$g(x) = cf(x)$.

2. If $f(x) \mid g(x)$ and $g(x) \mid h(x)$, prove that $f(x) \mid h(x)$.
3. If $p(x)$ is irreducible and $g(x) \mid p(x)$, prove that either $g(x)$ is a constant or $g(x) = cp(x)$ for some rational number c.
4. If $p(x)$ is irreducible, prove that $cp(x)$ is irreducible for any rational $c \neq 0$.
5. If a polynomial $f(x)$ with integral coefficients factors into a product $g(x)h(x)$ of two polynomials with coefficients in Q, prove that there is a factoring $g_1(x)h_1(x)$ with integral coefficients.
6. If $f(x)$ and $g(x)$ are primitive polynomials, and if $f(x) \mid g(x)$ and $g(x) \mid f(x)$, prove that $f(x) = \pm g(x)$.

9.2 Algebraic Numbers

Definition 9.4 *A complex number ξ is called an algebraic number if it satisfies some polynomial equation $f(x) = 0$ where $f(x)$ is a polynomial over Q.*

Every rational number r is an algebraic number because $f(x)$ can be taken as $x - r$ in this case.

Theorem 9.8 *An algebraic number ξ satisfies a unique irreducible monic polynomial equation $g(x) = 0$ over Q. Furthermore every polynomial equation over Q satisfied by ξ is divisible by $g(x)$.*

Proof. From all polynomial equations over Q satisfied by ξ, choose one of lowest degree, say $G(x) = 0$. If the leading coefficient of $G(x)$ is c, define $g(x) = c^{-1}G(x)$, so that $g(\xi) = 0$ and $g(x)$ is monic. The polynomial $g(x)$ is irreducible, for if $g(x) = h_1(x)h_2(x)$, then one at least of $h_1(\xi) = 0$ and $h_2(\xi) = 0$ would hold, contrary to the fact that $G(x) = 0$ and $g(x) = 0$ are polynomial equations over Q of least degree satisfied by ξ.

Next let $f(x) = 0$ be any polynomial equation over Q having ξ as a root. Applying Theorem 9.1, we get $f(x) = g(x)q(x) + r(x)$. The remainder $r(x)$ must be identically zero, for otherwise the degree of $r(x)$ would be less than that of $g(x)$, and ξ would be a root of $r(x)$ since $f(\xi) = g(\xi) = 0$. Hence $g(x)$ is a divisor of $f(x)$.

Finally to prove that $g(x)$ is unique, suppose that $g_1(x)$ is an irreducible monic polynomial such that $g_1(\xi) = 0$. Then $g(x) \mid g_1(x)$ by the argument above, say $g_1(x) = g(x)q(x)$. But the irreducibility of $g_1(x)$ then implies that $q(x)$ is a constant, in fact $q(x) = 1$ since $g_1(x)$ and $g(x)$ are monic. Thus we have $g_1(x) = g(x)$.

Definition 9.5 *The minimal equation of an algebraic number ξ is the equation $g(x) = 0$ described in Theorem 9.8. The minimal polynomial of ξ is $g(x)$. The degree of an algebraic number is the degree of its minimal polynomial.*

Definition 9.6 *An algebraic number ξ is an algebraic integer if it satisfies some monic polynomial equation*

$$f(x) = x^n + b_1 x^{n-1} + \cdots + b_n = 0 \tag{9.3}$$

with integral coefficients.

Theorem 9.9 *Among the rational numbers, the only ones that are algebraic integers are the integers $0, \pm 1, \pm 2, \cdots$.*

Proof. Any integer m is an algebraic integer because $f(x)$ can be taken as $x - m$. On the other hand, if any rational number m/q is an algebraic integer, then we may suppose $(m, q) = 1$, and we have

$$\left(\frac{m}{q}\right)^n + b_1\left(\frac{m}{q}\right)^{n-1} + \cdots + b_n = 0,$$

$$m^n + b_1 q m^{n-1} + \cdots + b_n q^n = 0.$$

Thus $q \mid m^n$, so that $q = \pm 1$, and m/q is an integer.

The word "integer" in Definition 9.6 is thus simply a generalization of our previous usage. In algebraic number theory, $0, \pm 1, \pm 2, \cdots$ are often referred to as "rational integers" to distinguish them from the other algebraic integers, that are not rational. For example, $\sqrt{2}$ is an algebraic integer but not a rational integer.

Theorem 9.10 *The minimal equation of an algebraic integer is monic with integral coefficients.*

Proof. The equation is monic by definition, so we need prove only that the coefficients are integers. Let the algebraic integer ξ satisfy $f(x) = 0$ as in (9.3), and let its minimal equation be $g(x) = 0$, monic and irreducible over Q. By Theorem 9.8, $g(x)$ is a divisor of $f(x)$, say $f(x) = g(x)h(x)$, and the quotient $h(x)$, like $f(x)$ and $g(x)$, is monic and has coefficients in Q. Applying Theorem 9.7, we see that $g(x)$ has integral coefficients.

Theorem 9.11 *Let n be a positive rational integer and ξ a complex number. Suppose that the complex numbers $\theta_1, \theta_2, \cdots, \theta_n$, not all zero, satisfy the equations*

$$\xi\theta_j = a_{j,1}\theta_1 + a_{j,2}\theta_2 + \cdots + a_{j,n}\theta_n, \qquad j = 1, 2, \cdots, n, \tag{9.4}$$

where the n^2 coefficients $a_{j,i}$ are rational. Then ξ is an algebraic number. Moreover, if the $a_{j,i}$ are rational integers, ξ is an algebraic integer.

Proof. Equations (9.4) can be thought of as a system of homogeneous linear equations in $\theta_1, \theta_2, \cdots, \theta_n$. Since the θ_i are not all zero, the determinant of coefficients must vanish:

$$\begin{vmatrix} \xi - a_{1,1} & -a_{1,2} & \cdots & -a_{1,n} \\ -a_{2,1} & \xi - a_{2,2} & \cdots & -a_{2,n} \\ \cdots & \cdots & \cdots & \cdots \\ -a_{n,1} & -a_{n,2} & \cdots & \xi - a_{n,n} \end{vmatrix} = 0.$$

Expansion of this determinant gives an equation $\xi^n + b_1\xi^{n-1} + \cdots + b_n = 0$, where the b_i are polynomials in the $a_{j,k}$. Thus the b_i are rational, and they are rational integers if the $a_{j,k}$ are.

Theorem 9.12 *If α and β are algebraic numbers, so are $\alpha + \beta$ and $\alpha\beta$. If α and β are algebraic integers, so are $\alpha + \beta$ and $\alpha\beta$.*

Proof. Suppose that α and β satisfy

$$\alpha^m + a_1\alpha^{m-1} + \cdots + a_m = 0,$$
$$\beta^r + b_1\beta^{r-1} + \cdots + b_r = 0$$

with rational coefficients a_i and b_j. Let $n = mr$, and define the complex numbers $\theta_1, \cdots, \theta_n$ as the numbers

$$\begin{array}{llll} 1, & \alpha, & \alpha^2, & \cdots, \quad \alpha^{m-1}, \\ \beta, & \alpha\beta, & \alpha^2\beta, & \cdots, \quad \alpha^{m-1}\beta, \\ \cdots & \cdots & \cdots & \cdots \\ \beta^{r-1}, & \alpha\beta^{r-1}, & \alpha^2\beta^{r-1}, & \cdots, \quad \alpha^{m-1}\beta^{r-1}, \end{array}$$

in any order. Thus $\theta_1, \cdots, \theta_n$ are the numbers $\alpha^s\beta^t$ with $s = 0, 1, \cdots, m-1$ and $t = 0, 1, \cdots, r-1$. Hence for any θ_j,

$$\alpha\theta_j = \alpha^{s+1}\beta^t = \begin{cases} \text{some } \theta_k & \text{if } \quad s+1 \leqq m-1 \\ (-a_1\alpha^{m-1} - a_2\alpha^{m-2} - \cdots - a_m)\beta^t & \text{if } \quad s+1 = m. \end{cases}$$

In either case we see that there are rational constants $h_{j,1}, \cdots, h_{j,n}$ such that $\alpha\theta_j = h_{j,1}\theta_1 + \cdots + h_{j,n}\theta_n$. Similarly there are rational constants $k_{j,1}, \cdots, k_{j,n}$ such that $\beta\theta_j = k_{j,1}\theta_1 + \cdots + k_{j,n}\theta_n$, and hence $(\alpha + \beta)\theta_j = (h_{j,1} + k_{j,1})\theta_1 + \cdots + (h_{j,n} + k_{j,n})\theta_n$. These equations are of the form (9.4), and so we conclude that $\alpha + \beta$ is algebraic. Furthermore, if α and β are algebraic integers, then the a_j, b_j, $h_{j,i}$, $k_{j,i}$ are all rational integers, and $\alpha + \beta$ is an algebraic integer.

We also have $\alpha\beta\theta_j = \alpha(k_{j,1}\theta_1 + \cdots + k_{j,n}\theta_n) = k_{j,1}\alpha\theta_1 + \cdots + k_{j,n}\alpha\theta_n$ from which we find $\alpha\beta\theta_j = c_{j,1}\theta_1 + \cdots + c_{j,n}\theta_n$ where $c_{j,i} = k_{j,1}h_{1,i} + k_{j,2}h_{2,i} + \cdots + k_{j,n}h_{n,i}$. Again we apply Theorem 9.11 to conclude that $\alpha\beta$ is algebraic, and that it is an algebraic integer if α and β are.

This theorem states that the set of algebraic numbers is closed under addition and multiplication, and likewise for the set of algebraic integers. The following result states a little more.

Theorem 9.13 *The set of all algebraic numbers forms a field. The class of all algebraic integers forms a ring.*

Proof. Rings and fields are defined in Definition 2.12. The rational numbers 0 and 1 serve as the zero and unit for the system. Most of the postulates are easily seen to be satisfied if we remember that algebraic numbers are complex numbers whose properties we are familiar with. The only place where any difficulty arises is in proving the existence of additive and multiplicative inverses. If $\alpha \neq 0$ is a solution of

$$a_0x^n + a_1x^{n-1} + \cdots + a_n = 0$$

then $-\alpha$ and α^{-1} are solutions of

$$a_0x^n - a_1x^{n-1} + a_2x^{n-2} - \cdots + (-1)^n a_n = 0$$

and

$$a_0 + a_1x + a_2x^2 + \cdots + a_nx^n = 0,$$

respectively. Therefore if α is an algebraic number, then so are $-\alpha$ and α^{-1}. If α is an algebraic integer, then so is $-\alpha$, but not necessarily α^{-1}. Therefore the algebraic numbers form a field, the algebraic integers a ring.

PROBLEMS

1. Find the minimal polynomial of each of the following algebraic numbers: $7, \sqrt[3]{7}, (1 + \sqrt[3]{7})/2, 1 + \sqrt{2} + \sqrt{3}$. Which of these are algebraic integers?
2. Prove that if α is algebraic of degree n, then $-\alpha$, α^{-1}, and $\alpha - 1$ are also of degree n, assuming $\alpha \neq 0$ in the case of α^{-1}.
3. Prove that if α is algebraic of degree n, and β is algebraic of degree m, then $\alpha + \beta$ is of degree $\leqq mn$. Prove a similar result for $\alpha\beta$.
4. Prove that the set of all real algebraic numbers (i.e., algebraic numbers that are real) forms a field, and the set of all real algebraic integers forms a ring.

9.3 Algebraic Number Fields

The field discussed in Theorem 9.13 contains the totality of algebraic numbers. In general, an *algebraic number field* is any subset of this total collection that is a field itself. For example, if ξ is an algebraic number, then it can be readily verified that the collection of all numbers of the form $f(\xi)/h(\xi)$, $h(\xi) \neq 0$, f and h polynomials over Q, constitutes a field. This field is denoted by $Q(\xi)$, and it is called the extension of Q by ξ.