6. Number Fields

So far we have mainly focused on the ring of integers $\mathbb{Z}$. But modern number theory is not only about integers. From this point on we will enlarge our vision and study the so-called algebraic integers.

6.1. Algebraic numbers and algebraic integers.

We first introduce the following terminologies, which will be convenient for our discussions:

Definition 6.1. An *algebraic number* is a complex number that is a root of a non-zero polynomial $f(x)$ with coefficients in $\mathbb{Q}$. An *algebraic integer* is a complex number that is a root of a non-zero monic (leading coefficient 1) polynomial $f(x)$ with coefficients in $\mathbb{Z}$.

Example 6.2. For example, $\sqrt{2}$ is an algebraic integer because it is a root of the polynomial $x^2 - 2$; $i = \sqrt{-1}$ is also an algebraic integer because it is a root of $x^2 + 1$; so is a fifth root of unity $\cos\frac{2\pi}{5} + i\sin\frac{2\pi}{5}$ because it is a root of $x^5 - 1$. They are also algebraic numbers.

Remark 6.3. We make the following remarks about this definition.

(1) It is clear that every $a \in \mathbb{Z}$ is an algebraic integer. To avoid any potential confusion, we sometimes call any element $a \in \mathbb{Z}$ a *rational integer* (especially when both notions appear in the same sentence).

(2) Clearly every algebraic integer is an algebraic number. But the converse is not true; see Exercise 6.1.

(3) There are complex numbers which are not algebraic numbers. They are usually called *transcendental* numbers. Typical examples include the ratio of the circumference and diameter of a circle $\pi = 3.14159\ldots$, and the base of the natural logarithm $e = 2.71828\ldots$. We will not explain why they are not algebraic, but it is a standard topic in transcendental number theory.

Example 6.4. A slightly more complicated example is $\sqrt{2} + \sqrt{3}i$. We show it is an algebraic integer by definition. Let $x = \sqrt{2} + \sqrt{3}i$. We rewrite it as $x - \sqrt{2} = \sqrt{3}i$ and square both sides to get $x^2 - 2\sqrt{2}x + 2 = -3$. We rewrite it as $x^2 + 5 = 2\sqrt{2}x$ and square both sides again to get $x^4 + 10x^2 + 25 = 8x^2$. Hence $x^4 + 2x^2 + 25$ is a monic polynomial in $\mathbb{Z}[x]$ for which $\sqrt{2} + \sqrt{3}i$ is a root.

We want to have a more straightforward way to understand the above example. Given two algebraic integers, we ask whether their sum and product are still algebraic integers. We will see the answer is yes. Before proving it we establish the following criterion:

Lemma 6.5. *Let $V = \{\gamma_1, \gamma_2, \cdots, \gamma_n\}$ be a finite set of non-zero complex numbers. Suppose a complex number α has the property that for each $i = 1, 2, \cdots, n$, the product $\alpha\gamma_i$ can be written as an integral linear combination of elements in the set V. Then α is an algebraic integer.*

Proof. By assumption, for each $i = 1, 2, \cdots, n$, we can write

$$\alpha\gamma_i = \sum_{j=1}^{n} a_{ij}\gamma_j,$$

where each $a_{ij} \in \mathbb{Z}$.

Using the language of linear algebra, we have

$$\alpha \cdot \mathbf{v} = \mathbf{M} \cdot \mathbf{v},$$

where

$$\mathbf{M} = \begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n1} & a_{n2} & \cdots & a_{nn} \end{pmatrix}, \quad \mathbf{v} = \begin{pmatrix} \gamma_1 \\ \gamma_2 \\ \vdots \\ \gamma_n \end{pmatrix}.$$

Since $\mathbf{v} \neq 0$, we see that α is an eigenvalue of the square matrix $\mathbf{M}$. In other words, α is a solution of the equation

$$\det(x \cdot \mathbf{I} - \mathbf{M}) = 0.$$

Since all entries of $\mathbf{M}$ are integers, it is clear that the left-hand side of the equation is a polynomial with integer coefficients, whose leading term is x^n. Therefore α is an algebraic integer, as desired. □

Now we can prove the following important result:

Proposition 6.6. *The sum and product of two algebraic integers are algebraic integers.*

Proof. Suppose α and β are algebraic integers. If either $\alpha = 0$ or $\beta = 0$, the statement is clear. From now on we assume $\alpha \neq 0$ and $\beta \neq 0$. We want to apply Lemma 6.5 to show that $\alpha + \beta$ and $\alpha\beta$ are also algebraic integers. Suppose α and β satisfy

$$\alpha^n + a_1\alpha^{n-1} + a_2\alpha^{n-2} + \cdots + a_{n-1}\alpha + a_n = 0$$
$$\beta^m + b_1\beta^{m-1} + b_2\beta^{m-2} + \cdots + b_{m-1}\beta + b_m = 0,$$

where each a_i and b_j are integers. Let

$$V = \left\{\alpha^i\beta^j \mid 0 \leqslant i < n, 0 \leqslant j < m\right\}.$$

For each element $\alpha^i\beta^j \in V$, we claim that $(\alpha+\beta)\cdot\alpha^i\beta^j$ and $\alpha\beta\cdot\alpha^i\beta^j$ can both be written as integral linear combinations of elements in V. Indeed, we have

$$(\alpha+\beta)\cdot\alpha^i\beta^j = \alpha^{i+1}\beta^j + \alpha^i\beta^{j+1} \tag{6.1}$$

$$\alpha\beta\cdot\alpha^i\beta^j = \alpha^{i+1}\beta^{j+1}. \tag{6.2}$$

If $0 \leqslant i \leqslant n-2$ and $0 \leqslant j \leqslant m-2$, then our claim is already true. Otherwise, if $i = n-1$ and/or $j = m-1$, we can replace α^n by $-(a_1\alpha^{n-1} + a_2\alpha^{n-2} + \cdots + a_{n-1}\alpha + a_n)$ and/or β^m by $-(b_1\beta^{m-1} + b_2\beta^{m-2} + \cdots + b_{m-1}\beta + b_m)$ in the right-hand sides of (6.1) and (6.2), then their expansions are still integral linear combinations of elements of V. Therefore our claim is true. By Lemma 6.5, we conclude that $\alpha+\beta$ and $\alpha\beta$ are both algebraic integers. □

Corollary 6.7. *The set of all algebraic integers forms a commutative ring with* 1*.*

Proof. We have to check that the addition, the additive inverse and the multiplication are all well-defined in the set of algebraic integers, and all algebraic laws required in the definition of a ring hold in this set.

Proposition 6.6 proved that the addition and the multiplication are both well-defined. The existence of additive inverse is given by Exercise 6.1. All algebraic laws related concerning the addition and the multiplication hold because they hold for complex numbers. Hence the set of algebraic integers forms a ring. □