CHAPTER 2

Algebraic Numbers and Algebraic Integers

2.1. Gaussian Integers

In this chapter, we study the problem of adjoining irrational numbers to the rational number field $\mathbb{Q}$ to form algebraic number fields, as well as the ring of integers within any such algebraic number field.

However, before we study the problem in general, we first of all investigate the special case when we adjoin the complex number i, where $\mathrm{i}^2 = -1$, to the rational number field $\mathbb{Q}$ to obtain the algebraic number field $\mathbb{Q}(\mathrm{i})$ of all numbers of the form $a + b\mathrm{i}$, where $a, b \in \mathbb{Q}$. Many of the techniques in the general situation can be motivated and developed from this special case.

It is easy to see that $\mathbb{Q}(\mathrm{i})$, with the usual addition and multiplication in $\mathbb{C}$, forms a field. The subset $\mathbb{Z}[\mathrm{i}]$ of all numbers of the form $a+b\mathrm{i}$, where $a, b \in \mathbb{Z}$, forms a subring of $\mathbb{Q}(\mathrm{i})$. Elements of this subring $\mathbb{Z}[\mathrm{i}]$ are called gaussian integers.

Our first task is to develop a theory of divisibility among gaussian integers.

Suppose that $\alpha, \beta \in \mathbb{Z}[\mathrm{i}]$ and $\alpha \neq 0$. Then we say that α divides β, denoted by $\alpha \mid \beta$, if there exists $\gamma \in \mathbb{Z}[\mathrm{i}]$ such that $\beta = \alpha\gamma$; in other words, we have a factorization $\beta = \alpha\gamma$. In this case, we say that α is a divisor of β.

Furthermore, we say that a gaussian integer $u \in \mathbb{Z}[\mathrm{i}]$ is a unit if $u \mid 1$. We also say that two gaussian integers $\alpha, \beta \in \mathbb{Z}[\mathrm{i}]$ are associates if $\alpha = u\beta$ for some unit $u \in \mathbb{Z}[\mathrm{i}]$. Finally, we say that a gaussian integer $\pi \in \mathbb{Z}[\mathrm{i}]$ is a gaussian prime if π is not a unit and if any divisor of π is either a unit or an associate of π.

Recall that divisibility in $\mathbb{Z}$ is governed by the magnitude of the integers. In the case of gaussian integers, this role is now played by essentially the modulus of the gaussian integer interpreted as a complex number. We consider instead the square of this quantity. Accordingly, for every gaussian integer $\alpha = a + b\mathrm{i} \in \mathbb{Z}[\mathrm{i}]$, where $a, b \in \mathbb{Z}$, we define the norm of α by $N(\alpha) = \alpha\overline{\alpha} = a^2 + b^2$, where $\overline{\alpha} = a - b\mathrm{i}$ denotes the complex conjugate of α.

THEOREM 2.1. *Suppose that $\alpha, \beta \in \mathbb{Z}[\mathrm{i}]$. Then*

(i) *$N(\alpha)$ is a non-negative rational integer;*
(ii) *$N(\alpha\beta) = N(\alpha)N(\beta)$;*
(iii) *$N(\alpha) = 1$ if and only if α is a unit;*
(iv) *α is a unit if and only if $\alpha = \pm 1$ or $\alpha = \pm\mathrm{i}$; and*
(v) *α is a gaussian prime if $N(\alpha)$ is a rational prime.*

PROOF. (i) and (ii) are trivial.

To prove (iii), suppose first of all that $N(\alpha) = 1$. Then $\alpha\overline{\alpha} = 1$. Since $\overline{\alpha}$ is also a gaussian integer, it follows that $\alpha \mid 1$, so that α is a unit. Suppose now that α is a unit. Then $\alpha \mid 1$. Hence there exists a gaussian integer β such that $\alpha\beta = 1$. It follows from (ii) that $N(\alpha)N(\beta) = N(\alpha\beta) = N(1) = 1$, and so $N(\alpha) \mid 1$ in $\mathbb{Z}$. Since $N(\alpha)$ is non-negative, it follows that $N(\alpha) = 1$.

It is easy to show that ± 1 or $\pm \mathrm{i}$ are units. Suppose now that the gaussian integer $\alpha = a + b\mathrm{i}$ is a unit. Then it follows from (iii) that $a^2 + b^2 = 1$. The only solutions are $(a, b) = (\pm 1, 0)$ and $(a, b) = (0, \pm 1)$, giving rise to $\alpha = \pm 1$ or $\alpha = \pm \mathrm{i}$ respectively, proving (iv).

To prove (v), suppose that $\beta \mid \alpha$. Then there exists a gaussian integer γ such that $\alpha = \beta\gamma$. It now follows from (ii) that $N(\alpha) = N(\beta)N(\gamma)$ in $\mathbb{Z}$. Since $N(\alpha)$ is a rational prime and non-negative, we must have $N(\beta) = 1$ or $N(\gamma) = 1$. It follows from (iii) that β or γ is a unit. If γ is a unit, then β is an associate of α. ◯

THEOREM 2.2. *Suppose that $\alpha, \beta \in \mathbb{Z}[\mathrm{i}]$, and $\alpha \neq 0$. Then there exist $\gamma, \rho \in \mathbb{Z}[\mathrm{i}]$ such that $\beta = \alpha\gamma + \rho$, where $N(\rho) < N(\alpha)$.*

PROOF. Clearly

$$\frac{\beta}{\alpha} = A + B\mathrm{i},$$

where $A, B \in \mathbb{Q}$. We now choose $c, d \in \mathbb{Z}$ such that

$$|A - c| \leqslant \tfrac{1}{2} \quad \text{and} \quad |B - d| \leqslant \tfrac{1}{2},$$

and write $\gamma = c + d\mathrm{i}$ and $\rho = \beta - \alpha\gamma$. Clearly $\gamma, \rho \in \mathbb{Z}[\mathrm{i}]$. To show that $N(\rho) < N(\alpha)$, we now note that

$$\begin{aligned} |\rho| = |\beta - \alpha\gamma| = |\beta - \alpha(c + d\mathrm{i})| &= |\alpha| \left| \frac{\beta}{\alpha} - (c + d\mathrm{i}) \right| \\ &= |\alpha||(A - c) + (B - d)\mathrm{i}| = |\alpha|((A - c)^2 + (B - d)^2)^{\frac{1}{2}} < |\alpha|, \end{aligned}$$

and the result follows on noting that $N(\rho) = |\rho|^2$ and $N(\alpha) = |\alpha|^2$. ◯

THEOREM 2.3. *Suppose that $\alpha, \beta \in \mathbb{Z}[\mathrm{i}]$, and $\pi \in \mathbb{Z}[\mathrm{i}]$ is a gaussian prime. If $\pi \mid \alpha\beta$, then $\pi \mid \alpha$ or $\pi \mid \beta$.*

PROOF. We may assume that $\pi \nmid \alpha$, for otherwise the conclusion of the theorem already holds. It follows from Theorem 2.2 that there exist $\gamma, \rho \in \mathbb{Z}[\mathrm{i}]$ such that $\alpha = \pi\gamma + \rho$, where $N(\rho) < N(\pi)$ and $\rho \neq 0$, so that $0 < N(\rho) < N(\pi)$. Clearly the set

$$S = \{\alpha\xi + \pi\eta : \xi, \eta \in \mathbb{Z}[\mathrm{i}]\}$$

is non-empty, and contains the element $\rho = \alpha - \pi\gamma$ with positive norm. It follows that there exists an element in S with least positive norm. Suppose that this element is

$$\mu = \alpha\xi_0 + \pi\eta_0, \tag{2.1}$$

where $\xi_0, \eta_0 \in \mathbb{Z}[\mathrm{i}]$. Then

$$\mu\beta = \alpha\beta\xi_0 + \pi\eta_0\beta,$$

so that $\pi \mid \mu\beta$. To show that $\pi \mid \beta$, it remains to show that μ is a unit. Clearly

$$N(\mu) \leqslant N(\rho) < N(\pi). \tag{2.2}$$

By Theorem 2.2, there exist $\tau, \sigma \in \mathbb{Z}[\mathrm{i}]$ such that $\pi = \mu\tau + \sigma$, where $N(\sigma) < N(\mu)$. Combining this with (2.1), we have

$$\sigma = \pi - \mu\tau = \alpha(-\xi_0\tau) + \pi(1 - \eta_0\tau) \in S.$$

In view of the minimality of $N(\mu)$, we must therefore have $N(\sigma) = 0$ and so $\sigma = 0$ and $\pi = \mu\tau$. Since π is prime, it follows that one of μ or τ must be a unit. If τ is a unit, then $N(\tau) = 1$, and so it follows from $N(\pi) = N(\mu)N(\tau)$ that $N(\pi) = N(\mu)$, contradicting (2.2). It follows that μ is a unit. ◯

Using Theorem 2.3 a finite number of times, we can easily deduce the following generalization.

THEOREM 2.4. *Suppose that $\alpha_1, \ldots, \alpha_k \in \mathbb{Z}[\mathrm{i}]$, and $\pi \in \mathbb{Z}[\mathrm{i}]$ is a gaussian prime. If $\pi \mid \alpha_1 \ldots \alpha_k$, then $\pi \mid \alpha_j$ for some $j = 1, \ldots, k$.*

We can now establish a unique factorization theorem for gaussian integers.

THEOREM 2.5. *Every $\alpha \in \mathbb{Z}[\mathrm{i}]$, not zero or a unit, is representable as a product of gaussian primes, uniquely up to units, associates and the order of factors.*

PROOF. To establish the existence of factorization, we use induction on the norm. Clearly all the gaussian integers with norm 2 are gaussian primes, in view of Theorem 2.1(v). Suppose now that all gaussian integers with norm less than n can be factorized into products of gaussian primes. Let α be a guassian integer with $N(\alpha) = n$. If α is a gaussian prime, then there is nothing more to prove. If α is not a gaussian prime, then $\alpha = \alpha_1\alpha_2$, where neither gaussian integer α_1 nor α_2 is a unit. Since $N(\alpha) = N(\alpha_1)N(\alpha_2)$, it follows that $1 < N(\alpha_1) < n$ and $1 < N(\alpha_2) < n$. By the induction hypothesis, both α_1 and α_2 can be factorized into products of gaussian primes. It follows that α can be factorized into a product of gaussian primes.

To establish uniqueness of factorization, suppose that

$$\alpha = \pi_1 \dots \pi_r = u\kappa_1 \dots \kappa_s,$$

where u is a unit, and $\pi_1, \dots, \pi_r, \kappa_1, \dots, \kappa_s$ are gaussian primes. By Theorem 2.4, we must have $\pi_1 \mid \kappa_j$ for some $j = 1, \dots, s$. Assume, without loss of generality, that $\pi_1 \mid \kappa_1$. Then

$$\pi_2 \dots \pi_r = u_1\kappa_2 \dots \kappa_s,$$

where u_1 is a unit. Repeating this argument a finite number of times, we conclude that $r = s$, and uniqueness of factorization follows. ◯

At this point, we give a proof of Fermat's theorem concerning sums of two squares, using ideas from gaussian integers and gaussian primes. Recall that Fermat's theorem states that if $p \equiv 1 \bmod 4$ is a rational prime, then there exist $a, b \in \mathbb{Z}$ such that $p = a^2 + b^2$.

PROOF OF FERMAT'S THEOREM. Our starting point, as in Fermat's proof, is to observe that -1 is a quadratic residue modulo p, and so there exists $x \in \mathbb{Z}$ such that $x^2 + 1 \equiv 0 \bmod p$. Next, note that in view of Theorem 2.5, there exists a gaussian prime π which divides p. Then it follows from Theorem 2.1(ii) that $N(\pi) \mid N(p) = p^2$. Since $N(\pi)$ is a rational integer different from 1, it follows that we must have $N(\pi) = p$ or $N(\pi) = p^2$. Suppose that $N(\pi) = p^2$. Then it is easy to see that p/π is a gaussian integer satisfying $N(p/\pi) = 1$, in view of Theorem 2.1(ii). This implies that p and π are associates, so that p is a gaussian prime. Since $p \mid (x^2 + 1) = (x + \mathrm{i})(x - \mathrm{i})$, it follows from Theorem 2.3 that $p \mid (x + \mathrm{i})$ or $p \mid (x - \mathrm{i})$, neither of which is true, since

$$\frac{x}{p} \pm \frac{1}{p}\mathrm{i} \notin \mathbb{Z}[\mathrm{i}].$$

It follows that we must have $N(\pi) = p$. Suppose now that $\pi = a + b\mathrm{i}$, where $a, b \in \mathbb{Z}$. Then clearly $a^2 + b^2 = p$. ◯

We complete this section on gaussian integers by determining all the gaussian primes. The crucial step in the argument is summarized in the following result.

THEOREM 2.6. *Every gaussian prime divides exactly one positive rational prime.*

PROOF. Let π be a gaussian prime. Since $N(\pi) = \pi\overline{\pi}$, it follows that $\pi \mid N(\pi)$. On the other hand, we clearly have $N(\pi) > 1$. Since $N(\pi)$ is a positive integer, we can write $N(\pi) = p_1 \dots p_r$, where $p_1, \dots, p_r$ are rational primes. It follows from Theorem 2.4 that $\pi \mid p_j$ for some $j = 1, \dots, r$, so that π divides at least one rational prime.

Suppose now that p and q are distinct positive rational primes. Then $(p, q) = 1$, so there exist rational integers u and v such that $1 = pu + qv$. It follows that if π divides both p and q, then π must also divide 1, clearly impossible. Hence π divides at most one positive rational prime. ◯

THEOREM 2.7. *The set of all gaussian primes consists of the following and their associates:*

(i) *the number* $1 + \mathrm{i}$*;*
(ii) *the numbers* $a + b\mathrm{i}$*, where* $a, b \in \mathbb{N}$ *and* $a^2 + b^2 = p \equiv 1 \bmod 4$ *is a rational prime; and*
(iii) *the rational primes* $q \equiv 3 \bmod 4$*.*

PROOF. In view of Theorem 2.6, it is sufficient to factorize the positive rational primes into products of gaussian primes. We distinguish three cases:

(i) The rational prime $2 = (1 + \mathrm{i})(1 - \mathrm{i}) = -\mathrm{i}(1 + \mathrm{i})^2$. The number i is a unit and so not a gaussian prime. On the other hand, $N(1 + \mathrm{i}) = 2$ is a rational prime, so it follows from Theorem 2.1(v) that $1 + \mathrm{i}$ is a gaussian prime.

(ii) Let $p \equiv 1 \bmod 4$ be a positive rational prime. By Fermat's theorem, there exist positive integers a and b such that $a^2 + b^2 = p$. It follows that

$$p = (a + b\mathrm{i})(a - b\mathrm{i}) = -\mathrm{i}(a + b\mathrm{i})(b + a\mathrm{i}).$$

Both numbers $a + b\mathrm{i}$ and $b + a\mathrm{i}$ are gaussian primes, since their norm is the rational prime p.

(iii) Let $q \equiv 3 \bmod 4$ be a positive rational prime. Suppose that $\pi = a + b\mathrm{i}$ is a gaussian prime and $\pi \mid q$. Clearly $N(\pi) > 1$. Since $N(\pi) \mid N(q) = q^2$, it follows that $N(\pi) = q$ or $N(\pi) = q^2$. But $N(\pi) \neq q$, for otherwise $a^2 + b^2 = q \equiv 3 \bmod 4$, an impossibility. Hence $N(\pi) = q^2$. This implies that π and q are associates, so that q is a gaussian prime. ◯

2.2. Field Extensions

In this section, we give briefly the algebraic background of field extensions. Here we make no restrictions on the fields involved.

Suppose that K and L are fields such that $K \subseteq L$. Then we say that the field L is an extension of the field K, denoted by $L : K$. The field L has a natural structure as a vector space over K, where vector addition is addition in L and scalar multiplication of $\lambda \in K$ and $v \in L$ is simply $\lambda v \in L$. The dimension of this vector space is called the degree of the extension $L : K$, or the degree of L over K, and denoted by $[L : K]$.

THEOREM 2.8. *Suppose that H, K and L are fields satisfying $H \subseteq K \subseteq L$. Then*

$$[L : H] = [L : K][K : H], \tag{2.3}$$

provided that the terms on the right hand side of (2.3) *are finite.*

We say that the field extension $L : K$ is finite, or L is a finite extension of K, if $[L : K]$ is finite.

PROOF OF THEOREM 2.8. Let $\{v_i : i \in I\}$ be a basis of L over K, and let $\{w_j : j \in J\}$ be a basis of K over H. To establish (2.3), it suffices to show that the set

$$\{v_i w_j : i \in I,\ j \in J\} \tag{2.4}$$

is a basis of L over H. For every $\alpha \in L$, we can write

$$\alpha = \sum_{i \in I} \beta_i v_i,$$

where $\beta_i \in K$ for every $i \in I$. For every $i \in I$, we can write

$$\beta_i = \sum_{j \in J} \gamma_{ij} w_j,$$

where $\gamma_{ij} \in H$ for every $j \in J$. We therefore have

$$\alpha = \sum_{i \in I} \sum_{j \in J} \gamma_{ij} v_i w_j.$$

Hence the set (2.4) spans L as a vector space over H. It remains to show that the elements in (2.4) are linearly independent over H. Suppose that

$$\sum_{i \in I} \sum_{j \in J} \delta_{ij} v_i w_j = 0,$$

where $\delta_{ij} \in H$ for every $i \in I$ and $j \in J$. Then

$$\sum_{i \in I} \left(\sum_{j \in J} \delta_{ij} w_j \right) v_i = 0.$$

Since

$$\sum_{j \in J} \delta_{ij} w_j \in K$$

for every $i \in I$ and the elements in $\{v_i : i \in I\}$ are linearly independent over K, it follows that

$$\sum_{j \in J} \delta_{ij} w_j = 0$$

for every $i \in I$. Since $\delta_{ij} \in H$ for every $i \in I$ and $j \in J$ and the elements in $\{w_j : j \in J\}$ are linearly independent over H, it follows that $\delta_{ij} = 0$ for every $i \in I$ and $j \in J$. ◯

Suppose that $L : K$ be a finite field extension. We say that an element $\alpha \in L$ is algebraic over K if there exists a polynomial $q(t) \in K[t]$, not identically zero and such that $q(\alpha) = 0$. In other words, $\alpha \in L$ is algebraic over K if it is the root of a polynomial with coefficients in K.

It is easy to see that if $\alpha \in L$ is the root of a polynomial with coefficients in K, then it is also the root of many other polynomials with coefficients in K. Our next result shows that among all such polynomials, there must be a "smallest" one.

THEOREM 2.9. *Suppose that α is algebraic over a field K. Then there exists a unique monic polynomial $p(t) \in K[t]$ of smallest degree such that $p(\alpha) = 0$. Furthermore, this polynomial $p(t)$ is irreducible in $K[t]$.*

REMARKS. (i) In Theorem 2.9, we have implicitly assumed that α belongs to a field L where L is an extension of K.

(ii) A monic polynomial in $K[t]$ is a polynomial of the type $q(t) = q_n t^n + \ldots + q_0$, where $q_n = 1$, the multiplicative identity in K. In other words, the leading coefficient of a monic polynomial $q(t)$ must be equal to 1.

(iii) The polynomial $p(t)$ in Theorem 2.9 is sometimes called the minimum polynomial of α over K.

PROOF OF THEOREM 2.9. Suppose that $q(t) \in K[t]$ such that $q(\alpha) = 0$. Since K is a field, we can divide all the coefficients of $q(t)$ by the leading coefficient and obtain a monic polynomial in $K[t]$ with α as a root. Let S denote the set of all monic polynomials in $K[t]$ with α as a root. Then S is non-empty. Among the polynomials in S, there must be one of smallest degree, $p(t)$ say.

To show that $p(t)$ is unique, suppose on the contrary that the polynomial $r(t) \in S$ is of the same degree as $p(t)$. Let $s(t) = p(t) - r(t)$. Since $p(t), r(t) \in S$, we must have $p(\alpha) = r(\alpha) = 0$, and so $s(\alpha) = 0$. On the other hand, both $p(t)$ and $r(t)$ are monic and of the same degree, and so $s(t)$ is of smaller degree than $p(t)$. We can now divide all the coefficients of $s(t)$ by its leading coefficient to obtain a monic polynomial in $K[t]$, of smaller degree than $p(t)$ and with α as a root. This contradicts the minimality of the degree of $p(t)$.

To show that $p(t)$ is irreducible, suppose that

$$p(t) = p_1(t)p_2(t),$$

where $p_1(t), p_2(t) \in K[t]$. Since $p(\alpha) = p_1(\alpha)p_2(\alpha) = 0$, we may assume without loss of generality that $p_1(\alpha) = 0$. Multiplying the coefficients of $p_1(t)$ and $p_2(t)$ by elements of K if necessary, we may further assume that both $p_1(t)$ and $p_2(t)$ are monic. Clearly, the degree of $p_1(t)$ cannot exceed the degree of $p(t)$. On the other hand, in view of the minimality of the degree of $p(t)$, the degree of $p_1(t)$ cannot be smaller than the degree of $p(t)$. It follows that $p_1(t)$ and $p(t)$ must have the same degree, and must therefore be equal in view of the uniqueness of $p(t)$. Hence $p_2(t) = 1$ always, so that $p(t)$ is irreducible in $K[t]$. ◯

Suppose that $L : K$ is a field extension. If $\alpha \in L$, we can adjoin the element α to the field K and extend addition and multiplication in K to include α, in the same way as we adjoin the number i to the field $\mathbb{Q}$ in the last section. The collection of elements of K, together with α and their sums and products, now form a field $K(\alpha)$. Since $\alpha \in L$, it is clear that $K \subseteq K(\alpha) \subseteq L$. On the other hand, if $\alpha \notin K$, then $K(\alpha) \neq K$. Indeed, we can think of $K(\alpha)$ as the smallest subfield of L which contains α and all the elements of K.

Recall the example of $\mathbb{Q}(\mathrm{i})$. Since i is a root of the monic polynomial $t^2 + 1 \in \mathbb{Q}[t]$, it is algebraic over $\mathbb{Q}$. On the other hand, it is easy to see that $\mathbb{Q}(\mathrm{i})$ can be interpreted as a vector space over $\mathbb{Q}$, with basis $\{1, \mathrm{i}\}$, say. More to the point, we have $[\mathbb{Q}(\mathrm{i}) : \mathbb{Q}] = 2$, so that the field extension $\mathbb{Q}(\mathrm{i}) : \mathbb{Q}$ is finite.

Generalizing this observation, we prove the following result.

THEOREM 2.10. *Suppose that $L : K$ is a field extension. Then an element $\alpha \in L$ is algebraic over K if and only if $K(\alpha)$ is a finite extension of K.*

PROOF. Suppose that $K(\alpha)$ is a finite extension of K. Let $n = [K(\alpha) : K]$. Then the elements $1, \alpha, \ldots, \alpha^n$ are linearly dependent over K, so it follows that there exist $a_0, a_1, \ldots, a_n \in K$ such that

$a_0 + a_1\alpha + \ldots + a_n\alpha^n = 0$. Clearly the polynomial $q(t) = a_n t^n + \ldots + a_0 \in K[t]$ and $q(\alpha) = 0$, so that α is algebraic over K.

Suppose now that α is algebraic over K. Let

$$p(t) = t^n + p_{n-1}t^{n-1} + \ldots + p_0,$$

where $p_0, \ldots, p_{n-1} \in K$, be the minimum polynomial of α over K. To show that $K(\alpha)$ is a finite extension of K, it suffices to show that $K(\alpha)$ is the vector space over K spanned by the set $\{1, \alpha, \ldots, \alpha^{n-1}\}$. Since any element of $K(\alpha)$ is of the form $b_0 + b_1\alpha + \ldots + b_m\alpha^m$ for some non-negative integer m and coefficients $b_0, \ldots, b_m \in K$, it suffices to show that for every non-negative integer m, the term α^m can be expressed as a linear combination of the elements of $\{1, \alpha, \ldots, \alpha^{n-1}\}$ with coefficients in K. We prove this by induction on m. The statement is trivial if $m < n$. On the other hand, we have

$$\alpha^n = -p_0 - p_1\alpha - \ldots - p_{n-1}\alpha^{n-1},$$

so that the term α^n can be expressed as a linear combination of the elements of $\{1, \alpha, \ldots, \alpha^{n-1}\}$ with coefficients in K. Suppose now that $m > n$ and for every $k < m$, the term α^k can be expressed as a linear combination of the elements of $\{1, \alpha, \ldots, \alpha^{n-1}\}$ with coefficients in K. Note that

$$\alpha^m = -p_0\alpha^{m-n} - p_1\alpha^{m-n+1} - \ldots - p_{n-1}\alpha^{m-1}.$$

By the induction hypothesis, every term on the right hand side of this expression can be expressed as a linear combination of the elements of $\{1, \alpha, \ldots, \alpha^{n-1}\}$ with coefficients in K. This must therefore also be the case for α^m. ◯

2.3. Algebraic Numbers

A number $\alpha \in \mathbb{C}$ is said to be an algebraic number if it is algebraic over $\mathbb{Q}$; in other words, if α satisfies a non-zero polynomial equation with coefficients in $\mathbb{Q}$. We denote by $\mathbb{A}$ the set of all algebraic numbers.

THEOREM 2.11. *The set $\mathbb{A}$ forms a subfield of $\mathbb{C}$.*

PROOF. We need to show that if $\alpha, \beta \in \mathbb{C}$ are algebraic numbers, then so are $\alpha + \beta$, $\alpha - \beta$ and $\alpha\beta$, as well as α/β if $\beta \neq 0$. These are all elements of $\mathbb{Q}(\alpha, \beta)$, the field obtained by adjoining the numbers α and β to the field $\mathbb{Q}$.

We first show that $\mathbb{Q}(\alpha, \beta)$ is a finite extension of $\mathbb{Q}$. To see this, note that $\mathbb{Q} \subseteq \mathbb{Q}(\alpha) \subseteq \mathbb{Q}(\alpha, \beta)$, and so it follows from Theorem 2.8 that

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

provided that the terms on the right hand side are finite. Since α is algebraic over $\mathbb{Q}$, it follows from Theorem 2.10 that $[\mathbb{Q}(\alpha) : \mathbb{Q}]$ is finite. Since β is algebraic over$\mathbb{Q}$, there exists a polynomial $q(t) \in \mathbb{Q}[t]$, not identically zero and such that $q(\beta) = 0$. Clearly $q(t) \in (\mathbb{Q}(\alpha))[t]$, and so β is algebraic over $\mathbb{Q}(\alpha)$. Also $\mathbb{Q}(\alpha, \beta) = (\mathbb{Q}(\alpha))(\beta)$. It follows from Theorem 2.10 that $[\mathbb{Q}(\alpha, \beta) : \mathbb{Q}(\alpha)]$ is also finite.

To complete the proof, it suffices to show that for every $\gamma \in \mathbb{Q}(\alpha, \beta)$, the field $\mathbb{Q}(\gamma)$ is a finite extension of $\mathbb{Q}$, in view of Theorem 2.10. But this is an immediate consequence of the simple observation that $\mathbb{Q} \subseteq \mathbb{Q}(\gamma) \subseteq \mathbb{Q}(\alpha, \beta)$. ◯

Our purpose here is not to study the set $\mathbb{A}$. Instead, we are interested in finite extensions of $\mathbb{Q}$. More precisely, we say that a subfield K of $\mathbb{C}$ is an algebraic number field if K is a finite extension of $\mathbb{Q}$. The number $[K : \mathbb{Q}]$ is called the degree of K.

Suppose that K is an algebraic number field. It is a simple exercise to show that all the elements of K are algebraic numbers, so that $K \subseteq \mathbb{A}$. On the other hand, K is a finite dimensional vector space over $\mathbb{Q}$. If $\{\alpha_1, \ldots, \alpha_n\}$ is a basis of K over $\mathbb{Q}$, then it is easy to see that $K = \mathbb{Q}(\alpha_1, \ldots, \alpha_n)$, the field obtained by adjoining the numbers $\alpha_1, \ldots, \alpha_n$ to $\mathbb{Q}$.

In fact, an algebraic number field has a far simpler description. As a first step, we consider the following reduction argument.

THEOREM 2.12. *Suppose that $K = H(\alpha, \beta)$, where H is an algebraic number field and $\alpha, \beta \in \mathbb{A}$. Then there exists an algebraic number $\gamma \in K$ such that $K = H(\gamma)$.*

PROOF. Observe first of all that α and β are algebraic over H, since $\mathbb{Q} \subseteq H$ clearly implies $\mathbb{Q}[t] \subseteq H[t]$. Let $p(t), q(t) \in H[t]$ denote respectively the minimum polynomials of α and β over H, with roots

$$\alpha^{(1)}, \ldots, \alpha^{(n)} \quad \text{and} \quad \beta^{(1)}, \ldots, \beta^{(m)}$$

in $\mathbb{C}$. Here we use the convention that $\alpha = \alpha^{(1)}$ and $\beta = \beta^{(1)}$. We also assume that $m \geqslant 2$, for otherwise $\beta \in H$ and the proof is complete.

By Theorem 2.9, the polynomials $p(t)$ and $q(t)$ are irreducible in $H[t]$. It follows from Theorem 1.4 that the roots $\alpha^{(1)}, \ldots, \alpha^{(n)}$ are distinct and the roots $\beta^{(1)}, \ldots, \beta^{(m)}$ are distinct. Hence for every $i = 1, \ldots, n$ and $j = 2, \ldots, m$, the equation

$$\alpha^{(i)} + x\beta^{(j)} = \alpha^{(1)} + x\beta^{(1)}$$

has at most one solution in H. Also, there are only finitely many such equations. We can therefore choose a number $c \in H$ such that

$$\alpha^{(i)} + c\beta^{(j)} \neq \alpha^{(1)} + c\beta^{(1)}$$

for every $i = 1, \ldots, n$ and $j = 2, \ldots, m$. Now let $\gamma = \alpha + c\beta$. We next show that $H(\gamma) = H(\alpha, \beta)$. It is clear that $H(\gamma) \subseteq H(\alpha, \beta)$. To show that $H(\alpha, \beta) \subseteq H(\gamma)$, it suffices to show that $\alpha, \beta \in H(\gamma)$. Indeed, since $\alpha = \gamma - c\beta$, it suffices to show that $\beta \in H(\gamma)$.

Note first of all that $p(\gamma - c\beta) = 0$. It follows that the number β satisfies the equations $p(\gamma - ct) = 0$ and $q(t) = 0$. On the other hand, it is easy to show that the polynomials $p(\gamma - ct)$ and $q(t)$ have only the root $\beta = \beta^{(1)}$ in common. Let $r(t) \in (H(\gamma))[t]$ be the minimum polynomial of β over $H(\gamma)$. Then it is not difficult to show that $r(t) \mid p(\gamma - ct)$ and $r(t) \mid q(t)$ in $(H(\gamma))[t]$. But then the polynomial $r(t)$ cannot be of higher degree than 1, for otherwise the polynomials $p(\gamma - ct)$ and $q(t)$ would have more than one root in common. Hence $r(t) = t + \mu$ for some $\mu \in H(\gamma)$. It is easy to see that $\beta = -\mu \in H(\gamma)$ as required. ◯

Suppose now that K is an algebraic umber field. Starting with the description $K = \mathbb{Q}(\alpha_1, \ldots, \alpha_n)$, where $\{\alpha_1, \ldots, \alpha_n\}$ is a basis of K as a vector space over $\mathbb{Q}$, and applying Theorem 2.12 a finite number of times, we obtain the following far simpler description of K.

THEOREM 2.13. *Suppose that K is an algebraic number field. Then there exists an algebraic number $\theta \in K$ such that $K = \mathbb{Q}(\theta)$.*

Suppose that $K = \mathbb{Q}(\theta)$ is an algebraic number field. We complete this section by establishing a relationship between the degree of K and the degree of the minimum polynomial of the algebraic number θ.

THEOREM 2.14. *Suppose that $K = \mathbb{Q}(\theta)$ is an algebraic number field. Then* $\deg p(t) = [K : \mathbb{Q}]$, *where $p(t) \in \mathbb{Q}[t]$ is the minimum polynomial of θ over $\mathbb{Q}$.*

PROOF. We elaborate on our proof of Theorem 2.10. Let

$$m = \deg p(t) \quad \text{and} \quad n = [K : \mathbb{Q}].$$

Then the elements $1, \theta, \ldots, \theta^n$ are linearly dependent over $\mathbb{Q}$. An argument similar to the first part of the proof of Theorem 2.10 will give $m \leqslant n$. On the other hand, as in the second part of the proof of Theorem 2.10, K is spanned by the set $\{1, \theta, \ldots, \theta^{m-1}\}$ as a vector space over $\mathbb{Q}$. Hence $m \geqslant n$. ◯

REMARK. In fact, we have also shown that the set $\{1, \theta, \ldots, \theta^{n-1}\}$, where $n = [K : \mathbb{Q}]$, is a basis of the algebraic number field $K = \mathbb{Q}(\theta)$ as a vector space over $\mathbb{Q}$.

2.4. Conjugates

Suppose that $K = \mathbb{Q}(\theta)$ is an algebraic number field of degree n, and $p(t) \in \mathbb{Q}[t]$ is the minimum polynomial of θ over $\mathbb{Q}$, with distinct roots

$$\theta^{(1)}, \ldots, \theta^{(n)} \tag{2.5}$$

in $\mathbb{C}$. The complex numbers (2.5) are called the conjugates of θ, with the convention that $\theta = \theta^{(1)}$.

Suppose next that $\alpha \in K = \mathbb{Q}(\theta)$. Since the set $\{1, \theta, \ldots, \theta^{n-1}\}$ forms a basis of K as a vector space over $\mathbb{Q}$, there exists a unique polynomial $r(t) \in \mathbb{Q}[t]$ with $\deg r(t) < n$ such that $\alpha = r(\theta)$. The elements $\alpha^{(i)} = r(\theta^{(i)})$, where $i = 1, \ldots, n$, are called the K-conjugates of α, and the polynomial

$$f_\alpha(t) = \prod_{i=1}^{n} \left(t - \alpha^{(i)}\right) = \prod_{i=1}^{n} \left(t - r(\theta^{(i)})\right)$$

is called the field polynomial of α over K.

THEOREM 2.15. *Suppose that $\alpha \in K = \mathbb{Q}(\theta)$, where $[K : \mathbb{Q}] = n$. Then*

(i) *the field polynomial $f_\alpha(t) \in \mathbb{Q}[t]$, and is a power of the minimum polynomial $p_\alpha(t) \in \mathbb{Q}[t]$ of α over $\mathbb{Q}$;*
(ii) *the K-conjugates of α are the roots of $p_\alpha(t)$ in $\mathbb{C}$, each repeated n/m times, and where $m = \deg p_\alpha(t)$ is a divisor of n;*
(iii) *the element $\alpha \in \mathbb{Q}$ if and only if all its K-conjugates are identical; and*
(iv) *$\mathbb{Q}(\alpha) = \mathbb{Q}(\theta)$ if and only if all the K-conjugates of α are distinct.*

PROOF. (i) It is easy to see that the coefficients of $f_\alpha(t)$ are symmetric polynomials of the form $h(\theta^{(1)}, \ldots, \theta^{(n)})$. By Theorem 1.8, these symmetric polynomials can be expressed as polynomials where the variables are the elementary symmetric polynomials

$$s_1(\theta^{(1)}, \ldots, \theta^{(n)}), \ldots, s_n(\theta^{(1)}, \ldots, \theta^{(n)}) \tag{2.6}$$

and the coefficients are in $\mathbb{Q}$. Note that each of the terms in (2.6) is a coefficient of the minimum polynomial $p(t)$ of θ over $\mathbb{Q}$, and is therefore an element of $\mathbb{Q}$. It follows that $f_\alpha(t) \in \mathbb{Q}[t]$. On the other hand, it is easy to check that $f_\alpha(\alpha) = 0$, and so $p_\alpha(t) \mid f_\alpha(t)$ in $\mathbb{Q}[t]$. We can therefore write

$$f_\alpha(t) = p_\alpha^s(t) h(t),$$

where $p_\alpha(t)$ and $h(t)$ are coprime in $\mathbb{Q}[t]$. To complete the proof, it suffices to prove that $h(t)$ is identically equal to 1. Clearly $h(t)$ is monic, so it suffices to prove that $h(t)$ is constant. Suppose on the contrary that $h(t)$ is non-constant. Then at least one of the roots $r(\theta^{(i)})$ of $f_\alpha(t)$ must also be a root of $h(t)$, and so the polynomial $h(r(t))$ vanishes when $t = \theta^{(i)}$ for some $i = 1, \ldots, n$. If $p(t) \in \mathbb{Q}[t]$ is the minimum polynomial of θ over $\mathbb{Q}$, then it is also the minimum polynomial of $\theta^{(i)}$ over $\mathbb{Q}$, and so $p(t) \mid h(r(t))$ in $\mathbb{Q}[t]$. It follows that $h(r(t))$ vanishes at $\theta^{(i)}$ for every $i = 1, \ldots, n$, so that in particular, we have $h(r(\theta)) = h(\alpha) = 0$. This implies that $p_\alpha(t) \mid h(t)$ in $\mathbb{Q}[t]$, contradicting our assumption that $p_\alpha(t)$ and $h(t)$ are coprime in $\mathbb{Q}[t]$.

(ii) is an immediate consequence of (i).

(iii) If all the K-conjugates of α are the same, then $f_\alpha(t) = (t - \alpha)^n$, so that $p_\alpha(t) = t - \alpha$, whence $\alpha \in \mathbb{Q}$. Conversely, if $\alpha \in \mathbb{Q}$, then $p_\alpha(t) = t - \alpha$, so that $f_\alpha(t) = (t - \alpha)^n$, whence all the K-conjugates of α are the same.

(iv) Since $\alpha \in \mathbb{Q}(\theta)$, we must have $\mathbb{Q} \subseteq \mathbb{Q}(\alpha) \subseteq \mathbb{Q}(\theta)$. By Theorem 2.8, we have

$$[\mathbb{Q}(\theta) : \mathbb{Q}] = [\mathbb{Q}(\theta) : \mathbb{Q}(\alpha)][\mathbb{Q}(\alpha) : \mathbb{Q}].$$

In view of Theorem 2.14, we have $\mathbb{Q}(\alpha) = \mathbb{Q}(\theta)$ if and only if $m = n$, if and only if $p_\alpha(t) = f_\alpha(t)$, if and only if all the K-conjugates of α are distinct. ◯

REMARKS. (i) Note that an important consequence of Theorem 2.15 is the fact that the values of the K-conjugates $\alpha^{(1)}, \ldots, \alpha^{(n)}$ are independent of the choice of θ such that $K = \mathbb{Q}(\theta)$, provided that $\alpha \in K$.

(ii) Suppose that θ is the real cube root of 5. Then $K = \mathbb{Q}(\theta)$ is a subfield of $\mathbb{R}$. The conjugates of θ are θ, $\omega\theta$ and $\omega^2\theta$, where ω is a non-real cube root of 1. Clearly $\omega\theta$ and $\omega^2\theta$ are not elements of K. Hence the conjugates of θ need not be in K. Similarly, if $\alpha \in K$, then the K-conjugates of α need not be in K.

2.5. Algebraic Integers

We have already seen two examples of "integers" within an algebraic number field, the rational integers within $\mathbb{Q}$ and the gaussian integers within $\mathbb{Q}(\mathrm{i})$. Our task in this section is to give a reasonable definition of "integers" within an algebraic number field.

REMARK. Suppose that $K = \mathbb{Q}(\theta)$ is an algebraic number field. It seems reasonable that the set of integers within this algebraic number field should satisfy the following four conditions:

(i) The integers in K form a ring. In other words, if α and β are integers in K, then so are $\alpha + \beta$, $\alpha - \beta$ and $\alpha\beta$.

(ii) If $\alpha \in \mathbb{Q}$ is an integer in K, then $\alpha \in \mathbb{Z}$. In other words, no rational number apart from the rational integers can be integers in K.

(iii) If $\alpha \in K$ is an integer in K, then its K-conjugates should also be integers, though they do not necessarily belong to K.

(iv) For every $\gamma \in K$, there exists $m \in \mathbb{N}$ such that $m\gamma$ is an integer in K.

The following definition turns out to satisfy all these four requirements. A number $\alpha \in \mathbb{C}$ is said to be an algebraic integer if there exists a monic polynomial $q(t) \in \mathbb{Z}[t]$ such that $q(\alpha) = 0$; in other words, if α is a root of a monic polynomial with rational integer coefficients.

Clearly condition (iii) is automatically satisfied. It is also not difficult to show that condition (iv) is satisfied. On the other hand, condition (ii) will follow from the result below.

THEOREM 2.16. *A number $\alpha \in \mathbb{C}$ is an algebraic integer if and only if its minimum polynomial over $\mathbb{Q}$ has coefficients in $\mathbb{Z}$.*

PROOF. Let $p(t) \in \mathbb{Q}[t]$ be the minimum polynomial of α over $\mathbb{Q}$. If $p(t) \in \mathbb{Z}[t]$, then α is an algebraic integer. Conversely, if α is an algebraic integer, then there exists a monic polynomial $q(t) \in \mathbb{Z}[t]$ such that $q(\alpha) = 0$. On the other hand, we know that $p(t) \mid q(t)$ in $\mathbb{Q}[t]$. It follows from Gauss's lemma that there exists a non-zero $\lambda \in \mathbb{Q}$ such that $\lambda p(t) \in \mathbb{Z}[t]$ and $\lambda p(t) \mid q(t)$ in $\mathbb{Z}[t]$. Since both $p(t)$ and $q(t)$ are monic, we must have $\lambda = 1$. ◯

THEOREM 2.17. *Suppose that $K = \mathbb{Q}(\theta)$ is an algebraic number field. Then the algebraic integers in K form a ring.*

PROOF. It is sufficient to show that if α and β are integers, then so are $\alpha + \beta$, $\alpha - \beta$ and $\alpha\beta$. Let

$$\alpha^{(1)}, \ldots, \alpha^{(m)} \quad \text{and} \quad \beta^{(1)}, \ldots, \beta^{(n)}$$

denote respectively the conjugates of α and β, with the convention that $\alpha = \alpha^{(1)}$ and $\beta = \beta^{(1)}$. Suppose that $p(t) \in \mathbb{Q}[t]$ is the minimum polynomial of α over $\mathbb{Q}$.

To show that $\alpha + \beta$ is an algebraic integer, consider the polynomial

$$g(t) = \prod_{j=1}^{n} p(t - \beta^{(j)}).$$

By Theorem 2.16, we have $p(t) \in \mathbb{Z}[t]$. Hence the coefficients of $g(t)$ are symmetric polynomials in $\beta^{(1)}, \ldots, \beta^{(n)}$ with coefficients in $\mathbb{Z}$. It follows from Theorem 1.8 that $g(t) \in \mathbb{Z}[t]$. On the other hand, since $p(t)$ is monic, it follows that $g(t)$ is also monic. It is easy to check that $g(\alpha + \beta) = 0$, and so $\alpha + \beta$ is an algebraic integer.

The case for $\alpha - \beta$ is almost similar.

To show that $\alpha\beta$ is an algebraic integer, consider the polynomial

$$h(t) = \prod_{j=1}^{n} (\beta^{(j)})^m p\left(\frac{t}{\beta^{(j)}}\right).$$

Similar arguments as above show that $h(t) \in \mathbb{Z}[t]$. Note also that $h(t)$ is monic and $h(\alpha\beta) = 0$. It follows that $\alpha\beta$ is an algebraic integer. ◯

To complete this section, we now apply similar techniques to show that algebraic integers can be characterized in terms of other algebraic integers.

THEOREM 2.18. *Suppose that $\alpha \in \mathbb{C}$ is a root of a monic polynomial equation whose coefficients are algebraic integers. Then α is an algebraic integer.*

PROOF. Suppose that $\alpha \in \mathbb{C}$ is a root of the polynomial

$$q(t) = t^n + \gamma_{n-1} t^{n-1} + \ldots + \gamma_0,$$

where $\gamma_0, \ldots, \gamma_{n-1}$ are algebraic numbers. For every $j = 0, \ldots, n-1$, denote the conjugates of γ_j by $\gamma_j^{(1)}, \ldots, \gamma_j^{(m_j)}$, and consider the monic polynomial

$$g(t) = \prod_{i_0=1}^{m_0} \ldots \prod_{i_{n-1}=1}^{m_{n-1}} \left(t^n + \gamma_{n-1}^{(i_{n-1})} t^{n-1} + \ldots + \gamma_0^{(i_0)} \right).$$

Multiplying out, it is not difficult to see that each coefficient in $g(t)$ is a sum of numbers of the form

$$\sum_{j_1+\ldots+j_s=k} \sum_{i_{j_1}} \cdots \sum_{i_{j_s}} \gamma_{j_1}^{(i_{j_1})} \ldots \gamma_{j_s}^{(i_{j_s})} = \sum_{j_1+\ldots+j_s=k} \prod_{\mu=1}^{s} \left(\sum_{i_{j_\mu}} \gamma_{j_\mu}^{(i_{j_\mu})} \right).$$

The usual arguments on symmetric polynomials give

$$\sum_{i_{j_\mu}} \gamma_{j_\mu}^{(i_{j_\mu})} \in \mathbb{Q},$$

in view of Theorem 1.8. Hence all the coefficients in the polynomial $g(t)$ are in $\mathbb{Q}$. These coefficients are also algebraic integers, in view of requirement (iii) and Theorem 2.17. It now follows from requirement (ii) that $g(t) \in \mathbb{Z}[t]$. Finally, note that $q(t)$ is a factor of $g(t)$, so we must have $g(\alpha) = 0$. ◯

2.6. Discriminants and Integral Bases

In this section, we establish a simple way of describing the ring of integers within an algebraic number field. To achieve this, we first introduce the notion of the discriminant of a basis of an algebraic number field.

Suppose that $K = \mathbb{Q}(\theta)$ is an algebraic number field of degree n, and $\{\alpha_1, \ldots, \alpha_n\}$ is a basis of K as a vector space over $\mathbb{Q}$. For every $j = 1, \ldots, n$, we let $\alpha_j^{(1)}, \ldots, \alpha_j^{(n)}$ denote the K-conjugates of α_j, and define the discriminant of the basis $\{\alpha_1, \ldots, \alpha_n\}$ to be the quantity

$$\Delta[\alpha_1, \ldots, \alpha_n] = \begin{vmatrix} \alpha_1^{(1)} & \ldots & \alpha_n^{(1)} \\ \vdots & & \vdots \\ \alpha_1^{(n)} & \ldots & \alpha_n^{(n)} \end{vmatrix}^2.$$

It is easy to see that the discriminant is well defined in the sense that its value does not depend on the ordering of either the set $\{\alpha_1, \ldots, \alpha_n\}$ or the K-conjugates, provided that the K-conjugates are dictated by the same ordering of the conjugates $\theta^{(1)}, \ldots, \theta^{(n)}$ of θ.

THEOREM 2.19. *Suppose that $K = \mathbb{Q}(\theta)$ is an algebraic number field of degree n. Suppose further that $\{\alpha_1, \ldots, \alpha_n\}$ and $\{\beta_1, \ldots, \beta_n\}$ are bases of K as a vector space over $\mathbb{Q}$. If for every $k = 1, \ldots, n$, we have*

$$\beta_k = \sum_{j=1}^{n} c_{jk} \alpha_j, \tag{2.7}$$

where $c_{jk} \in \mathbb{Q}$ for every $j, k = 1, \ldots, n$, then

$$\Delta[\beta_1, \ldots, \beta_n] = \begin{vmatrix} c_{11} & \ldots & c_{1n} \\ \vdots & & \vdots \\ c_{n1} & \ldots & c_{nn} \end{vmatrix}^2 \Delta[\alpha_1, \ldots, \alpha_n].$$

PROOF. The result will follow on taking determinants and squaring if we can show that

$$\begin{pmatrix} \beta_1^{(1)} & \ldots & \beta_n^{(1)} \\ \vdots & & \vdots \\ \beta_1^{(n)} & \ldots & \beta_n^{(n)} \end{pmatrix} = \begin{pmatrix} \alpha_1^{(1)} & \ldots & \alpha_n^{(1)} \\ \vdots & & \vdots \\ \alpha_1^{(n)} & \ldots & \alpha_n^{(n)} \end{pmatrix} \begin{pmatrix} c_{11} & \ldots & c_{1n} \\ \vdots & & \vdots \\ c_{n1} & \ldots & c_{nn} \end{pmatrix}.$$

In other words, we need to show that for every $i, k = 1, \ldots, n$, we have

$$\beta_k^{(i)} = \sum_{j=1}^{n} c_{jk} \alpha_j^{(i)}. \tag{2.8}$$

Recall that for every $j = 1, \ldots, n$, there exists a unique polynomial $r_j(t) \in \mathbb{Q}[t]$ with $\deg r_j(t) < n$ such that $\alpha_j = r_j(\theta)$. Similarly, for every $k = 1, \ldots, n$, there exists a unique polynomial $s_k(t) \in \mathbb{Q}[t]$ with $\deg s_k(t) < n$ such that $\beta_k = s_k(\theta)$. It then follows from (2.7) that for every $k = 1, \ldots, n$, we must have

$$s_k(t) = \sum_{j=1}^{n} c_{jk} r_j(t).$$

The identity (2.8) now follows on letting $t = \theta^{(i)}$. ◯

Let us now calculate the discriminant of the basis $\{1, \theta, \ldots, \theta^{n-1}\}$ of an algebraic number field $K = \mathbb{Q}(\theta)$, where $[K : \mathbb{Q}] = n$. Using the fact that $(\theta^i)^{(j)} = (\theta^{(j)})^i$ for every $i = 0, \ldots, n-1$ and $j = 1, \ldots, n$, we have

$$\begin{aligned}\Delta[1, \theta, \ldots, \theta^{n-1}] &= \begin{vmatrix} 1 & \theta^{(1)} & (\theta^{(1)})^2 & \ldots & (\theta^{(1)})^{n-1} \\ \vdots & \vdots & \vdots & & \vdots \\ 1 & \theta^{(n)} & (\theta^{(n)})^2 & \ldots & (\theta^{(n)})^{n-1} \end{vmatrix}^2 \\ &= \prod_{1 \leqslant i < j \leqslant n} (\theta^{(i)} - \theta^{(j)})^2.\end{aligned}$$

Here the discriminant is the square of a Vandermonde determinant. Note that since the conjugates of θ are distinct, we must have $\Delta[1, \theta, \ldots, \theta^{n-1}] \neq 0$. On the other hand, it is clear that $\Delta[1, \theta, \ldots, \theta^{n-1}]$ is symmetric with respect to the conjugates of θ. It follows from Theorem 1.8 that $\Delta[1, \theta, \ldots, \theta^{n-1}] \in \mathbb{Q}$. Also $\Delta[1, \theta, \ldots, \theta^{n-1}] > 0$ if all the conjugates of θ are real. We have therefore proved the following result.

THEOREM 2.20. *Suppose that $K = \mathbb{Q}(\theta)$ is an algebraic number field. Then the discriminant of any basis of K is rational and non-zero. Furthermore, if all the conjugates of θ are real, then the discriminant of any basis of K is positive.*

Suppose that $K = \mathbb{Q}(\theta)$ is an algebraic number field of degree n. Recall that K has a basis of n elements as a vector space over $\mathbb{Q}$. For example, the set $\{1, \theta, \ldots, \theta^{n-1}\}$ is such a basis.

The ring $\mathfrak{O}$ of algebraic integers in K is an abelian group under addition. We say that a set $\{\alpha_1, \ldots, \alpha_s\} \subseteq \mathfrak{O}$ is an integral basis, or $\mathbb{Z}$-basis, of the ring $\mathfrak{O}$ if every element $\alpha \in \mathfrak{O}$ is uniquely representable in the form

$$\alpha = b_1\alpha_1 + \ldots + b_s\alpha_s,$$

where $b_1, \ldots, b_s \in \mathbb{Z}$.

Our aim here is to show that an integral basis for $\mathfrak{O}$ exists and contains exactly n elements. The first step in this direction is given by the following result on the discriminant of bases of the algebraic number field K which consist entirely of algebraic integers.

THEOREM 2.21. *Suppose that $K = \mathbb{Q}(\theta)$ is an algebraic number field of degree n. Suppose further that $\{\alpha_1, \ldots, \alpha_n\} \subseteq \mathfrak{O}$ is a basis of K as a vector space over $\mathbb{Q}$. Then $\Delta[\alpha_1, \ldots, \alpha_n] \in \mathbb{Z} \setminus \{0\}$.*

PROOF. On the one hand, we have $\Delta[\alpha_1, \ldots, \alpha_n] \in \mathbb{Q} \setminus \{0\}$, in view of Theorem 2.20. On the other hand, $\alpha_1, \ldots, \alpha_n$ and all their K-conjugates are algebraic integers, in view of condition (iii) concerning algebraic integers. It follows from Theorem 2.17 that $\Delta[\alpha_1, \ldots, \alpha_n]$ is an algebraic integer. The result now follows from condition (ii) concerning algebraic integers. ◯

Theorem 2.21 enables us to use the Principle of induction to establish the existence of integral bases.

THEOREM 2.22. *Suppose that $K = \mathbb{Q}(\theta)$ is an algebraic number field of degree n. Then the ring $\mathfrak{O}$ of algebraic integers in K has an integral basis of n elements.*

PROOF. In view of condition (iv) concerning algebraic integers, we assume without loss of generality that θ is an algebraic integer. Let S denote the set of all bases of K which consist entirely of algebraic integers. Then $\{1, \theta, \ldots, \theta^{n-1}\} \in S$, so that S is non-empty. As a consequence of Theorem 2.21, we conclude that there exists a basis $\{\omega_1, \ldots, \omega_n\} \in S$ such that $|\Delta[\omega_1, \ldots, \omega_n]|$ is minimal. We prove that $\{\omega_1, \ldots, \omega_n\}$ is an integral basis of $\mathfrak{O}$.

Suppose on the contrary that $\{\omega_1, \ldots, \omega_n\}$ is not an integral basis of $\mathfrak{O}$. Then there exists $\alpha \in \mathfrak{O}$ which is not representable as a linear combination of the elements of $\{\omega_1, \ldots, \omega_n\}$ with coefficients in $\mathbb{Z}$. On the other hand, since $\alpha \in K$ and $\{\omega_1, \ldots, \omega_n\}$ is a basis of K, we have a unique representation

$$\alpha = b_1\omega_1 + \ldots + b_n\omega_n,$$

where $b_1, \ldots, b_n \in \mathbb{Q}$. Then at least one of the coefficients $b_1, \ldots, b_n$ does not belong to $\mathbb{Z}$. We may assume without loss of generality that $b_1 \notin \mathbb{Z}$. Then $b_1 = b + r$, where $b \in \mathbb{Z}$ and $0 < r < 1$. Consider now the basis $\{\nu_1, \omega_2, \ldots, \omega_n\} \in S$, where $\nu_1 = \alpha - b\omega_1 \in \mathfrak{O}$. The change of basis matrix from the basis $\{\omega_1, \ldots, \omega_n\}$ to the basis $\{\nu_1, \omega_2, \ldots, \omega_n\}$ is given by the upper triangular matrix

$$\begin{pmatrix} b_1 - b & b_2 & b_3 & b_4 & \ldots & b_n \\ & 1 & 0 & 0 & \ldots & 0 \\ & & 1 & 0 & \ldots & 0 \\ & & & 1 & & \vdots \\ & & & & \ddots & 0 \\ & & & & & 1 \end{pmatrix},$$

with determinant r. It follows from Theorem 2.19 that

$$\Delta[\nu_1, \omega_2, \ldots, \omega_n] = r^2\Delta[\omega_1, \ldots, \omega_n],$$

contradicting the minimality of $|\Delta[\omega_1, \ldots, \omega_n]|$. ◯

2.7. Quadratic Number Fields

A quadratic number field is an algebraic number field K of degree 2. Then $K = \mathbb{Q}(\theta)$, where θ is a root of a quadratic polynomial irreducible over $\mathbb{Q}$. In view of condition (iv) concerning algebraic integers, we may assume that θ is an algebraic integer. Suppose that θ is a root of the polynomial $t^2 + bt + c$, where $b, c \in \mathbb{Z}$. Then

$$\theta = \frac{-b \pm \sqrt{b^2 - 4c}}{2}.$$

If we write $b^2 - 4c = s^2d$, where $s, d \in \mathbb{Z}$ and d is squarefree, then it is easy to see that $\mathbb{Q}(\theta) = \mathbb{Q}(\sqrt{d})$. We have therefore established the following result.

THEOREM 2.23. *Every quadratic number field is of the form $\mathbb{Q}(\sqrt{d})$, where $d \in \mathbb{Z}$ is squarefree.*

Consider a quadratic number field $\mathbb{Q}(\sqrt{d})$, where $d \in \mathbb{Z}$ is squarefree. Our next task is to determine all the algebraic integers in $\mathbb{Q}(\sqrt{d})$.

It is easy to see that every number in $\mathbb{Q}(\sqrt{d})$ is of the form

$$\frac{\ell + m\sqrt{d}}{n}, \tag{2.9}$$

where $\ell, m, n \in \mathbb{Z}$ and $n \neq 0$. We may further assume that ℓ, m, n are relatively prime and $n \in \mathbb{N}$.

The number (2.9) is an algebraic integer if and only if it satisfies a quadratic equation of the form $t^2 + bt + c = 0$, where $b, c \in \mathbb{Z}$; in other words, if

$$(\ell + m\sqrt{d})^2 + bn(\ell + m\sqrt{d}) + cn^2 = 0.$$

This last equation is satisfied if and only if

$$\ell^2 + m^2d + bn\ell + cn^2 = 0 \quad \text{and} \quad m(2\ell + bn) = 0. \tag{2.10}$$

The case $m = 0$ is trivial, for then (2.9) is an integer if and only if $n \mid \ell$. We may therefore assume that $m \neq 0$, so that

$$-2\ell = bn. \tag{2.11}$$

Substituting this into the first equation in (2.10), we obtain

$$m^2d - \ell^2 + cn^2 = 0.$$

Let $g = (\ell, n)$. Then $g^2 \mid m^2d$. Since d is squarefree, it follows that $g \mid m$. Since ℓ, m, n are relatively prime, we must have $g = 1$, so that $(\ell, n) = 1$. It follows from (2.11) that $n \mid 2$, so that $n = 1$ or $n = 2$.

Suppose that $n = 1$. Then the equations in (2.10) are satisfied with $b = -2\ell$ and $c = \ell^2 - m^2 d$. It remains to investigate the case when $n = 2$. Note that the number

$$\frac{\ell + m\sqrt{d}}{2} \tag{2.12}$$

satisfies the quadratic equation

$$t^2 - \ell t + \frac{\ell^2 - m^2 d}{4} = 0,$$

and is therefore an algebraic integer if and only if $(\ell^2 - m^2 d)/4 \in \mathbb{Z}$; in other words, if and only if $\ell^2 \equiv m^2 d \bmod 4$. The condition $(\ell, n) = 1$ implies that ℓ must be odd, so that $\ell^2 \equiv 1 \bmod 4$. It follows that the number (2.12) is an algebraic integer if and only if ℓ is odd and $m^2 d \equiv 1 \bmod 4$. This last congruence holds if and only if m is odd and $d \equiv 1 \bmod 4$.

We have therefore proved the following result.

THEOREM 2.24. *Suppose that $d \in \mathbb{Z}$ is squarefree, and $\mathfrak{O}$ is the ring of integers in the quadratic number field $\mathbb{Q}(\sqrt{d})$.*

(i) *If $d \not\equiv 1 \bmod 4$, then $\{1, \sqrt{d}\}$ is an integral basis of $\mathfrak{O}$.*
(ii) *If $d \equiv 1 \bmod 4$, then $\{1, \frac{1}{2} + \frac{1}{2}\sqrt{d}\}$ is an integral basis of $\mathfrak{O}$.*

REMARKS. (i) Note that in $\mathbb{Q}(\mathrm{i})$, the ring of integers is precisely the collection of all gaussian integers.

(ii) It is easy to see that the quadratic fields $\mathbb{Q}(\sqrt{d})$, where $d \in \mathbb{Z}$, are pairwise distinct.

2.8. Cyclotomic Number Fields

The starting point for cyclotomic number fields is the irreducibility of the cyclotomic polynomial

$$f(t) = t^{p-1} + t^{p-2} + \ldots + t + 1 \tag{2.13}$$

in $\mathbb{Q}[t]$ for any positive rational prime p. To see this, note that

$$f(t+1) = t^{p-1} + p(t^{p-2} + \ldots) + p,$$

and the irreducibility now follows immediately from Eisenstein's criterion.

For any positive rational prime p, the p-th cyclotomic number field is the algebraic number field $\mathbb{Q}(\zeta)$, where $\zeta = \mathrm{e}^{2\pi\mathrm{i}/p}$ is a primitive p-th root of unity. Clearly the polynomial (2.13) is the minimum polynomial of ζ over $\mathbb{Q}$, so that $\mathbb{Q}(\zeta)$ is an algebraic number field of degree $p-1$. Also, the case $p = 2$ is trivial, since $\zeta = -1$ in this case, and $\mathbb{Q}(-1) = \mathbb{Q}$. We therefore assume that p is an odd positive rational prime.

An obvious choice for a basis of $\mathbb{Q}(\zeta)$ as a vector space over $\mathbb{Q}$ is given by the set $\{1, \zeta, \ldots, \zeta^{p-2}\}$. Our aim in this section is to prove the following stronger result.

THEOREM 2.25. *Suppose that p is an odd positive rational prime, $\zeta = \mathrm{e}^{2\pi\mathrm{i}/p}$ and $\mathfrak{O}$ is the ring of integers in the cyclotomic number field $\mathbb{Q}(\zeta)$. Then the set $\{1, \zeta, \ldots, \zeta^{p-2}\}$ is an integral basis of $\mathfrak{O}$.*

We begin by investigating the discriminant of our chosen basis.

THEOREM 2.26. *Under the hypotheses of Theorem 2.25, we have*

$$\Delta[1, \zeta, \ldots, \zeta^{p-2}] = (-1)^{\frac{1}{2}(p-1)} p^{p-2}.$$

PROOF. As in the discussion before Theorem 2.20, we have

$$\Delta[1, \zeta, \ldots, \zeta^{p-2}] = \prod_{1 \leqslant i < j \leqslant p-1} (\zeta^i - \zeta^j)^2.$$

Clearly $\zeta, \ldots, \zeta^{p-1}$ are the roots of the minimum polynomial (2.13), and

$$\frac{t^p - 1}{t - 1} = t^{p-1} + t^{p-2} + \ldots + t + 1 = \prod_{j=1}^{p-1} (t - \zeta^j). \tag{2.14}$$

Differentiating formally with respect to t, letting $t = \zeta^i$ and noting that $\zeta^p = 1$, we obtain

$$-\frac{p\zeta^{p-i}}{1-\zeta^i} = \prod_{\substack{j=1\\ j\neq i}}^{p-1}(\zeta^i - \zeta^j). \tag{2.15}$$

Substituting $t = 0$ and $t = 1$ into (2.14), we obtain respectively

$$\prod_{i=1}^{p-1}\zeta^{p-i} = \prod_{j=1}^{p-1}\zeta^j = 1 \quad \text{and} \quad \prod_{i=1}^{p-1}(1-\zeta^i) = p, \tag{2.16}$$

so that

$$\prod_{i=1}^{p-1}\frac{\zeta^{p-i}}{1-\zeta^i} = \frac{1}{p}.$$

Combining this with (2.15), we obtain

$$\begin{aligned} p^{p-2} &= \prod_{i=1}^{p-1}\prod_{\substack{j=1\\ j\neq i}}^{p-1}(\zeta^i - \zeta^j) = \left(\prod_{i=1}^{p-1}\prod_{\substack{j=1\\ i<j}}^{p-1}(\zeta^i - \zeta^j)\right)\left(\prod_{i=1}^{p-1}\prod_{\substack{j=1\\ i>j}}^{p-1}(\zeta^i - \zeta^j)\right) \\ &= (-1)^{\frac{1}{2}(p-1)(p-2)}\prod_{1\leqslant i<j\leqslant p-1}(\zeta^i - \zeta^j)^2 = (-1)^{\frac{1}{2}(p-1)}\prod_{1\leqslant i<j\leqslant p-1}(\zeta^i - \zeta^j)^2. \end{aligned}$$

The result now follows on multiplying both sides by $(-1)^{\frac{1}{2}(p-1)}$. ◯

We next appeal to the number $\lambda = 1 - \zeta$.

THEOREM 2.27. *Under the hypotheses of Theorem 2.25, and with $\lambda = 1-\zeta$, the set $\{1, \lambda, \ldots, \lambda^{p-2}\}$ is a basis of $\mathbb{Q}(\zeta)$. Furthermore, we have*

$$\Delta[1, \lambda, \ldots, \lambda^{p-2}] = \Delta[1, \zeta, \ldots, \zeta^{p-2}].$$

PROOF. Note that for every $j = 0, \ldots, p-2$, we have

$$\lambda^j = (1-\zeta)^j = 1 - j\zeta + \ldots + (-1)^j\zeta^j.$$

It follows that the vector $(1, \lambda, \ldots, \lambda^{p-2})$ is obtained from the vector $(1, \zeta, \ldots, \zeta^{p-2})$ by multiplication by a triangular matrix with diagonal entries ± 1. The determinant of this triangular matrix is equal to ± 1. The first assertion follows immediately, and the second assertion follows in view of Theorem 2.19. ◯

Our aim here is to show that the set $\{1, \lambda, \ldots, \lambda^{p-2}\}$ is an integral basis of $\mathfrak{O}$, the ring of integers of $\mathbb{Q}(\zeta)$. To do so, we need the following intermediate result.

THEOREM 2.28. *Under the hypotheses of Theorem 2.25, and with $\lambda = 1 - \zeta$, every element of $\mathfrak{O}$ can be expressed in the form*

$$\frac{a_0 + a_1\lambda + \ldots + a_{p-2}\lambda^{p-2}}{p^k}, \tag{2.17}$$

where $a_0, \ldots, a_{p-2} \in \mathbb{Z}$ and $k \in \mathbb{Z}$ is non-negative.

PROOF. Let $\{\omega_1, \ldots, \omega_{p-1}\}$ be an integral basis of $\mathfrak{O}$. For every $j = 0, \ldots, p-2$, the number λ^j is an algebraic integer. It follows that

$$\lambda^j = \sum_{i=1}^{p-1} c_{ij}\omega_i, \tag{2.18}$$

where $c_{ij} \in \mathbb{Z}$ for every $i = 1, \ldots, p-1$ and $j = 0, \ldots, p-2$. Let d denote the determinant of the matrix (c_{ij}). Then it follows from Theorems 2.19, 2.26 and 2.27 that

$$(-1)^{\frac{1}{2}(p-1)}p^{p-2} = d^2\Delta[\omega_1, \ldots, \omega_{p-1}].$$

On the other hand, $\Delta[\omega_1, \ldots, \omega_{p-1}] \in \mathbb{Z} \setminus \{0\}$ by Theorem 2.21. It follows that $d = \pm p^k$ for some non-negative integer k. Solving the system of equations (2.18) by Cramer's rule, we see that each of

$\omega_1, \ldots, \omega_{p-1}$ can be expressed in the form (2.17). The result now follows, since $\{\omega_1, \ldots, \omega_{p-1}\}$ is an integral basis of $\mathfrak{O}$. ◯

THEOREM 2.29. *Under the hypotheses of Theorem 2.25, and with $\lambda = 1-\zeta$, the set $\{1, \lambda, \ldots, \lambda^{p-2}\}$ is an integral basis of $\mathfrak{O}$.*

PROOF. Suppose that the set $\{1, \lambda, \ldots, \lambda^{p-2}\}$ is not an integral basis of $\mathfrak{O}$. Then there exists an algebraic integer of the form (2.17) where k is positive and p does not divide all the rational integers $a_0, \ldots, a_{p-2}$. It follows that there exists an algebraic integer of the form

$$\frac{a_0 + a_1\lambda + \ldots + a_{p-2}\lambda^{p-2}}{p},$$

where p does not divide all the rational integers $a_0, \ldots, a_{p-2}$. Let m satisfy $p \nmid a_m$ and $p \mid a_i$ for every $i = 0, \ldots, m-1$. Then

$$\frac{a_m\lambda^m + \ldots + a_{p-2}\lambda^{p-2}}{p}$$

is an algebraic integer. By (2.16) and noting that $m \leqslant p-2$, we have

$$p = (1-\zeta)\ldots(1-\zeta^{p-1}) = (1-\zeta)^{p-1}u = \lambda^{p-1}u = \lambda^{m+1}v,$$

where u and v are algebraic integers. It follows that

$$\frac{a_m\lambda^m + \ldots + a_{p-2}\lambda^{p-2}}{\lambda^{m+1}}$$

is an algebraic integer, and therefore so is a/λ, where $a = a_m$.

We now show that if $a \in \mathbb{Z}$ and $p \nmid a$, then a/λ cannot be an algebraic integer. Let $t = a/\lambda$. Then

$$1 = \zeta^p = \left(1 - \frac{a}{t}\right)^p,$$

so that $t^p - (t-a)^p = 0$. It follows that a/λ is a root of the polynomial

$$g(t) = pt^{p-1} + p(\ldots) + a^{p-1}.$$

Since $p \nmid a$, it follows from Eisenstein's criterion that the polynomial $t^{p-1}g(1/t)$ is irreducible over $\mathbb{Q}$, and so $g(t)$ is irreducible over $\mathbb{Q}$. Since the monic polynomial $p^{-1}g(t) \notin \mathbb{Z}[t]$, it follows that a/λ is not an algebraic integer. ◯

PROOF OF THEOREM 2.25. By Theorem 2.29, the set $\{1, \lambda, \ldots, \lambda^{p-2}\}$ forms an integral basis of $\mathfrak{O}$. If we recall the proof of Theorem 2.22, then we see that the quantity

$$|\Delta[1, \lambda, \ldots, \lambda^{p-2}]|$$

is minimal among all bases of $\mathbb{Q}(\zeta)$ consisting only of algebraic integers. It follows from Theorem 2.27 that the quantity

$$|\Delta[1, \zeta, \ldots, \zeta^{p-2}]|$$

is also minimal among all bases of $\mathbb{Q}(\zeta)$ consisting only of algebraic integers. Hence $\{1, \zeta, \ldots, \zeta^{p-2}\}$ is an integral basis of $\mathfrak{O}$. ◯

2.9. Factorization

Suppose that $K = \mathbb{Q}(\theta)$ is an algebraic number field, and $\mathfrak{O}$ is the ring of algebraic integers in K.

Suppose that $\alpha, \beta \in \mathfrak{O}$ and $\alpha \neq 0$. Then we say that α divides β, denoted by $\alpha \mid \beta$, if there exists $\gamma \in \mathfrak{O}$ such that $\beta = \alpha\gamma$; in other words, we have a factorization $\beta = \alpha\gamma$. In this case, we say that α is a divisor of β.

Furthermore, we say that an algebraic integer $u \in \mathfrak{O}$ is a unit if $u \mid 1$. We also say that two algebraic integers $\alpha, \beta \in \mathfrak{O}$ are associates if $\alpha = u\beta$ for some unit $u \in \mathfrak{O}$. Finally, we say that an algebraic integer $\pi \in \mathfrak{O}$ is a prime if π is not a unit and if any divisor of π is either a unit or an associate of π.

As in the case for gaussian integers, we now define a norm on the algebraic integers in $\mathfrak{O}$. Suppose that $K = \mathbb{Q}(\theta)$ is of degree n over $\mathbb{Q}$. For every $\alpha \in K$, let $\alpha^{(1)}, \ldots, \alpha^{(n)}$ denote the K-conjugates of α. We define the norm of α by

$$N(\alpha) = \alpha^{(1)} \ldots \alpha^{(n)}.$$

THEOREM 2.30. *Suppose that $K = \mathbb{Q}(\theta)$ is an algebraic number field, and $\mathfrak{O}$ is the ring of algebraic integers in K. Suppose further that $\alpha, \beta \in \mathfrak{O}$. Then*

(i) *$N(\alpha)$ is a non-zero rational integer;*
(ii) *$N(\alpha\beta) = N(\alpha)N(\beta)$;*
(iii) *α is a unit in K if and only if $N(\alpha) = \pm 1$; and*
(iv) *α is a prime in K if $N(\alpha)$ is a rational prime.*

PROOF. (i) The field polynomial $f_\alpha(t)$ of α over K is a power of the minimum polynomial $p_\alpha(t)$ of α over $\mathbb{Q}$. Since $\alpha \in \mathfrak{O}$, we must have $p_\alpha(t) \in \mathbb{Z}[t]$, and so $f_\alpha(t) \in \mathbb{Z}[t]$. But

$$f_\alpha(t) = (t - \alpha^{(1)}) \dots (t - \alpha^{(n)}).$$

Hence $N(\alpha)$ is simply $(-1)^n$ times the coefficient of the constant term in $f_\alpha(t)$, and so must belong to $\mathbb{Z}$. On the other hand, the coefficient of the constant term in $p_\alpha(t)$ must be non-zero, since $p_\alpha(t)$ is irreducible in $\mathbb{Q}[t]$. It follows that the coefficient of the constant term in $f_\alpha(t)$ must be non-zero. Hence $N(\alpha)$ is non-zero.

(ii) Note that if $\alpha^{(1)}, \dots, \alpha^{(n)}$ and $\beta^{(1)}, \dots, \beta^{(n)}$ are respectively the K-conjugates of α and β, then $\alpha^{(1)}\beta^{(1)}, \dots, \alpha^{(n)}\beta^{(n)}$ are the K-conjugates of $\alpha\beta$.

(iii) Suppose that $N(\alpha) = \alpha^{(1)} \dots \alpha^{(n)} = \pm 1$. Since $\alpha^{(2)} \dots \alpha^{(n)}$ is an algebraic integer and

$$\alpha^{(2)} \dots \alpha^{(n)} = \frac{N(\alpha)}{\alpha} \in K,$$

it follows that $\alpha^{(2)} \dots \alpha^{(n)} \in \mathfrak{O}$, and so $\alpha \mid 1$, whence α is a unit. Suppose now that α is a unit. Then $\alpha \mid 1$, so there exists $\beta \in \mathfrak{O}$ such that $\alpha\beta = 1$. It follows from (ii) that

$$N(\alpha)N(\beta) = N(\alpha\beta) = N(1) = 1,$$

and so $N(\alpha) \mid 1$ in $\mathbb{Z}$. It follows that $N(\alpha) = \pm 1$.

(iv) Suppose that $\beta \mid \alpha$. Then there exists $\gamma \in \mathfrak{O}$ such that $\alpha = \beta\gamma$. It now follows from (ii) that $N(\alpha) = N(\beta)N(\gamma)$ in $\mathbb{Z}$. Since $N(\alpha)$ is a rational prime, we must have $N(\beta) = \pm 1$ or $N(\gamma) = \pm 1$. It follows from (iii) that β or γ is a unit. If γ is a unit, then β is an associate of α. ◯

We leave it as an exercise for the reader to establish the following result.

THEOREM 2.31. *Suppose that $K = \mathbb{Q}(\theta)$ is an algebraic number field, and $\mathfrak{O}$ is the ring of algebraic integers in K. Then every element in $\mathfrak{O}$, not zero or a unit, is representable as a product of primes in $\mathfrak{O}$.*

REMARK. Note that we have not claimed uniqueness of factorization. Consider the quadratic number field $\mathbb{Q}(\sqrt{15})$. It follows from Theorem 2.24 that the ring of integers is given by $\mathbb{Z}[\sqrt{15}]$. Here, it can be shown that the algebraic integer 10 has two essentially different factorizations

$$10 = 2 \times 5 = (5 + \sqrt{15})(5 - \sqrt{15})$$

into primes in $\mathbb{Z}[\sqrt{15}]$. This is the motivation for ideal theory which we study in Chapter 3.