Chapter I

Algebraic Integers

§ 1. The Gaussian Integers

The equations

$$2 = 1+1,\ 5 = 1+4,\ 13 = 4+9,\ 17 = 1+16,\ 29 = 4+25,\ 37 = 1+36$$

show the first prime numbers that can be represented as a sum of two squares. Except for 2, they are all $\equiv 1 \bmod 4$, and it is true in general that any odd prime number of the form $p = a^2 + b^2$ satisfies $p \equiv 1 \bmod 4$, because perfect squares are $\equiv 0$ or $\equiv 1 \bmod 4$. This is obvious. What is not obvious is the remarkable fact that the converse also holds:

(1.1) Theorem. *For all prime numbers $p \neq 2$, one has:*

$$p = a^2 + b^2 \quad (a, b \in \mathbb{Z}) \quad \Longleftrightarrow \quad p \equiv 1 \bmod 4.$$

The natural explanation of this arithmetic law concerning the ring $\mathbb{Z}$ of rational integers is found in the larger domain of the **gaussian integers**

$$\mathbb{Z}[i] = \left\{ a + bi \;\middle|\; a, b \in \mathbb{Z} \right\}, \quad i = \sqrt{-1}.$$

In this ring, the equation $p = x^2 + y^2$ turns into the product decomposition

$$p = (x + iy)(x - iy),$$

so that the problem is now when and how a prime number $p \in \mathbb{Z}$ factors in $\mathbb{Z}[i]$. The answer to this question is based on the following result about unique factorization in $\mathbb{Z}[i]$.

(1.2) Proposition. *The ring $\mathbb{Z}[i]$ is euclidean, therefore in particular factorial.*

Proof: We show that $\mathbb{Z}[i]$ is euclidean with respect to the function $\mathbb{Z}[i] \to \mathbb{N} \cup \{0\}$, $\alpha \mapsto |\alpha|^2$. So, for $\alpha, \beta \in \mathbb{Z}[i]$, $\beta \neq 0$, one has to verify the existence of gaussian integers γ, ρ such that

$$\alpha = \gamma\beta + \rho \quad \text{and} \quad |\rho|^2 < |\beta|^2.$$

It clearly suffices to find $\gamma \in \mathbb{Z}[i]$ such that $\left|\frac{\alpha}{\beta} - \gamma\right| < 1$. Now, the

gaussian integers form a **lattice** in the complex plane $\mathbb{C}$ (the points with integer coordinates with respect to the basis $1, i$). The complex number $\frac{\alpha}{\beta}$ lies in some mesh of the lattice and its distance from the nearest lattice point is not greater than half the length of the diagonal of the mesh, i.e. $\frac{1}{2}\sqrt{2}$. Therefore there exists an element $\gamma \in \mathbb{Z}[i]$ with $\left|\frac{\alpha}{\beta} - \gamma\right| \leq \frac{1}{2}\sqrt{2} < 1$. □

Based on this result about the ring $\mathbb{Z}[i]$, theorem (1.1) now follows like this: it is sufficient to show that a prime number $p \equiv 1 \bmod 4$ of $\mathbb{Z}$ does not remain a prime element in the ring $\mathbb{Z}[i]$. Indeed, if this is proved, then there exists a decomposition

$$p = \alpha \cdot \beta$$

into two non-units α, β of $\mathbb{Z}[i]$. The **norm** of $z = x + iy$ is defined by

$$N(x + iy) = (x + iy)(x - iy) = x^2 + y^2,$$

i.e., by $N(z) = |z|^2$. It is multiplicative, so that one has

$$p^2 = N(\alpha) \cdot N(\beta).$$

Since α and β are not units, it follows that $N(\alpha), N(\beta) \neq 1$ (see exercise 1), and therefore $p = N(\alpha) = a^2 + b^2$, where we put $\alpha = a + bi$.

Finally, in order to prove that a rational prime of the form $p = 1 + 4n$ cannot be a prime element in $\mathbb{Z}[i]$, we note that the congruence

$$-1 \equiv x^2 \bmod p$$

admits a solution, namely $x = (2n)!$. Indeed, since $-1 \equiv (p-1)! \bmod p$ by Wilson's theorem, one has

$$\begin{aligned} -1 \equiv (p-1)! &= \big[1 \cdot 2 \cdots (2n)\big]\big[(p-1)(p-2)\cdots(p-2n)\big] \\ &\equiv \big[(2n)!\big]\big[(-1)^{2n}(2n)!\big] = \big[(2n)!\big]^2 \bmod p. \end{aligned}$$

Thus we have $p \mid x^2 + 1 = (x + i)(x - i)$. But since $\frac{x}{p} \pm \frac{i}{p} \notin \mathbb{Z}[i]$, p does not divide any of the factors $x + i$, $x - i$, and is therefore not a prime element in the factorial ring $\mathbb{Z}[i]$.

The example of the equation $p = x^2 + y^2$ shows that even quite elementary questions about rational integers may lead to the consideration of higher domains of integers. But it was not so much for this equation that we have introduced the ring $\mathbb{Z}[i]$, but rather in order to preface the general theory of algebraic integers with a concrete example. For the same reason we will now look at this ring a bit more closely.

When developing the theory of divisibility for a ring, two basic problems are most prominent: on the one hand, to determine the **units** of the ring in question, on the other, its **prime elements**. The answer to the first question in the present case is particularly easy. A number $\alpha = a + bi \in \mathbb{Z}[i]$ is a unit if and only if its norm is 1:

$$N(\alpha) := (a + ib)(a - ib) = a^2 + b^2 = 1$$

(exercise 1), i.e., if either $a^2 = 1$, $b^2 = 0$, or $a^2 = 0$, $b^2 = 1$. We thus obtain the

(1.3) Proposition. *The group of units of the ring $\mathbb{Z}[i]$ consists of the fourth roots of unity,*

$$\mathbb{Z}[i]^* = \{1, -1, i, -i\}.$$

In order to answer the question for primes, i.e., irreducible elements of the ring $\mathbb{Z}[i]$, we first recall that two elements α, β in a ring are called **associated**, symbolically $\alpha \sim \beta$, if they differ only by a unit factor, and that every element associated to an irreducible element π is also irreducible. Using theorem (1.1) we obtain the following precise list of all prime numbers of $\mathbb{Z}[i]$.

(1.4) Theorem. *The prime elements π of $\mathbb{Z}[i]$, up to associated elements, are given as follows.*

(1) $\pi = 1 + i$,

(2) $\pi = a + bi$ *with* $a^2 + b^2 = p$, $p \equiv 1 \bmod 4$, $a > |b| > 0$,

(3) $\pi = p$, $p \equiv 3 \bmod 4$.

Here, p denotes a prime number of $\mathbb{Z}$.

Proof: Numbers as in (1) or (2) are prime because a decomposition $\pi = \alpha \cdot \beta$ in $\mathbb{Z}[i]$ implies an equation

$$p = N(\pi) = N(\alpha) \cdot N(\beta),$$

with some prime number p. Hence either $N(\alpha) = 1$ or $N(\beta) = 1$, so that either α or β is a unit.

Numbers $\pi = p$, where $p \equiv 3 \bmod 4$, are prime in $\mathbb{Z}[i]$, because a decomposition $p = \alpha \cdot \beta$ into non-units α, β would imply that $p^2 = N(\alpha) \cdot N(\beta)$, so that $p = N(\alpha) = N(a + bi) = a^2 + b^2$, which according to (1.1) would yield $p \equiv 1 \bmod 4$.

This being said, we have to check that an arbitrary prime element π of $\mathbb{Z}[i]$ is associated to one of those listed. First of all, the decomposition

$$N(\pi) = \pi \cdot \bar{\pi} = p_1 \cdots p_r ,$$

with rational primes p_i, shows that $\pi \mid p$ for some $p = p_i$. This gives $N(\pi) \mid N(p) = p^2$, so that either $N(\pi) = p$ or $N(\pi) = p^2$. In the case $N(\pi) = p$ we get $\pi = a + bi$ with $a^2 + b^2 = p$, so π is of type (2) or, if $p = 2$, it is associated to $1 + i$. On the other hand, if $N(\pi) = p^2$, then π is associated to p since p/π is an integer with norm one and thus a unit. Moreover, $p \equiv 3 \bmod 4$ has to hold in this case because otherwise we would have $p = 2$ or $p \equiv 1 \bmod 4$ and because of (1.1) $p = a^2 + b^2 = (a + bi)(a - bi)$ could not be prime. This completes the proof. □

The proposition also settles completely the question of how prime numbers $p \in \mathbb{Z}$ decompose in $\mathbb{Z}[i]$. The prime $2 = (1+i)(1-i)$ is associated to the square of the prime element $1+i$. Indeed, the identity $1-i = -i(1+i)$ shows that $2 \sim (1+i)^2$. The prime numbers $p \equiv 1 \bmod 4$ split into two conjugate prime factors

$$p = (a + bi)(a - bi) ,$$

and the prime numbers $p \equiv 3 \bmod 4$ remain prime in $\mathbb{Z}[i]$.

The gaussian integers play the same rôle in the field

$$\mathbb{Q}(i) = \{ a + bi \mid a, b \in \mathbb{Q} \}$$

as the rational integers do in the field $\mathbb{Q}$. So they should be viewed as the "integers" in $\mathbb{Q}(i)$. This notion of integrality is relative to the coordinates of the basis $1, i$. However, we also have the following characterization of the gaussian integers, which is independent of a choice of basis.

(1.5) Proposition. *$\mathbb{Z}[i]$ consists precisely of those elements of the extension field $\mathbb{Q}(i)$ of $\mathbb{Q}$ which satisfy a monic polynomial equation*

$$x^2 + ax + b = 0$$

with coefficients $a, b \in \mathbb{Z}$.

Proof: An element $\alpha = c + id \in \mathbb{Q}(i)$ is a zero of the polynomial

$$x^2 + ax + b \in \mathbb{Q}[x] \quad \text{with} \quad a = -2c,\ b = c^2 + d^2 .$$

If c and d are rational integers, then so are a and b. Conversely, if a and b are integers, then so are $2c$ and $2d$. From $(2c)^2 + (2d)^2 = 4b \equiv 0 \bmod 4$ it follows that $(2c)^2 \equiv (2d)^2 \equiv 0 \bmod 4$, since squares are always $\equiv 0$ or $\equiv 1$. Hence c and d are integers. □

The last proposition leads us to the general notion of an algebraic integer as being an element satisfying a monic polynomial equation with rational integer coefficients. For the domain of the gaussian integers we have obtained in this section a complete answer to the question of the units, the question of prime elements, and to the question of unique factorization.

These questions indicate already the fundamental problems in the general theory of algebraic integers. But the answers we found in the special case $\mathbb{Z}[i]$ are not typical. Novel features will present themselves instead.

Exercise 1. $\alpha \in \mathbb{Z}[i]$ is a unit if and only if $N(\alpha) = 1$.

Exercise 2. Show that, in the ring $\mathbb{Z}[i]$, the relation $\alpha\beta = \varepsilon\gamma^n$, for α, β relatively prime numbers and ε a unit, implies $\alpha = \varepsilon'\xi^n$ and $\beta = \varepsilon''\eta^n$, with ε', ε'' units.

Exercise 3. Show that the integer solutions of the equation

$$x^2 + y^2 = z^2$$

such that $x, y, z > 0$ and $(x, y, z) = 1$ ("pythagorean triples") are all given, up to possible permutation of x and y, by the formulæ

$$x = u^2 - v^2, \quad y = 2uv, \quad z = u^2 + v^2,$$

where $u, v \in \mathbb{Z}$, $u > v > 0$, $(u, v) = 1$, u, v not both odd.

Hint: Use exercise 2 to show that necessarily $x + iy = \varepsilon\alpha^2$ with a unit ε and with $\alpha = u + iv \in \mathbb{Z}[i]$.

Exercise 4. Show that the ring $\mathbb{Z}[i]$ cannot be ordered.

Exercise 5. Show that the only units of the ring $\mathbb{Z}[\sqrt{-d}] = \mathbb{Z} + \mathbb{Z}\sqrt{-d}$, for any rational integer $d > 1$, are ± 1.

Exercise 6. Show that the ring $\mathbb{Z}[\sqrt{d}] = \mathbb{Z} + \mathbb{Z}\sqrt{d}$, for any squarefree rational integer $d > 1$, has infinitely many units.

Exercise 7. Show that the ring $\mathbb{Z}[\sqrt{2}] = \mathbb{Z} + \mathbb{Z}\sqrt{2}$ is euclidean. Show furthermore that its units are given by $\pm(1 + \sqrt{2})^n$, $n \in \mathbb{Z}$, and determine its prime elements.

§ 2. Integrality

An **algebraic number field** is a finite field extension K of $\mathbb{Q}$. The elements of K are called **algebraic numbers**. An algebraic number is called **integral**, or an **algebraic integer**, if it is a zero of a monic polynomial $f(x) \in \mathbb{Z}[x]$. This notion of integrality applies not only to algebraic numbers, but occurs in many different contexts and therefore has to be treated in full generality.