8. Algebraic numbers: Rings and fields

Proposition 8.7 *Suppose that for some $\xi \in \mathbb{C}$ there exist $\theta_1, \ldots, \theta_n \in \mathbb{C}$, not all zero, such that, for all j with $1 \le j \le n$, we have $\xi\theta_j = a_{j1}\theta_1 + a_{j2}\theta_2 + \ldots + a_{jn}\theta_n$. If all $a_{ji} \in \mathbb{Q}$, then ξ is an algebraic number; if all $a_{ji} \in \mathbb{Z}$, then ξ is an algebraic integer.*

Proof. In matrix form this can be written as

$$\begin{bmatrix} a_{11}-\xi & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22}-\xi & \cdots & a_{2n} \\ \cdots & \cdots & \cdots & \cdots \\ a_{n1} & a_{n2} & \cdots & a_{nn}-\xi \end{bmatrix} \begin{bmatrix} \theta_1 \\ \theta_2 \\ \vdots \\ \theta_n \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{bmatrix}$$

The determinant of this system must vanish. Expanding it we obtain a polynomial which has ξ as root. □

Proposition 8.8 *If α and β are algebraic numbers (algebraic integers), so are $\alpha+\beta$ and $\alpha\beta$.*

Proof. Let $\alpha^m + a_1\alpha^{m-1} + \ldots + a_m = 0$ and $\beta^n + b_1\beta^{n-1} + \ldots + b_n = 0$, with $a_i, b_j \in \mathbb{Q}$ (or $a_i, b_j \in \mathbb{Z}$). For $k = mn$, let $\theta_1, \ldots, \theta_k$ be the numbers $\alpha^i\beta^j$ where $0 \le i < m$ and $0 \le j < n$ (in any order). It is easy to see that we may apply Proposition 8.7 to obtain the conclusion for $\xi_1 = \alpha+\beta$ and $\xi_2 = \alpha\beta$. □

Theorem 8.9 *The set of all algebraic numbers $\overline{\mathbb{Q}}$ (algebraic integers $\overline{\mathbb{Z}}$) is a field (a ring).* □

Exercise 8.3 *Find the minimal polynomial for each of the following algebraic numbers: -3, $\sqrt[3]{2}$, $(1+\sqrt[3]{9})/2$, $1+\sqrt{2}+\sqrt{3}$. Which of these are algebraic integers?*

Recall that from the theory of fields we know that if ξ is an algebraic number of *degree n* over a field F, then every element in the field $F(\xi)$ can be written uniquely in the form $a_0 + a_1\xi + \ldots + a_{n-1}\xi^{n-1}$, where $a_i \in F$. If $g(x)$ is the minimal polynomial of ξ over F, then the field $F(\xi)$ depends on the choice of ξ but different choices of roots of $g(x)$ yield isomorphic fields. This is because $F(\xi) \cong F[x]/(g(x))$. This also implies that if $\xi_1, \ldots, \xi_n$ are algebraic over F, then the extension $F(\xi_1, \ldots, \xi_n)$ is finite, i.e. is a finite-dimensional vector space over F.

Theorem 8.10 *The field of all algebraic numbers $\overline{\mathbb{Q}}$ is algebraically closed, i.e. every polynomial $f(x) \in \overline{\mathbb{Q}}[x]$ has a root in $\overline{\mathbb{Q}}$. The ring $\overline{\mathbb{Z}}$ of all algebraic integers is integrally closed, i.e. every monic polynomial $f(x) \in \overline{\mathbb{Z}}[x]$ has a root in $\overline{\mathbb{Z}}$.*

Sketch of the proof Let $f(x) = \sum_{0 \le j \le n} c_j x^j$ and ξ is any complex root of $f(x)$. The coefficients $c_j \in \overline{\mathbb{Q}}$ are algebraic, hence the extension $K = \mathbb{Q}(c_1, \ldots, c_n)$ is finite. Since ξ is algebraic over K, the extension $K(\xi)$ of K is also finite. Now we have a tower of extensions $\mathbb{Q} \subset K \subset K(\xi)$ and each extension step of the tower is finite. Then $K(\xi)$ is a finite extension of $\mathbb{Q}$, hence ξ is algebraic over $\mathbb{Q}$. □

Exercise 8.4 *The roots of $g(x) = x^3 - 2$ are $\sqrt[3]{2}$, $\omega\sqrt[3]{2}$, and $\omega^2\sqrt[3]{2}$, where $\omega = (-1+i\sqrt{3})/2$. Prove that, for $i = 0, 1, 2$, the fields $\mathbb{Q}(\omega^i\sqrt[3]{2})$ are isomorphic but distinct.*

An *algebraic number field* is any finite extension of $\mathbb{Q}$. Any algebraic number field must contain the ring $\mathbb{Z}$. The following result shows that, in general, an algebraic number field also contains algebraic integers different from rational integers.

Lemma 8.11 *For any algebraic number α there is an integer $n \in \mathbb{Z}$ such that $n\alpha$ is an algebraic integer.* $\square$

Exercise 8.5 *Prove that for any $n \geq 3$ the numbers $\alpha_n = \cos(2\pi/n)$ are algebraic numbers but not algebraic integers. Determine the smallest b for which $b\alpha_n$ are algebraic integers for all $n \geq 3$.*

Theorem 8.11 *The algebraic integers of any algebraic number field form a ring.* $\square$

Let F be an algebraic number field and let $I(F)$ be the set of algebraic integers of F. We say that $0 \neq \alpha \in I(F)$ is a *divisor* of $\beta \in I(F)$ if there is a $\gamma \in I(F)$ such that $\beta = \alpha\gamma$. We write $\alpha|\beta$ to denote that α is a divisor of β. Any divisor of 1 is called a *unit* of F. Nonzero $\alpha, \beta \in I(F)$ are called *associates* if α/β is a unit. For example, $3 + 2\sqrt{2}$ is a unit in $\mathbb{Q}(\sqrt{2})$ since $(3 + 2\sqrt{2})(3 - 2\sqrt{2}) = 1$.

Theorem 8.12 *The units of an algebraic number field form a multiplicative group.* $\square$

Advanced Exercise: *Determine the group of units of $\mathbb{Q}(\sqrt{2})$.*