8. Algebraic numbers: Introduction

A complex number ξ is called *algebraic* if it is a root of a polynomial over $\mathbb{Q}$ (equivalently, over $\mathbb{Z}$). Any complex number that is not algebraic is called *transcendental*.

Exercise 8.1 Show that there are only countably many polynomials over $\mathbb{Q}$ and deduce that the set of all algebraic (transcendental) numbers is countable (uncountable).

Lemma 8.1 *For an algebraic number ξ let $g(x) \in \mathbb{Q}[x]$ be a monic polynomial of smallest degree with $g(\xi) = 0$. Then $g(x)$ is irreducible over $\mathbb{Q}$ and every polynomial $f(x) \in \mathbb{Q}[x]$ such that $f(\xi) = 0$ is divisible by $g(x)$. In particular, $g(x)$ is unique.* □

The polynomial $g(x)$ from Lemma 8.1 is called the *minimal polynomial* of ξ, and the *degree* of ξ is defined to be the degree of $g(x)$.

Before proceeding any further we will need two results about polynomials with integer coefficients. A polynomial $f(x) \in \mathbb{Z}[x]$ is said to be *primitive* if the greatest common divisor of its coefficients is 1.

Lemma 8.2 *The product of two primitive polynomials is primitive.*

Proof. Let $g(x)$ and $h(x)$ be two primitive polynomials in $\mathbb{Z}[x]$. Suppose their product $f(x) = g(x)h(x)$ is not primitive and all its coefficients are divisible by a prime p. Let $\sigma\colon \mathbb{Z} \to \mathbb{Z}_p$ be the canonical homomorphism which is extended to a homomorphism from $\mathbb{Z}[x] \to \mathbb{Z}_p[x]$ in the natural fashion

$$\sigma(\sum_{0\le i\le n} a_i x^i) = \sum_{0\le i\le n} a_i^\sigma x^i.$$

(we denote the extension with the same letter). Then this extension is also a homomorphism. We have $\sigma(g(x)) \neq 0$ and $\sigma(h(x)) \neq 0$. At the same time $\sigma(g(x))\sigma(h(x)) = \sigma(f(x)) = 0$. This contradicts to the absence of zero divisors in $\mathbb{Z}_p[x]$. □

Lemma 8.3 (Gauss.) *Let $f(x) \in \mathbb{Z}[x]$ be a monic polynomial such that $f(x) = g(x)h(x)$ where $g(x), h(x) \in \mathbb{Q}[x]$. If both $g(x)$ and $h(x)$ are monic, then $g(x), h(x) \in \mathbb{Z}[x]$.*

Proof. Let $c, d \in \mathbb{N}$ be the least such that $cg(x), dh(x) \in \mathbb{Z}[x]$. Then $cg(x)$ and $dh(x)$ are primitive. By Lemma 8.2 their product $cdf(x)$ is primitive, and since $f(x) \in \mathbb{Z}[x]$ we have $c = d = 1$. □

Exercise 8.2 (Eisenstein's criterion) *Let $f(x)$ is a polynomial with integer coefficients and p be a prime number. Suppose that:*

1. *the leading coefficient of $f(x)$ is not divisible by p,*
2. *all other coefficients are divisible by p,*
3. *constant term of $f(x)$ is not divisible by p^2.*

Prove that $f(x)$ is irreducible over $\mathbb{Q}$.

Central concept: An algebraic number ξ is called an *algebraic integer* if it is a root of a *monic* polynomial with *integer* coefficients.

Proposition 8.4 *The minimal polynomial of an algebraic integer has integer coefficients.* □

Lemma 8.5 *In $\mathbb{Q}$, the only algebraic integers are the integers $0, \pm 1, \pm 2, \ldots$* □

In algebraic number theory, the integers $0, \pm 1, \pm 2, \ldots$ are often called *rational integers* to distinguish them from the other algebraic integers (such as $\sqrt{2}$) that are not rational.

Theorem 8.6 (Liouville, 1851) *The number* $\beta = \sum_{j \geq 1} 10^{-j!}$ *is transcendental.*

Proof. Suppose that $f(\beta) = 0$ for some $f(x) = \sum_{0 \leq j \leq n} c_j x^j \in \mathbb{Z}[x]$. For any $x \in (0,1)$ we have $|f'(x)| < \sum_{1 \leq j \leq n} |jc_j| = C$. Letting $\beta_k = \sum_{1 \leq j \leq k} 10^{-j!}$, we have $\beta - \beta_k = \sum_{j \geq k+1} 10^{-j!} < 2 \cdot 10^{-(k+1)!}$. By the mean value theorem, for some θ_k between β and β_k we have $|f(\beta) - f(\beta_k)| = |f'(\theta_k)| \cdot |\beta - \beta_k| < 2C/10^{(k+1)!}$. Using $f(\beta) = 0$ and $f(\beta_k) \neq 0$ for large k we obtain $|f(\beta) - f(\beta_k)| = |\sum_{0 \leq j \leq n} c_j \beta_k^j| \geq 1/10^{n \cdot k!}$. Comparing the last two bounds gives a contradiction for large k. $\square$

Historical comment. In 1873 Hermite proved that the base of the natural logarithms $e = 2.718218\ldots$ is transcendental. In 1882 Lindemann proved Euler's conjecture (1755) that π is transcendental. One of the most beautiful theorems was proved in 1934 independently by A.O. Gelfond and T. Schneider. They proved that if a is any algebraic number, different from 0 or 1, and b is any irrational number, then the number a^b is transcendental. For example, $2^{\sqrt{2}}$ is transcendental. It is not known though that $e + \pi$ is even irrational!