta - ct) \in K_1(\theta)[t]$$

and then β is a zero of both $q(t)$ and $r(t)$ as polynomials over $K_1(\theta)$. Now these polynomials have only one common zero, for if $q(\xi) = r(\xi) = 0$ then ξ is one of $\beta_1, \ldots, \beta_m$ and also $\theta - c\xi$ is one of $\alpha_1, \ldots, \alpha_n$. Our choice of c forces $\xi = \beta$. Let $h(t)$ be the minimum polynomial of β over $K_1(\theta)$. Then $h(t) \mid q(t)$ and $h(t) \mid r(t)$. Since q and r have just one common zero in $\mathbf{C}$ we must have $\partial h = 1$, so that

$$h(t) = t + \mu$$

for $\mu \in K_1(\theta)$. Now $0 = h(\beta) = \beta + \mu$ so that $\beta = -\mu \in K_1(\theta)$ as required. □

Example 2.3. $\mathbf{Q}(\sqrt{2}, \sqrt[3]{5})$.

We have

$$\alpha_1 = \sqrt{2}, \alpha_2 = -\sqrt{2},$$

$$\beta_1 = \sqrt[3]{5}, \beta_2 = \omega\sqrt[3]{5}, \beta_3 = \omega^2\sqrt[3]{5}$$

where

$$\omega = \tfrac{1}{2}(-1 + \sqrt{-3})$$

is a complex cube root of 1. The number $c = 1$ satisfies

$$\alpha_i + c\beta_k \neq \alpha + c\beta$$

for $i = 1, 2$, $k = 2, 3$; since the number on the left is not real in any of the four cases, whereas that on the right is. Hence $\mathbf{Q}(\sqrt{2}, \sqrt[3]{5}) = \mathbf{Q}(\sqrt{2} + \sqrt[3]{5})$.

The expression of K as $\mathbf{Q}(\theta)$ is, of course, not unique; for $\mathbf{Q}(\theta) = \mathbf{Q}(-\theta) = \mathbf{Q}(\theta + 1) = \ldots$ etc.

2.2 Conjugates and Discriminants

If $K = \mathbf{Q}(\theta)$ is a number field there will, in general, be several distinct monomorphisms $\sigma : K \to \mathbf{C}$. For instance, if $K = \mathbf{Q}(i)$ where $i = \sqrt{-1}$ then we have the possibilities

$$\begin{aligned} \sigma_1(x + iy) &= x + iy, \\ \sigma_2(x + iy) &= x - iy, \end{aligned}$$

for $x, y \in \mathbf{Q}$. The full set of such monomorphisms will play a fundamental part in the theory, so we begin with a description.

Theorem 2.4. *Let $K = \mathbf{Q}(\theta)$ be a number field of degree n over $\mathbf{Q}$. Then there are exactly n distinct monomorphisms $\sigma_i : K \to \mathbf{C}$ $(i = 1, \ldots, n)$. The elements $\sigma_i(\theta) = \theta_i$ are the distinct zeros in $\mathbf{C}$ of the minimum polynomial of θ over $\mathbf{Q}$.*

Proof: Let $\theta_1, \ldots, \theta_n$ be the (by Corollary 1.3 distinct) zeros of the minimum polynomial p of θ. Then each θ_i also has minimum polynomial p (it must divide p, and p is irreducible) and so there is a unique field isomorphism $\sigma_i : \mathbf{Q}(\theta) \to \mathbf{Q}(\theta_i)$ such that $\sigma_i(\theta) = \theta_i$. In fact, if $\alpha \in \mathbf{Q}(\theta)$ then $\alpha = r(\theta)$ for a unique $r \in \mathbf{Q}[t]$ with $\partial r < n$; and we must have

$$\sigma_i(\alpha) = r(\theta_i).$$

(See Garling [28] Corollary 2 to Theorem 7.4, p. 66; Stewart [71], Theorem 3.8, p. 43.) Conversely if $\sigma : K \to \mathbf{C}$ is a monomorphism then σ is the identity on $\mathbf{Q}$. Then we have

$$0 = \sigma(p(\theta)) = p(\sigma(\theta))$$

so that $\sigma(\theta)$ is one of the θ_i, hence σ is one of the σ_i. □

Keep this notation, and for each $\alpha \in K = \mathbf{Q}(\theta)$ define the *field polynomial* of α over K to be

$$f_\alpha(t) = \prod_{i=1}^{n}(t - \sigma_i(\alpha)).$$

As it stands, this is in $K[t]$. In fact more is true:

Theorem 2.5. *The coefficients of the field polynomial are rational numbers, so that $f_\alpha(t) \in \mathbf{Q}[t]$.*

Proof: We have $\alpha = r(\theta)$ for $r \in \mathbf{Q}[t]$, $\partial r < n$. Now the field polynomial takes the form

$$f_\alpha(t) = \prod_{i}(t - r(\theta_i))$$

where the θ_i run through all zeros of the minimum polynomial p of θ, whose coefficients are in $\mathbf{Q}$. It is easy to see that the coefficients of $f_\alpha(t)$ are of the form

$$h(\theta_1, \ldots, \theta_n)$$

where $h(t_1, \ldots, t_n)$ is a symmetric polynomial in $\mathbf{Q}[t_1, \ldots, t_n]$. By Corollary 1.14 the result follows. □

The elements $\sigma_i(\alpha)$, for $i = 1, \ldots, n$, are called the *K-conjugates* of α. Although the θ_i are distinct (and are the K-conjugates of θ) it is not always the case that the K-conjugates of α are distinct: for instance $\sigma_i(1) = 1$ for all i. The precise situation is given by:

Theorem 2.6. *With the above notation,*

(a) The field polynomial f_α is a power of the minimum polynomial p_α,

(b) The K-conjugates of α are the zeros of p_α in $\mathbf{C}$, each repeated n/m times where $m = \partial p_\alpha$ is a divisor of n,

(c) The element $\alpha \in \mathbf{Q}$ if and only if all of its K-conjugates are equal,

(d) $\mathbf{Q}(\alpha) = \mathbf{Q}(\theta)$ if and only if all K-conjugates of α are distinct.

Proof: The main point is (a). Now $q = p_\alpha$ is irreducible, and α is a zero of $f = f_\alpha$, so that $f = q^s h$ where q and h are coprime and both are monic. (This follows from factorizing f into irreducibles.) We claim that h is constant. If not, some $\alpha_i = \sigma_i(\alpha) = r(\theta_i)$ is a zero of h, where $\alpha = r(\theta)$. Hence if $g(t) = h(r(t))$ then $g(\theta_i) = 0$. Let p be the minimum polynomial of θ over $\mathbf{Q}$, and hence also of each θ_i. Then $p|g$, so that $g(\theta_j) = 0$ for all j, and in particular $g(\theta) = 0$. Therefore, $h(\alpha) = h(r(\theta)) = g(\theta) = 0$ and so q divides h, a contradiction. Hence h is constant and monic, so $h = 1$ and $f = q^s$.

(b) is an immediate consequence of (a) on referring to the definition of the field polynomial.

To prove (c), it is clear that $\alpha \in \mathbf{Q}$ implies $\sigma_i(\alpha) \in \mathbf{Q}$. Conversely if all $\sigma_i(\alpha)$ are equal then, since the zeros of $q = p_\alpha$ are distinct and $f_\alpha = q^s$, then $\partial q = 1$ and so $\alpha \in \mathbf{Q}$.

Finally for (d): if all $\sigma_i(\alpha)$ are distinct then $\partial p_\alpha = n$, and hence $[\mathbf{Q}(\alpha) : \mathbf{Q}] = n = [\mathbf{Q}(\theta) : \mathbf{Q}]$. This implies that $\mathbf{Q}(\alpha) = \mathbf{Q}(\theta)$. Conversely if $\mathbf{Q}(\alpha) = \mathbf{Q}(\theta)$ then $\partial p_\alpha = n$ and so the $\sigma_i(\alpha)$ are distinct. □

Warning. Note that the K-conjugates of α need not be elements of K. Even the θ_i need not be elements of K. For example, let θ be the real cube root of 2. Then $\mathbf{Q}(\theta)$ is a subfield of $\mathbf{R}$. The K-conjugates of θ, however, are $\theta, \omega\theta, \omega^2\theta$, where $\omega = \frac{1}{2}(-1+\sqrt{-3})$. The last two of these are nonreal, hence do not lie in $\mathbf{Q}(\theta)$.

Still with $K = \mathbf{Q}(\theta)$ of degree n, let $\{\alpha_i, \ldots, \alpha_n\}$ be a basis of K (as vector space over $\mathbf{Q}$). We define the *discriminant* of this basis to be

$$\Delta[\alpha_1, \ldots, \alpha_n] = \{\det[\sigma_i(\alpha_j)]\}^2. \tag{2.1}$$

If we pick another basis $\{\beta_1, \ldots, \beta_n\}$ then

$$\beta_k = \sum_{i=1}^{n} c_{ik}\alpha_i \qquad (c_{ik} \in \mathbf{Q})$$

for $k = 1, \ldots, n$, and

$$\det(c_{ik}) \neq 0.$$

The product formula for determinants, and the fact that the σ_i are monomorphisms (and hence the identity on $\mathbf{Q}$) shows that

$$\Delta[\beta_1, \ldots, \beta_n] = [\det(c_{ik})]^2 \Delta[\alpha_1, \ldots, \alpha_n].$$

Theorem 2.7. *The discriminant of any basis for $K = \mathbf{Q}(\theta)$ is rational and non-zero. If all K-conjugates of θ are real then the discriminant of any basis is positive.*

Proof: First we pick a basis with which we can compute: the obvious one is $\{1, \theta, \ldots, \theta^{n-1}\}$. If the conjugates of θ are $\theta_1, \ldots, \theta_n$ then

$$\Delta[1, \theta, \ldots, \theta^{n-1}] = (\det \theta_i^j)^2.$$

A determinant of the form $D = \det(t_i^j)$ is called a *Vandermonde* determinant, and has value

$$D = \prod_{1 \leq i < j \leq n} (t_i - t_j). \tag{2.2}$$

To see this, think of everything as lying inside $\mathbf{Q}[t_1, \ldots, t_n]$. Then for $t_i = t_j$ the determinant has two equal rows, so vanishes. Hence D is divisible by each $(t_i - t_j)$. To avoid repeating such a factor twice we take $i < j$. Then comparison of degrees easily shows that D has no other non-constant factors; comparing coefficients of $t_1 t_2^2 \ldots t_n^n$ gives 2.2.

Hence

$$\Delta = \Delta[1, \theta, \ldots, \theta^{n-1}] = [\prod(\theta_i - \theta_j)]^2.$$

Now D is antisymmetric in the t_i, so that D^2 is symmetric. Hence by the usual argument on symmetric polynomials (Corollary 1.14), Δ is rational. Since the θ_i are distinct, $\Delta \neq 0$.

Now let $\{\beta_1, \ldots, \beta_n\}$ be any basis. Then

$$\Delta[\beta_1, \ldots, \beta_n] = (\det c_{ik})^2 \Delta$$

for certain rational numbers c_{ik}, and $\det(c_{ik}) \neq 0$ so that

$$\Delta[\beta_1, \ldots \beta_n] \neq 0,$$

and is rational. Clearly if all θ_i are real then Δ is a positive real number, hence so is $\Delta[\beta_1, \ldots, \beta_n]$. □

With the above notation, Δ vanishes if and only if some θ_i is equal to another θ_j. Hence the non-vanishing of Δ allows us to 'discriminate' the θ_i, which motivates calling Δ the discriminant.

2.3 Algebraic Integers

A complex number θ is an *algebraic integer* if there is a *monic* polynomial $p(t)$ with integer coefficients such that $p(\theta) = 0$. In other words,

$$\theta^n + a_{n-1}\theta^{n-1} + \ldots + a_0 = 0$$

where $a_i \in \mathbf{Z}$ for all i.

For example, $\theta = \sqrt{-2}$ is an algebraic integer, since $\theta^2 + 2 = 0$; $\tau = \frac{1}{2}(1 + \sqrt{5})$ is an algebraic integer, since $\tau^2 - \tau - 1 = 0$. But $\phi = 22/7$ is not. It satisfies equations like $7\phi - 22 = 0$, but this is not monic; or like $\phi - 22/7 = 0$, whose coefficients are not integers; but it can be shown without difficulty that ϕ does not satisfy any monic polynomial equation with integer coefficients.

We write $\mathbf{B}$ for the set of algebraic integers. One of our aims is to prove that $\mathbf{B}$ is a subring of $\mathbf{A}$. We prepare for this by proving:

Lemma 2.8. *A complex number θ is an algebraic integer if and only if the additive group generated by all powers $1, \theta, \theta^2, \ldots$ is finitely generated.*

Proof: If θ is an algebraic integer, then for some n we have

$$\theta^n + a_{n-1}\theta^{n-1} + \ldots + a_0 = 0 \qquad (2.3)$$

where the $a_i \in \mathbf{Z}$. We claim that every power of θ lies in the additive group generated by $1, \theta, \ldots, \theta^{n-1}$. Call this group Γ. Then (2.3) shows that $\theta^n \in \Gamma$. Inductively, if $m \geq n$ and $\theta^m \in \Gamma$ then

$$\theta^{m+1} = \theta^{m+1-n}\theta^n = \theta^{m+1-n}(-a_{n-1}\theta^{n-1} - \ldots - a_0) \in \Gamma.$$

This proves that every power of θ lies in Γ, which gives one implication.

For the converse, suppose that every power of θ lies in a finitely generated additive group G. The subgroup Γ of G generated by the powers $1, \theta, \theta^2, \ldots, \theta^n$ must also be finitely generated (Proposition 1.19), so we will suppose that Γ has generators $v_1, \ldots, v_n$. Each v_i is a polynomial in θ with integer coefficients, so θv_i is also such a polynomial. Hence there exist integers b_{ij} such that

$$\theta v_i = \sum_{j=1}^{n} b_{ij} v_j.$$

This leads to a system of homogeneous equations for the v_i of the form

$$\begin{aligned}
(b_{11} - \theta)v_1 + b_{12}v_2 + \ldots + b_{1n}v_n &= 0 \\
b_{21}v_1 + (b_{22} - \theta)v_2 + \ldots + b_{2n}v_n &= 0 \\
&\ldots\ldots\ldots\ldots \\
b_{n1}v_1 + b_{n2}v_2 + \ldots + (b_{nn} - \theta)v_n &= 0.
\end{aligned}$$

Since there exists a solution $v_1, \ldots, v_n \in \mathbf{C}$, not all zero, it follows that the determinant

$$\begin{vmatrix}
b_{11} - \theta & b_{12} & \ldots & b_{1n} \\
b_{21} & b_{22} - \theta & \ldots & b_{2n} \\
\ldots & \ldots & \ldots & \ldots \\
b_{n1} & b_{n2} & \ldots & b_{nn} - \theta
\end{vmatrix}$$

is zero. Expanding this, we see that θ satisfies a monic polynomial equation with integer coefficients. □

Theorem 2.9. *The algebraic integers form a subring of the field of algebraic numbers.*

Proof: Let $\theta, \phi \in \mathbf{B}$. We have to show that $\phi + \theta$ and $\theta\phi \in \mathbf{B}$. By Lemma 2.8 all powers of θ lie in a finitely generated additive subgroup Γ_θ of $\mathbf{C}$, and all powers of ϕ lie in a finitely generated additive subgroup Γ_ϕ. But now all powers of $\theta + \phi$ and of $\theta\phi$ are integer linear combinations of elements $\theta^i\phi^j$ which lie in $\Gamma_\theta\Gamma_\phi \subseteq \mathbf{C}$. But if Γ_θ has generators $v_1, \ldots, v_n$ and Γ_ϕ has generators $w_1, \ldots, w_m$, then $\Gamma_\theta\Gamma_\phi$ is the additive group generated by all $v_i w_j$ for $1 \leq i \leq n$, $1 \leq j \leq m$. Hence all powers of $\theta + \phi$ and of $\theta\phi$ lie in a finitely generated additive subgroup of $\mathbf{C}$, so by Lemma 2.8 $\theta + \phi$ and $\theta\phi$ are algebraic integers. Hence $\mathbf{B}$ is a subring of $\mathbf{A}$. □

A simple extension of this technique allows us to prove the following useful theorem.

Theorem 2.10. *Let θ be a complex number satisfying a monic polynomial equation whose coefficients are algebraic integers. Then θ is an algebraic integer.*

Proof: Suppose that

$$\theta^n + \psi_{n-1}\theta^{n-1} + \ldots + \psi_0 = 0$$

where $\psi_0, \ldots, \psi_{n-1} \in \mathbf{B}$. Then these generate a subring Ψ of $\mathbf{B}$. The argument of Lemma 2.8 shows that all powers of θ lie inside a finitely

generated Ψ-submodule M of $\mathbf{C}$, spanned by $1, \theta, \ldots, \theta^{n-1}$. By Theorem 2.9, each ψ_i and all its powers lie inside a finitely generated additive group Γ_i with generators γ_{ij} $(1 \leq j \leq n_i)$. It follows that M lies inside the additive group generated by all elements

$$\gamma_{1j_1}, \gamma_{2j_2}, \cdots, \gamma_{n-1,j_{n-1}} \theta^k$$

$(1 \leq j_i \leq n_i,\ 0 \leq i \leq n-1,\ 0 \leq k \leq n-1)$, which is a finite set. So M is finitely generated as an additive group, and the theorem follows. □

Theorems 2.9 and 2.10 allow us to construct many new algebraic integers out of known ones. For instance, $\sqrt{2}$ and $\sqrt{3}$ are clearly algebraic integers. Then Theorem 2.9 says that numbers such as $\sqrt{2}+\sqrt{3}$, $7\sqrt{2}-41\sqrt{3}$, $(\sqrt{2})^5(1+\sqrt{3})^2$ are also algebraic integers. And Theorem 2.10 says that zeros of polynomials such as

$$t^{23} - (14 + \sqrt[5]{3})t^9 + (\sqrt[3]{2})t^5 - 19\sqrt{3}$$

are algebraic integers. It would not be easy, particularly in the last instance, to compute explicit polynomials over $\mathbf{Z}$ of which these algebraic integers are zeros; although it can in principle be done by using symmetric polynomials. In fact Theorems 2.9 and 2.10 can be proved this way.

For any number field K we write

$$\mathfrak{O} = K \cap \mathbf{B},$$

and call $\mathfrak{O}$ the *ring of integers* of K. The symbol '$\mathfrak{O}$' is a Gothic capital O (for 'order', the old terminology). In cases where it is not immediately clear which number field is involved, we write more explicitly $\mathfrak{O}_K$. Since K and $\mathbf{B}$ are subrings of $\mathbf{C}$ it follows that $\mathfrak{O}$ is a subring of K. Further $\mathbf{Z} \subseteq \mathbf{Q} \subseteq K$ and $\mathbf{Z} \subseteq \mathbf{B}$ so $\mathbf{Z} \subseteq \mathfrak{O}$.

The following lemma is easy to prove:

Lemma 2.11. *If $\alpha \in K$ then for some non-zero $c \in \mathbf{Z}$ we have $c\alpha \in \mathfrak{O}$.*

Corollary 2.12. *If K is a number field then $K = \mathbf{Q}(\theta)$ for an algebraic integer θ.*

Proof: We have $K = \mathbf{Q}(\phi)$ for an algebraic number ϕ by Theorem 2.2. By Lemma 2.11, $\theta = c\phi$ is an algebraic integer for some $0 \neq c \in \mathbf{Z}$. Clearly $\mathbf{Q}(\phi) = \mathbf{Q}(\theta)$. □

Warning. For $\theta \in \mathbf{C}$ let us write $\mathbf{Z}[\theta]$ for the set of elements $p(\theta)$, for polynomials $p \in \mathbf{Z}[t]$. If $K = \mathbf{Q}(\theta)$ where θ is an algebraic integer then

certainly $\mathfrak{O}$ contains $\mathbf{Z}[\theta]$ since $\mathfrak{O}$ is a ring containing θ. However, $\mathfrak{O}$ need not equal $\mathbf{Z}[\theta]$. For example, $\mathbf{Q}(\sqrt{5})$ is a number field and $\sqrt{5}$ an algebraic integer. But

$$\frac{1+\sqrt{5}}{2}$$

is a zero of $t^2 - t - 1$, hence an algebraic integer; and it lies in $\mathbf{Q}(\sqrt{5})$ so belongs to $\mathfrak{O}$. It does not belong to $\mathbf{Z}[\sqrt{5}]$.

There is a useful criterion, in terms of the minimum polynomial, for a number to be an algebraic integer:

Lemma 2.13. *An algebraic number α is an algebraic integer if and only if its minimum polynomial over $\mathbf{Q}$ has coefficients in $\mathbf{Z}$.*

Proof: Let p be the minimum polynomial of α over $\mathbf{Q}$, and recall that this is monic and irreducible in $\mathbf{Q}[t]$. If $p \in \mathbf{Z}[t]$ then α is an algebraic integer. Conversely, if α is an algebraic integer then $q(\alpha) = 0$ for some monic $q \in \mathbf{Z}[t]$, and $p|q$. By Gauss's Lemma 1.7 it follows that $p \in \mathbf{Z}[t]$, because some rational multiple λp lies in $\mathbf{Z}[t]$ and divides q, and the monicity of q and p implies $\lambda = 1$. □

To avoid confusion as to the usage of the word 'integer' we adopt the following convention: a *rational integer* is an element of $\mathbf{Z}$, and a plain *integer* is an algebraic integer. (The aim is to reserve the shorter term for the concept most often encountered.) Any remaining possibility of confusion is eliminated by:

Lemma 2.14. *An algebraic integer is a rational number if and only if it is a rational integer. Equivalently, $\mathbf{B} \cap \mathbf{Q} = \mathbf{Z}$.*

Proof: Clearly $\mathbf{Z} \subseteq \mathbf{B} \cap \mathbf{Q}$. Let $\alpha \in \mathbf{B} \cap \mathbf{Q}$; since $\alpha \in \mathbf{Q}$ its minimum polynomial over $\mathbf{Q}$ is $t - \alpha$. By Lemma 2.13 the coefficients of this are in $\mathbf{Z}$, hence $-\alpha \in \mathbf{Z}$, hence $\alpha \in \mathbf{Z}$. □

2.4 Integral Bases

Let K be a number field of degree n (over $\mathbf{Q}$). A *basis* (or $\mathbf{Q}$-*basis* for emphasis) of K is a basis for K as a vector space over $\mathbf{Q}$. By Corollary 2.11 we have $K = \mathbf{Q}(\theta)$ where θ is an algebraic integer, and it follows that

the minimum polynomial p of θ has degree n and that $\{1, \theta, \ldots, \theta^{n-1}\}$ is a basis for K.

The ring $\mathfrak{O}$ of integers of K is an abelian group under addition. A $\mathbf{Z}$-basis for $(\mathfrak{O}, +)$ is called an *integral basis* for K (or for $\mathfrak{O}$). Thus $\{\alpha_1, \ldots, \alpha_s,\}$ is an integral basis if and only if all $\alpha_i \in \mathfrak{O}$ and every element of $\mathfrak{O}$ is *uniquely* expressible in the form

$$a_1\alpha_1 + \ldots + a_s\alpha_s$$

for rational integers $a_1, \ldots, a_s$. It is obvious from Lemma 2.11 that any integral basis for K is a $\mathbf{Q}$-basis. Hence in particular $s = n$. But we have to verify that integral bases exist. In fact they do, but they are not always what naively we might expect them to be.

For instance we can assert that $K = \mathbf{Q}[\theta]$ $(= \mathbf{Q}(\theta))$ for an algebraic integer θ (Corollary 2.12), so that $\{1, \theta, \ldots, \theta^{n-1}\}$ is a $\mathbf{Q}$-basis for K which consists of integers, but it does not follow that $\{1, \theta, \ldots, \theta^{n-1}\}$ is an integral basis. Some of the elements in $\mathbf{Q}[\theta]$ with rational coefficients may also be integers. As an example, consider $K = \mathbf{Q}(\sqrt{5})$. We have seen that the element $\frac{1}{2} + \frac{1}{2}\sqrt{5}$ satisfies the equation

$$t^2 - t + 1 = 0$$

and so is an integer in $\mathbf{Q}(\sqrt{5})$, but it is not an element of $\mathbf{Z}[\sqrt{5}]$.

Our first problem, therefore, is to show that integral bases exist. That they do is equivalent to the statement that $(\mathfrak{O}, +)$ is a free abelian group of rank n. To prove this we first establish:

Lemma 2.15. *If $\{\alpha_1, \ldots, \alpha_n\}$ is a basis of K consisting of integers, then the discriminant $\Delta[\alpha_1, \ldots, \alpha_n]$ is a rational integer, not equal to zero.*

Proof: We know that $\Delta = \Delta[\alpha_1, \ldots, \alpha_n]$ is rational by Theorem 2.7, and it is an integer since the α_i are. Hence by Lemma 2.14 it is a rational integer. By Theorem 2.7, $\Delta \neq 0$. □

Theorem 2.16. *Every number field K possesses an integral basis, and the additive group of $\mathfrak{O}$ is free abelian of rank n equal to the degree of K.*

Proof: We have $K = \mathbf{Q}(\theta)$ for θ an integer. Hence there exist bases for K consisting of integers: for example $\{1, \theta, \ldots, \theta^{n-1}\}$. We have already seen that such $\mathbf{Q}$-bases need not be integral bases. However, the discriminant of a $\mathbf{Q}$-basis consisting of integers is always a rational integer (Lemma 2.15), so what we do is to select a basis $\{\omega_1, \ldots, \omega_n\}$ of integers for which

$$|\Delta[\omega_1, \ldots, \omega_n]|$$

is least. We claim that this is in fact an integral basis. If not, there is an integer ω of K such that

$$\omega = a_1\omega_1 + \ldots + a_n\omega_n$$

for $a_i \in \mathbf{Q}$, *not all in* $\mathbf{Z}$. Choose the numbering so that $a_1 \notin \mathbf{Z}$. Then $a_1 = a + r$ where $a \in \mathbf{Z}$ and $0 < r < 1$. Define

$$\psi_1 = \omega - a\omega_1, \qquad \psi_i = \omega_i \qquad (i = 2, \ldots, n).$$

Then $\{\psi_1, \ldots, \psi_n\}$ is a basis consisting of integers. The determinant relevant to the change of basis from the ω's to the ψ's is

$$\begin{vmatrix} a_1 - a & a_2 & a_3 & \ldots & a_n \\ 0 & 1 & 0 & \ldots & 0 \\ 0 & 0 & 1 & \ldots & 0 \\ \ldots & \ldots & \ldots & \ldots & \ldots \\ 0 & 0 & 0 & \ldots & 1 \end{vmatrix} = r,$$

and so

$$\Delta[\psi_1, \ldots, \psi_n] = r^2\Delta[\omega_1, \ldots, \omega_n].$$

Since $0 < r < 1$ this contradicts the choice of $\{\omega_1, \ldots, \omega_n\}$ making $|\Delta[\omega_1, \ldots, \omega_n]|$ minimal.

It follows that $\{\omega_1, \ldots, \omega_n\}$ is an integral basis, and so $(\mathfrak{O}, +)$ is free abelian of rank n. □

This raises the question of finding integral bases in cases such as $\mathbf{Q}(\sqrt{5})$ where the $\mathbf{Q}$-basis $\{1, \sqrt{5}\}$ is not an integral basis. We shall consider a more general case in the next chapter, but this particular example is worth a brief discussion here.

An element of $\mathbf{Q}(\sqrt{5})$ is of the form $p + q\sqrt{5}$ for $p, q \in \mathbf{Q}$, and has minimum polynomial

$$(t - p - q\sqrt{5})(t - p + q\sqrt{5}) = t^2 - 2pt + (p^2 - 5q^2).$$

Then $p + q\sqrt{5}$ is an integer if and only if the coefficients $2p, p^2 - 5q^2$ are rational integers. Thus $p = \frac{1}{2}P$ where P is a rational integer. For P even, we have p^2 a rational integer, so $5q^2$ is a rational integer also, implying q is a rational integer. For P odd, a straightforward calculation (performed in the next chapter in greater generality) shows $q = \frac{1}{2}Q$ where Q is also an odd rational integer.

From this it follows that $\mathfrak{O} = \mathbf{Z}[\frac{1}{2} + \frac{1}{2}\sqrt{5}]$ and an integral basis is $\{1, \frac{1}{2} + \frac{1}{2}\sqrt{5}\}$.

We can prove this by another route using the discriminant. The two monomorphisms $\mathbf{Q}(\sqrt{5}) \to \mathbf{C}$ are given by

$$\begin{aligned} \sigma_1(p+q\sqrt{5}) &= p+q\sqrt{5}, \\ \sigma_2(p+q\sqrt{5}) &= p-q\sqrt{5}. \end{aligned}$$

Hence the discriminant $\Delta[1, \frac{1}{2}+\frac{1}{2}\sqrt{5}]$ is given by

$$\begin{vmatrix} 1 & \frac{1}{2}+\frac{1}{2}\sqrt{5} \\ 1 & \frac{1}{2}-\frac{1}{2}\sqrt{5} \end{vmatrix}^2 = 5.$$

We define a rational integer to be *squarefree* if it is not divisible by the square of a prime. For example, 5 is squarefree, as are 6, 7, but not 8 or 9. Given a $\mathbf{Q}$-basis of K consisting of integers, we compute the discriminant and then we have:

Theorem 2.17. *Suppose $\alpha_1, \ldots, \alpha_n \in \mathfrak{O}$ form a $\mathbf{Q}$-basis for K. If $\Delta[\alpha_1, \ldots, \alpha_n]$ is squarefree then $\{\alpha_1, \ldots, \alpha_n\}$ is an integral basis.*

Proof: Let $\{\beta_1, \ldots, \beta_n\}$ be an integral basis. Then there exist rational integers c_{ij} such that $\alpha_i = \Sigma c_{ij}\beta_j$, and

$$\Delta[\alpha_1, \ldots, \alpha_n] = (\det c_{ij})^2 \Delta[\beta_1, \ldots, \beta_n].$$

Since the left-hand side is squarefree, we must have $\det c_{ij} = \pm 1$, so that (c_{ij}) is unimodular. Hence by Lemma 1.15 $\{\alpha_1, \ldots, \alpha_n\}$ is a $\mathbf{Z}$-basis for $\mathfrak{O}$, that is, an integral basis for K. □

For example, the $\mathbf{Q}$-basis $\{1, \frac{1}{2}+\frac{1}{2}\sqrt{5}\}$ for $\mathbf{Q}(\sqrt{5})$ consists of integers and has discriminant 5 (calculated above). Since 5 is squarefree, this is an integral basis. The reader should note that there exist integral bases whose discriminants are not squarefree (as we shall see later on), so the converse of Theorem 2.17 is false.

For two integral bases $\{\alpha_1, \ldots, \alpha_n\}$, $\{\beta_1, \ldots, \beta_n\}$ of an algebraic number field K, we have

$$\Delta[\alpha_1, \ldots, \alpha_n] = (\pm 1)^2 \Delta[\beta_1, \ldots, \beta_n] = \Delta[\beta_1, \ldots, \beta_n],$$

because the matrix corresponding to the change of basis is unimodular. Hence the discriminant of an integral basis is independent of which integral basis we choose. This common value is called the *discriminant of K* (or of $\mathfrak{O}$). It is always a non-zero rational integer. Obviously, isomorphic number fields have the same discriminant. The important role played by the discriminant will become apparent as the drama unfolds.

2.5 Norms and Traces

These important concepts often allow us to transform a problem about algebraic integers into one about rational integers. As usual, let $K = \mathbf{Q}(\theta)$ be a number field of degree n and let $\sigma_1, \ldots, \sigma_n$ be the monomorphisms $K \to \mathbf{C}$. Now the field polynomial is a power of the minimum polynomial by Theorem 2.6(a), so by Lemma 2.13 and Gauss's Lemma 1.7 it follows that $\alpha \in K$ is an integer if and only if the field polynomial has rational integer coefficients. For any $\alpha \in K$ we define the *norm*

$$\mathrm{N}_K(\alpha) = \prod_{i=1}^{n} \sigma_i(\alpha)$$

and *trace*

$$\mathrm{T}_K(\alpha) = \sum_{i=1}^{n} \sigma_i(\alpha).$$

Where the field K is clear from the context, we will abbreviate the norm and trace of α to $\mathrm{N}(\alpha)$ and $\mathrm{T}(\alpha)$ respectively.

Since the field polynomial is

$$f_\alpha(t) = \prod_{i=1}^{n} (t - \sigma_i(\alpha))$$

it follows from the remark above that *if α is an integer then the norm and trace of α are rational integers.* Since the σ_i are monomorphisms it is clear that

$$\mathrm{N}(\alpha\beta) = \mathrm{N}(\alpha)\mathrm{N}(\beta) \tag{2.4}$$

and if $\alpha \neq 0$ then $\mathrm{N}(\alpha) \neq 0$. If p, q are rational numbers then

$$\mathrm{T}(p\alpha + q\beta) = p\mathrm{T}(\alpha) + q\mathrm{T}(\beta). \tag{2.5}$$

For instance, if $K = \mathbf{Q}(\sqrt{7})$ then the integers of K are given by $\mathfrak{O} = \mathbf{Z}[\sqrt{7}]$ (as we shall see in Theorem 3.2). The maps σ_i are given by

$$\begin{aligned} \sigma_1(p+q\sqrt{7}) &= p+q\sqrt{7}, \\ \sigma_2(p+q\sqrt{7}) &= p-q\sqrt{7}. \end{aligned}$$

Hence

$$\begin{aligned} \mathrm{N}(p+q\sqrt{7}) &= p^2 - 7q^2, \\ \mathrm{T}(p+q\sqrt{7}) &= 2p. \end{aligned}$$

Since norms are not too hard to compute (they can always be found from symmetric polynomial considerations, often with short-cuts) whereas discriminants involve complicated work with determinants, the following result is sometimes useful:

Proposition 2.18. *Let $K = \mathbf{Q}(\theta)$ be a number field where θ has minimum polynomial p of degree n. The $\mathbf{Q}$-basis $\{1, \theta, \ldots, \theta^{n-1}\}$ has discriminant*

$$\Delta\left[1, \ldots, \theta^{n-1}\right] = (-1)^{n(n-1)/2}\mathrm{N}(\mathrm{D}p(\theta))$$

where $\mathrm{D}p$ is the formal derivative of p.

Proof: From the proof of Theorem 2.7 we obtain

$$\Delta = \Delta[1, \theta, \ldots, \theta^{n-1}] = \prod_{1 \le i < j \le n} (\theta_i - \theta_j)^2$$

where $\theta_1, \ldots, \theta_n$ are the conjugates of θ. Now

$$p(t) = \prod_{i=1}^{n} (t - \theta_i)$$

so that

$$\mathrm{D}p(t) = \sum_{j=1}^{n} \prod_{\substack{i=1 \\ i \ne j}}^{n} (t - \theta_i)$$

and therefore

$$\mathrm{D}p(\theta_j) = \prod_{\substack{i=1 \\ i \ne j}}^{n} (\theta_j - \theta_i).$$

Multiplying all these equations for $j = 1, \ldots, n$ we obtain

$$\prod_{j=1}^{n} \mathrm{D}p(\theta_j) = \prod_{\substack{i,j=1 \\ i \ne j}}^{n} (\theta_j - \theta_i).$$

The left-hand side is $\mathrm{N}(\mathrm{D}p(\theta))$. On the right, each factor $(\theta_i - \theta_j)$ for $i < j$ appears twice, once as $(\theta_i - \theta_j)$ and once as $(\theta_j - \theta_i)$. The product of these two factors is $-(\theta_i - \theta_j)^2$. On multiplying up, we get Δ multiplied by $(-1)^s$ where s is the number of pairs (i, j) with $1 \le i < j \le n$, which is given by

$$s = \tfrac{1}{2}n(n-1).$$

The result follows. □

We close this chapter by noting the following simple identity linking the discriminant and trace:

Proposition 2.19. *If $\{\alpha_1, \ldots, \alpha_n\}$ is any $\mathbf{Q}$-basis of K, then*

$$\Delta[\alpha_1, \ldots, \alpha_n] = \det(\mathrm{T}(\alpha_i \alpha_j)).$$

Proof: $\mathrm{T}(\alpha_i\alpha_j) = \sum_{r=1}^{n} \sigma_r(\alpha_i\alpha_j) = \sum_{r=1}^{n} \sigma_r(\alpha_i)\sigma_r(\alpha_j)$. Hence

$$\begin{aligned}
\Delta[\alpha_1, \ldots, \alpha_n] &= (\det(\sigma_i(\alpha_j)))^2 \\
&= (\det(\sigma_j(\alpha_i)))(\det(\sigma_i(\alpha_j))) \\
&= \det(\sum_{r=1}^{n} \sigma_r(\alpha_i)\sigma_r(\alpha_j)) \\
&= \det(\mathrm{T}(\alpha_i\alpha_j)).
\end{aligned}$$

□

2.6 Rings of Integers

We now discuss how to find the ring of integers of a given number field. With the methods available to us, this involves moderately heavy calculation; but by taking advantage of short cuts the technique can be made reasonably efficient. In particular we show in Example 2.3 below that not every number field has an integral basis of the form $\{1, \theta, \ldots, \theta^{n-1}\}$.

The method is based on the following result:

Theorem 2.20. *Let G be an additive subgroup of $\mathfrak{O}$ of rank equal to the degree of K, with $\mathbf{Z}$-basis $\{\alpha_1, \ldots, \alpha_n\}$. Then $|\mathfrak{O}/G|^2$ divides $\Delta[\alpha_1, \ldots, \alpha_n]$.*

Proof: By Theorem 1.16 there exists a $\mathbf{Z}$-basis for $\mathfrak{O}$ of the form $\{\beta_1, \ldots, \beta_n\}$ such that G has a $\mathbf{Z}$-basis $\{\mu_1\beta_1, \ldots, \mu_n\beta_n\}$ for suitable $\mu_i \in \mathbf{Z}$. Now

$$\Delta[\alpha_1, \ldots, \alpha_n] = \Delta[\mu_1\beta_1, \ldots, \mu_n\beta_n]$$

since by Lemma 1.15 a basis-change has a unimodular matrix; and the right-hand side is equal to

$$(\mu_1 \ldots \mu_n)^2 \Delta[\beta_1, \ldots, \beta_n] = (\mu_1 \ldots \mu_n)^2 \Delta$$

where Δ is the discriminant of K and so lies in $\mathbf{Z}$. But

$$|\mu_1 \ldots \mu_n| = |\mathfrak{O}/G|.$$