# Chapter 12

# Algebraic numbers and algebraic integers

## 12.1 Algebraic numbers

**Definition 12.1.** *A complex number $\alpha$ 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 $\pi$ 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 $\pi^e$ is transcendental.

**Proposition 12.1.** *$\alpha \in \mathbb{C}$ is an algebraic number if and only if there exists a finite-dimensional vector space $V \subset \mathbb{C}$ over $\mathbb{Q}$ such that*

$$\alpha V \subset V.$$

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

$$\begin{aligned} \alpha e_1 &= a_{11} e_1 + \cdots a_{1n} e_n \\ \alpha e_2 &= a_{21} e_1 + \cdots a_{2n} e_n \\ &\cdots \\ \alpha e_n &= a_{n1} e_1 + \cdots a_{nn} e_n, \end{aligned}$$

Where $a_{ij} in \mathbb{Q}$. Thus $\alpha$ satisfies the polynomial equation

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

where

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

Hence $\alpha \in \bar{\mathbb{Q}}$.

(This argument is sometimes known as 'the determinantal trick'. We shall be using it again shortly. There is an alternative way of establishing the result. If $\alpha V \subset V$ then we can think of $\alpha^i$ as a linear map

$$v \mapsto \alpha^i v : V \to V.$$

But if $\dim V = n$ then it is easy to see that $\dim \hom(V, V) = n^2$, since we can represent the linear maps $V \to V$ by $n \times n$ matrices. It follows that the $n^2 + 1$ linear maps $1, \alpha, \ldots, \alpha^{m^2}$ must be linearly dependent, showing that $\alpha$ satisfies a polynomial equation of degree $n^2$ or less.)

Conversely, suppose $\alpha$ satisfies the polynomial equation

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

where $a_i \in \mathbb{Q}$. Let $V$ be the vector space over $\mathbb{Q}$ generated by $1, \alpha, \ldots, \alpha^{n-1}$:

$$V = \langle 1, \alpha, \ldots, \alpha^{n-1} \rangle.$$

Then $\alpha V \subset V$. □

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

*Proof.* Suppose $\alpha, \beta$ satisfy the polynomial equation

$$f(x) = x^m + a_{m-1} x^{m-1} + \cdots + a_0 = 0,\ g(x) = x^n + b_{n-1} x^{n-1} + \cdots + b_0 = 0$$

with $a_i, b_j \in \mathbb{Q}$. Let $V, W$ be the vector spaces

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

over $\mathbb{Q}$. Then

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

Consider the vector space $VW$ over $\mathbb{Q}$ spanned by the $mn$ elements $\alpha^i\beta^j$:

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

Evidently

$$\alpha VW \subset VW,\ \beta VW \subset VW.$$

Hence

$$(\alpha+\beta)VW \subset VW,\ \alpha\beta VW \subset VW \implies \alpha+\beta,\ \alpha\beta \in \bar{\mathbb{Q}}.$$

Thus $\bar{\mathbb{Q}}$ is a ring.

(Note that each element of $VW$ is now necessarily of the form $vw$; it is a sum of such elements. This is similar to the definition of the tensor product $V \otimes_{\mathbb{Q}} V$, an element of which is not necessarily of the form $v \otimes w$, but is a sum of such elements. In fact there is a natural linear map $V \otimes W \to VW$; VW is a quotient-space of $V \otimes W$. Nb $VW$ can only be defined in this way because $V$ and $W$ are vector subspaces of $\mathbb{C}$.)

To see that $\bar{\mathbb{Q}}$ is a field, suppose $\alpha$ satisfies the equation

$$f(x) = x^n + a_1x^{n-1} + \cdots + a_n = 0.$$

Then $1/\alpha$ satisfies the polynomial equation

$$x^n f(1/x) = 0.$$

Thus

$$\alpha \in \bar{\mathbb{Q}} \implies 1/\alpha \in \bar{\mathbb{Q}}.$$

□

**Proposition 12.2.** *The field $\bar{\mathbb{Q}}$ is alebraically closed, ie if $\alpha \in \mathbb{C}$ satisfies*

$$f(x) = x^n + a_1x^{n-1} + \cdots + a_n = 0,$$

*where the coefficients satisfy $a_i \in \bar{\mathbb{Q}}$. Then $\alpha \in \bar{\mathbb{Q}}$.*

*Proof.* Suppose

$$a_iV_i \subset V_i$$

for $0 \le i \le n$. Let

$$U = \langle 1, \alpha, \ldots, \alpha^{n-1}\rangle V_1V_2\cdots V_n.$$

Then

$$\alpha U \subset U \implies \alpha \in \bar{\mathbb{Q}}.$$

□

## 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 $\bar{\mathbb{Z}}$.*

**Proposition 12.3.** *$\alpha \in \mathbb{C}$ is an algebraic integer if and only if there exists a finitely-generated abelian group $A \subset \mathbb{C}$ such that*

$$\alpha A \subset A.$$

(We shall see that the arguments we give in this Section are very similar to those in the last Section, except that finite-dimensional vector spaces are replaced by finitely-generated abelian groups.)

*Proof.* Let $a_1, \ldots, a_r$ generate $A$. $A$ is torsion-free, ie

$$na = 0 \implies n = 0 \text{ or } a = 0,$$

since that is true in $\mathbb{C}$.

**Lemma 12.1.** *A torsion-free finitely-generated abelian group $A$ has an integral basis $z_1, \ldots, z_n$, ie each $a \in A$ is uniquely expressible in the form*

$$a = \lambda_1 z_1 + \cdots + \lambda_n z_n,$$

*with $\lambda_i \in \mathbb{Z}$. In other words, $A = \mathbb{Z}^n$.*

*Proof.* Let $V = A \otimes_Z \mathbb{Q}$. In simpler terms (it is not really necessary to bring torsion products into it), $V$ is derived from $A$ by 'extending the scalars' from $\mathbb{Z}$ to $\mathbb{Q}$. Thus each $v \in V$ is expressible in the form

$$v = \lambda a,$$

with $\lambda \in \mathbb{Q},\ a \in A$. (Even simpler,

$$v = \frac{1}{n} a,$$

with $n \in \mathbb{N},\ n \neq 0$.) It is easy to see how addition of these elements and scalar multiplication by elements of $\mathbb{Q}$ is defined, and that $A \subset V$.

Let $e_1, \dots e_n$ be a basis for the vector space $V$. Thus each $a \in A$ is uniquely expressible in the form

$$a = \lambda_1 e_1 + \cdots + \lambda_n e_n,$$

with $\lambda_i \in \mathbb{Q}$.

Consider the coefficient $\lambda_{ij}$ of the basis element $e_i$ in the generator $a_j$ Suppose these $nr$ rationals are $\frac{a_{ij}}{d_{ij}}$. Let

$$d = \operatorname{lcm}\{d_{ij} : 1 \leq i \leq n,\ 1 \leq j \leq r\}.$$

Then since each $a \in A$ is a linear combination with integer coefficients of $a_1, \dots, a_r$, it follows that $a$ is expressible in the form

$$a = \frac{c_1}{d} f_1 + \cdots + \frac{c_n}{d} f_n,$$

with $c_i \in \mathbb{Z}$. (We don't claim these fractions are in their lowest terms.)

Now consider the $c$'s associated with a particular basis element, say $e_1$. It is easy the see that

$$I = \{c_1 : a = \frac{c_1}{d} e_1 + \cdots\}$$

is an ideal in $\mathbb{Z}$. But $\mathbb{Z}$ is a principal ideal domain (PID), ie all ideals in $\mathbb{Z}$ are of the form $(m) = \{nm : n \in \mathbb{Z}\}$. Let $I = (n_1)$. (Recall that $n_1$ is the smallest positive integer in $I$.)

Now if we set

$$z_i = \frac{n_i}{d} e_i,$$

we see that $z_1, \dots, z_n$ form an integral basis for $A$. □

Now suppose $\alpha \in \mathbb{Z}$. Then

$$\begin{aligned}
\alpha z_1 &= a_{11} z_1 + \cdots a_{1n} z_n \\
\alpha z_2 &= a_{21} z_1 + \cdots a_{2n} z_n \\
&\cdots \\
\alpha z_n &= a_{n1} z_1 + \cdots a_{nn} z_n,
\end{aligned}$$

Where $a_{ij} \in \mathbb{Z}$. Thus $\alpha$ satisfies the polynomial equation

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

where

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

Hence $\alpha \in \bar{\mathbb{Z}}$.

Conversely, suppose $\alpha$ satisfies the polynomial equation

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

where $a_i \in \mathbb{Z}$. Let $A$ be the abelian group generated by $1, \alpha, \ldots, \alpha^{n-1}$:

$$A = \langle 1, \alpha, \ldots, \alpha^{n-1} \rangle.$$

Then $\alpha A \subset A$. ☐

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

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

*Proof.* Suppose $\alpha, \beta$ satisfy the polynomial equations

$$f(x) = x^m + a_{m-1}x^{m-1} + \cdots + a_0 = 0,\ g(x) = x^n + b_{n-1}x^{n-1} + \cdots + b_0 = 0$$

with $a_i, b_j \in \mathbb{Z}$. Let $A, B$ be the abelian groups

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

over $\mathbb{Q}$. Then

$$\alpha A \subset A,\ \beta B \subset B.$$

Consider the abelian group $AB$ over $\mathbb{Z}$ spanned by the $mn$ elements $\alpha^i \beta^j$:

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

Evidently

$$\alpha AB \subset AB,\ \beta AB \subset AB.$$

Hence

$$(\alpha + \beta)AB \subset AB,\ (\alpha\beta)AB \subset AB \implies \alpha + \beta,\ \alpha\beta \in \bar{\mathbb{Z}}.$$

Thus $\bar{\mathbb{Q}}$ is a ring.

Finally,

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

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

$$x - n = 0.$$

☐

**Proposition 12.4.** *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 $c \in \mathbb{Z}$. □

**Proposition 12.5.** *The ring $\bar{\mathbb{Z}}$ of algebraic integers is alebraically closed, ie if $\alpha \in \mathbb{C}$ satisfies*

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

*where the coefficients $a_i \in \bar{\mathbb{Z}}$. Then $\alpha \in \bar{\mathbb{Z}}$.*

*Proof.* Suppose

$$a_i Z_i \subset Z_i$$

for $0 \leq i \leq n$. Let

$$A = \langle 1, \alpha, \ldots, \alpha^{n-1} \rangle Z_1 Z_2 \cdots Z_n.$$

Then

$$\alpha A \subset A \implies \alpha \in \bar{\mathbb{Z}}.$$

□