Algebraic number theory

Hugo Trebše (hugo.trebse@gmail.com)

October 26, 2024

Contents

1 Algebraic numbers and integers

Claim 1.1

$\overline{\mathbb{Z}}$ and $\overline{\mathbb{Q}}$ respectively denote the ring of algebraic integers, and the field of algebraic numbers. Elements of both are roots of polynomials with rational coefficients, but they differ in their minimal polynomials (which are by requirement monic).

Proof outline. Since

$$\mathbb{Z}[\alpha] = \langle 1, \alpha, \alpha^2, \ldots, \alpha^{n-1} \rangle_{\mathbb{Z}} \quad \text{and} \quad \mathbb{Z}[\beta] = \langle 1, \beta, \beta^2, \ldots, \beta^{k-1} \rangle_{\mathbb{Z}}$$

it follows that

$$\mathbb{Z}[\alpha, \beta] = \langle \alpha^i \cdot \beta^j \mid 0 \leq i \leq n-1,\ 0 \leq j \leq k-1 \rangle_{\mathbb{Z}}.$$

Since both $\alpha + \beta$ and $\alpha \cdot \beta$ are contained in $\mathbb{Z}[\alpha, \beta]$, they must be algebraic, otherwise $\langle \alpha+\beta \rangle_{\mathbb{Z}}$ and $\langle \alpha \cdot \beta \rangle_{\mathbb{Z}}$ would be infinite-dimensional subspaces of a finite-dimensional vector space $\mathbb{Z}[\alpha, \beta]$. □

By the rational root theorem it follows that $\overline{\mathbb{Z}} \cap \mathbb{Q} = \mathbb{Z}$

Definition 1.2

The conjugates of $\alpha \in \overline{\mathbb{Q}}$ are the roots of the minimal polynomial of α (including α).

Theorem 1.3: Kronecker's theorem

Let $\alpha \in \overline{\mathbb{Z}}$. If all conjugates of α have absolute value 1, then α is a root of unity.

Proof. Set $\alpha = \alpha_1$ and denote the algebraic conjugates of α as $\alpha_2, \ldots, \alpha_n$.

Observe the polynomial

$$p_k(X) = \prod_{i=1}^{n} (X - \alpha_i^k).$$

The coefficients of p_k are symmetric polynomials over $\mathbb{Z}$ in $\alpha_1^k, \alpha_2^k, \ldots, \alpha_n^k$ and hence symmetric polynomials in $\alpha_1, \alpha_2, \ldots, \alpha_n$. By the fundamental theorem of symmetric polynomials, the coefficients of p_k can be expressed as a polynomial over $\mathbb{Z}$ in the elementary symmetric polynomials of variables $\alpha_1, \alpha_2, \ldots, \alpha_n$. However, by the Vieta formulas on the minimal polynomial of α, we may conclude that the elementary symmetric polynomials in variables $\alpha_1, \alpha_2, \ldots, \alpha_n$ evaluate to rationals. It hence follows that the coefficients of p_k must be rational. But since the coefficients of p_k are also algebraic integers it follows that $p_k \in \mathbb{Z}[X]$

The m-th coefficient of p_k is, however, bounded from above by $\binom{n}{m}$ by the triangle inequality and the assumption that the α_i have absolute value at most 1. It hence follows that there are only finitely many distinct polynomials in the sequence $\{p_i\}_{i \in \mathbb{N}}$. It follows that there exists an infinite set of positive integers S, such that for all $a, b \in S$: $p_a = p_b$

By the definition of p_j it follows that $\{\alpha_1^a, \alpha_2^a, \ldots, \alpha_n^a\}$ is a permutation of $\{\alpha_1^b, \alpha_2^b, \ldots, \alpha_n^b\}$. As S is infinite, it must be that for some distinct $c, d \in S$:

$$(\alpha_1^c, \alpha_2^c, \ldots, \alpha_n^c) = (\alpha_1^d, \alpha_2^d, \ldots, \alpha_n^d)$$

which proves that all α_i are roots of unity. □

A much cleaner proof is available by using some linear algebra, but this classical proof uses properties symmetric polynomials, which are dear to me.

2 Quadratic integers

Definition 2.1

An integer (number) is quadratic, if it is an algebraic integer (number) of degree 2. For a quadratic number α, we define the *ring of integers* of $K = \mathbb{Q}(\alpha)$ as

$$\mathcal{O}_K = \mathbb{Q}(\alpha) \cap \overline{\mathbb{Z}}.$$

By a quick application of the quadratic formula and some modular analysis we see that:

Claim 2.2

For a squarefree rational integer d:

$$\mathcal{O}_{\mathbb{Q}(\sqrt{d})} = \begin{cases} \mathbb{Z}[\sqrt{d}]; \text{ if } d \not\equiv 1 \pmod 4 \\ \mathbb{Z}\left[\dfrac{1+\sqrt{d}}{2}\right]; \text{ if } d \equiv 1 \pmod 4 \end{cases}$$

From now on, we will denote the conjugate of a quadratic integer $\alpha = b + c\sqrt{d}$, as $\overline{\alpha} = b - c\sqrt{d}$. Like complex conjugation, conjugation is additive and multiplicative.

As a precursor to the general definition of the norm, we define the following:

Definition 2.3

Let $d \neq 1$ be a squarefree rational integer. We define the following multiplicative function $N_{\mathbb{Q}(\sqrt{d})} : \mathbb{Q}(\sqrt{d}) \to \mathbb{Q}$ as

$$N_{\mathbb{Q}(\sqrt{d})}(\alpha) = \alpha \cdot \overline{\alpha}.$$

We define a unit of a quadratic field as one should, and note that u is an unit $\iff$ the absolute value of its norm is 1.

3 Analytic number theory

Theorem 3.1

Let $\pi(x)$ be the number of primes less than $x \in \mathbb{R}$. Then

$$\lim_{x\to\infty} \frac{\pi(x)}{\left(\frac{x}{\log(x)}\right)}.$$

This, in particular, implies, that for every $\varepsilon > 0$, there exists $n_0 \in \mathbb{N}$, such that for all $n > n_0$, there exists a prime p satisfying:

$$n < p < (1+\varepsilon)n$$

Theorem 3.2: Nagura

For every $n > 25$, there exists a prime p satisfying:

$$n < p < \frac{6}{5}n$$