Chapter 12

Algebraic numbers and algebraic integers

12.1 Algebraic numbers

Definition 12.1. *A number $\alpha \in \mathbb{C}$ is said to be* algebraic *if it satisfies a polynomial equation*

$$f(x) = x^n + a_1 x^{n-1} + \cdots + a_n = 0$$

with rational coefficients $a_i \in \mathbb{Q}$.

For example, $\sqrt{2}$ and $i/2$ are algebraic.

A complex number is said to be *transcendental* if it is not algebraic. Both e and π are transcendental. It is in general extremely difficult to prove a number transcendental, and there are many open problems in this area, eg it is not known if π^e is transcendental.

Theorem 12.1. *The algebraic numbers form a field $\bar{\mathbb{Q}} \subset \mathbb{C}$.*

Proof. If α satisfies the equation $f(x) = 0$ then $-\alpha$ satisfies $f(-x) = 0$, while $1/\alpha$ satisfies $x^n f(1/x) = 0$ (where n is the degree of $f(x)$). It follows that $-\alpha$ and $1/\alpha$ are both algebraic. Thus it is sufficient to show that if α, β are algebraic then so are $\alpha + \beta, \alpha\beta$.

Lemma 12.1. *Suppose $V \subset \mathbb{C}$ is a finite-dimensional vector space over $\mathbb{Q}$, with $V \neq 0$; and suppose $x \in \mathbb{C}$. If*

$$xV \subset V$$

then $x \in \bar{\mathbb{Q}}$.

Proof. Let $e_1, \ldots, e_n$ be a basis for V. Suppose

$$\begin{aligned} xe_1 &= a_{11}e_1 + \cdots a_{1n}e_n \\ xe_2 &= a_{21}e_1 + \cdots a_{2n}e_n \\ &\cdots \\ xe_n &= a_{n1}e_1 + \cdots a_{nn}e_n. \end{aligned}$$

Then

$$\det(xI - A) = 0,$$

where

$$A = \begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & & \vdots \\ a_{n1} & a_{n2} & \cdots & a_{nn} \end{pmatrix}.$$

This is a polynomial equation with coefficients in $\mathbb{Q}$. Hence $x \in \bar{\mathbb{Q}}$. □

Consider the vector space

$$V = \langle \alpha^i \beta^j : 0 \le i < m,\ 0 \le j < n \rangle$$

over $\mathbb{Q}$ spanned by the mn elements $\alpha^i \beta^j$. Evidently

$$\alpha V \subset V,\ \beta V \subset V.$$

Thus

$$(\alpha + \beta)V \subset V,\ (\alpha\beta)V \subset V.$$

Hence $\alpha + \beta$ and $\alpha\beta$ are algebraic. □

12.2 Algebraic integers

Definition 12.2. *A number $\alpha \in \mathbb{C}$ is said to be an* algebraic integer *if it satisfies a monic polynomial equation*

$$f(x) = x^n + a_1 x^{n-1} + \cdots + a_n = 0$$

with integral coefficients $a_i \in \mathbb{Z}$. We denote the set of algebraic integers by $\bar{\mathbb{Z}}$.

Theorem 12.2. *The algebraic integers form a ring $\bar{\mathbb{Z}}$ with*

$$\mathbb{Z} \subset \bar{\mathbb{Z}} \subset \bar{\mathbb{Q}}.$$

Proof. Evidently

$$\mathbb{Z} \subset \bar{\mathbb{Z}},$$

since $n \in \mathbb{Z}$ satisfies the equation

$$x - n = 0.$$

We have to show that

$$\alpha, \beta \in \bar{\mathbb{Z}} \implies \alpha + \beta, \alpha\beta \in \bar{\mathbb{Z}}.$$

Lemma 12.2. *Suppose $S \subset \mathbb{C}$ is a finitely-generated abelian group, with $S \neq 0$; and suppose $x \in \mathbb{C}$. If*

$$xS \subset S$$

then $x \in \bar{\mathbb{Z}}$.

Proof. Let $s_1, \ldots, s_n$ generate S. Suppose

$$\begin{aligned} xs_1 &= a_{11}s_1 + \cdots a_{1n}s_n \\ xs_2 &= a_{21}s_1 + \cdots a_{2n}s_n \\ &\cdots \\ xs_n &= a_{n1}s_1 + \cdots a_{nn}s_n. \end{aligned}$$

Then

$$\det(xI - A) = 0.$$

This is a monic equation with coefficients in $\mathbb{Z}$. Hence $x \in \bar{\mathbb{Z}}$. □

Consider the abelian group

$$S = \langle \alpha^i \beta^j : 0 \le i < m,\ 0 \le j < n \rangle$$

generated by the mn elements $\alpha^i \beta^j$. Evidently

$$\alpha S \subset S,\ \beta S \subset S.$$

Thus

$$(\alpha + \beta)S \subset S,\ (\alpha\beta)S \subset S.$$

Hence $\alpha + \beta$ and $\alpha\beta$ are algebraic integers. □

Proposition 12.1. *A rational number $c \in \mathbb{Q}$ is an algebraic integer if and only if it is a rational integer:*

$$\bar{\mathbb{Z}} \cap \mathbb{Q} = \mathbb{Z}.$$

Proof. Suppose $c = m/n$, where $\gcd(m, n) = 1$; and suppose c satisfies the equation

$$x^d + a_1 x^{d-1} + \cdots + a_d = 0 \quad (a_i \in \mathbb{Z}).$$

Then

$$m^d + a_1 m^{d-1} n + \cdots + a_d n^d = 0.$$

Since n divides every term after the first, it follows that $n \mid m^d$. But that is incompatible with $\gcd(m, n) = 1$, unless $n = 1$, ie $c \in \mathbb{Z}$. □

12.3 Number fields and number rings

Suppose $F \subset \mathbb{C}$ is a field. Then $1 \in F$, by definition, and so

$$\mathbb{Q} \subset F \subset \mathbb{C}.$$

We can consider F as a vector space over $\mathbb{Q}$.

Definition 12.3. *An* algebraic number field *(or simply* number field *is a subfield $F \subset \mathbb{C}$ which is a finite-dimensional vector space over $\mathbb{Q}$. The* degree *of F is the dimension of this vector space:*

$$\deg F = \dim_{\mathbb{Q}} F.$$

Proposition 12.2. *The elements of a number field F are algebraic numbers:*

$$\mathbb{Q} \subset F \subset \bar{\mathbb{Q}}.$$

Proof. Suppose $\deg F = d$; and suppose $\alpha \in F$. Then the $d+1$ numbers

$$1, \alpha, \alpha^2, \ldots, \alpha^d$$

are linearly dependent over $\mathbb{Q}$, say

$$a_0 + a_1\alpha + a_2\alpha^2 + \cdots + a_d\alpha^d = 0.$$

Thus

$$f(\alpha) = 0,$$

where $f(x)$ is the polynomial

$$f(x) = a_0 + a_1 x + a_2 x^2 + \cdots + a_d x^d \in \mathbb{Q}[x].$$

□

Definition 12.4. *The algebraic integers in a number field F are said to form an* algebraic number ring *(or simply* number ring*).*

Thus the number ring associated to the number field F is

$$F \cap \bar{\mathbb{Z}}.$$

Proposition 12.3. *The number ring associated to the field of gaussian numbers is the ring Γ of gaussian integers.*

Proof. Suppose

$$z = x + iy \quad (x, y \in \mathbb{Q})$$

is a gaussian number. We have to show that z is an algebraic integer if and only if $x, y \in \mathbb{Z}$.

If $m, n \in \mathbb{Z}$ then $m + in \in \bar{\mathbb{Z}}$, since $m, n, i \in \bar{\mathbb{Z}}$ and $\bar{\mathbb{Z}}$ is a ring.

Conversely, suppose

$$z = x + iy \in \bar{\mathbb{Z}}.$$

Then

$$\bar{z} = x - iy \in \bar{\mathbb{Z}}$$

since z and $\bar{z}$ satisfy the same polynomials over $\mathbb{Q}$. Hence

$$z + \bar{z} = 2x \in \bar{\mathbb{Z}} \cap \mathbb{Q} = \mathbb{Z}.$$

Similarly

$$-iz = y - ix \in \bar{\mathbb{Z}} \implies 2y \in \mathbb{Z}.$$

Thus

$$z = \frac{m + in}{2},$$

with $m, n \in \mathbb{Z}$.

But now

$$\mathcal{N}(z) = z\bar{z} \in \bar{\mathbb{Z}} \cap \mathbb{Q} = \mathbb{Z},$$

ie

$$x^2 + y^2 = \frac{m^2 + n^2}{4} \in \mathbb{Z},$$

ie

$$m^2 + n^2 \equiv 0 \bmod 4.$$

But $m^2, n^2 \equiv 0$ or $1 \bmod 4$. So

$$\begin{aligned} m^2 + n^2 \equiv 0 \bmod 4 &\implies 2 \mid m, n \\ &\implies z \in \Gamma. \end{aligned}$$

□

Example: $\sqrt{2}$ is an algebraic integer, since it satisfies the equation

$$x^2 - 2 = 0.$$

But $\sqrt{2}/2$ is not an algebraic integer. For if it were,

$$(\sqrt{2}/2)^2 = 1/2$$

would be an algbraic integer (since $\bar{\mathbb{Z}}$ is a ring), which we have just seen is not so.

Algebraic number theory is the study of number rings. The first question one might ask is whether a given number ring is a Unique Factorisation Domain.

We have seen that the number rings Z and Γ are. But in general number rings are not UFDs.

The foundation of algebraic number theory was Dedekind's amazing discovery that unique factorisation could be recovered if one added what Dedekind called 'ideal numbers', and what are today called 'ideals'.

However, we are not going into that theory. We shall only be looking at a small number of quadratic number rings which are UFDs.

12.4 Integral closure

Recall that any integral domain A can be extended to its *field of fractions*, which we shall denote by $Q(A)$, since we follows exactly the same process as in creating the field of rational numbers $\mathbb{Q}$ from the ring of integers $\mathbb{Z}$. We define $Q(A)$ to be the quotient set X/E, where X is the set of pairs (n, d), with $n, d \in A$ and $d \neq 0$, and E is the equivalence relation

$$(n, d) \sim (n', d') \iff nd' = n'd.$$

We write n/d for the the element of $Q(A)$ represented by the the pair (n, d).

We define addition, multiplication and inversion in $Q(A)$ in the obvious way, and it is a trivial matter to verify that these satisfy the axioms for a field. Identifying $a \in A$ with $a/1 \in Q(A)$ allows us to identify A with a subset of $Q(A)$, so we can regard $Q(A)$ as an extension of A.

As an example of the construction we have $k[x] \to k(x)$, where $k(x)$ is the field of rational functions $f(x)/g(x)$, with $f(x), g(x) \in k[x]$.

If A is already a subring of a field F then we can identify $Q(A)$ with the subfield of F formed by the elements a/d with $a, d \in A$. So for example the field of algebraic numbers is the quotient-field of the ring of algebraic integers: $\bar{\mathbb{Q}} = Q(\bar{Z})$.