Algebraic number theory

Olivier Haution

Technische Universität München

Summer semester 2022

Foreword

These are notes for a course given at the Technische Universität München in Summer 2022. The course is based on the book [**Sam70**] by Pierre Samuel. We follow this reference very closely in certain sections, but also diverge somewhat in other sections.

Formally the prerequisites for this course are rather minimal: mostly familiarity with rings, fields, modules, and basic linear algebra (say, over fields). We will occasionally use the tensor product of modules, but only in the simple case of free modules. Familiarity with localisation and Galois theory will be helpful, but not strictly required (at least until the last part of the course). Basic analysis will also be used (Fubini's Theorem, Lebesgue measure on $\mathbb{R}^n$).

Contents

Introduction

In this introduction we provide some motivation for the general theory that will be developed in this course. In particular, we will prove in this section the following result, attributed to Girard in 1625: if p is an odd prime number, then

$$p = a^2 + b^2 \text{ for some } a, b \in \mathbb{Z} \quad \Longleftrightarrow \quad p = 1 \mod 4.$$

This result is sometimes attributed instead to Fermat, and the first proof is due to Euler in 1749. We will present a proof due to Dedekind which appeared in 1894, whose main idea is to use the so-called Gaussian integers:

Definition 0.1. The ring of *Gaussian integers* $\mathbb{Z}[i]$ is the subring of $\mathbb{C}$ consisting of the elements of the form $a + bi$ with $a, b \in \mathbb{Z}$ (as usual $i \in \mathbb{C}$ denotes a chosen element such that $i^2 = -1$).

We define the *norm* function as the restriction of the map $\mathbb{C} \to \mathbb{N}, \alpha \mapsto |\alpha^2|$, namely:

$$\mathrm{N}\colon \mathbb{Z}[i] \to \mathbb{N}, \quad a + bi \mapsto a^2 + b^2.$$

Note that $\mathrm{N}(0) = 0$, $\mathrm{N}(1) = 1$, and that $\mathrm{N}(\alpha) \geq 1$ whenever $\alpha \neq 0$. Further, it is easy to verify that

$$\mathrm{N}(\alpha\beta) = \mathrm{N}(\alpha)\,\mathrm{N}(\beta) \quad \text{for any } \alpha, \beta \in \mathbb{Z}[i].$$

We recall that in a commutative ring R, an element is called a unit if it admits a multiplicative inverse. The set of units is a group, denoted by $R^\times$.

Lemma 0.2. *An element $\alpha \in \mathbb{Z}[i]$ is a unit if and only if $\mathrm{N}(\alpha) = 1$.*

Proof. Indeed, if $\alpha \in \mathbb{Z}[i]^\times$, we have

$$1 = \mathrm{N}(1) = \mathrm{N}(\alpha\alpha^{-1}) = \mathrm{N}(\alpha)\,\mathrm{N}(\alpha^{-1}),$$

hence we must have $\mathrm{N}(\alpha) = 1$. Conversely if $\mathrm{N}(\alpha) = 1$, write $\alpha = a + bi$ with $a, b \in \mathbb{Z}$. Then $\overline{\alpha} = a - bi$ satisfies

$$\alpha\overline{\alpha} = a^2 + b^2 = \mathrm{N}(\alpha) = 1,$$

and so $\overline{\alpha}$ is the inverse of α. □

Remark 0.3. In fact, it is easy to see that $\mathbb{Z}[i]^\times = \{1, -1, i, -i\}$.

Definition 0.4. A commutative (unital associative) ring A is called a *principal ideal domain* if every ideal of A is of the form aA for some $a \in A$.

Example 0.5. Prominent examples of principal ideal domains are $\mathbb{Z}$, and the polynomial ring $k[X]$ when k is a field.

Lemma 0.6. *Let $\alpha, \beta \in \mathbb{Z}[i]$, with $\beta \neq 0$. Then there exists elements $\gamma, \rho \in \mathbb{Z}[i]$ such that*

$$\alpha = \gamma\beta + \rho \quad \textit{and} \quad \mathrm{N}(\rho) < \mathrm{N}(\beta).$$

PROOF. Let us write $\alpha/\beta = x + iy \in \mathbb{C}$, with $x, y \in \mathbb{R}$. Then we may find $a, b \in \mathbb{Z}$ such that $|x - a| \leq 1/2$ and $|y - b| \leq 1/2$. Set $\gamma = a + bi \in \mathbb{Z}[i]$, and $\rho = \alpha - \beta\gamma$. Then

$$\mathrm{N}(\rho) = |\alpha - \beta\gamma|^2 = |\beta|^2 \cdot \left|\frac{\alpha}{\beta} - \gamma\right|^2 = |\beta|^2 \cdot ((x-a)^2 + (y-b)^2) \leq \frac{|\beta|^2}{2} < \mathrm{N}(\beta). \qquad \square$$

PROPOSITION 0.7. *The ring $\mathbb{Z}[i]$ is a principal ideal domain.*

PROOF. Let I be an ideal of $\mathbb{Z}[i]$. Let us pick a nonzero element $\beta \in A$ such that $\mathrm{N}(\beta) \in \mathbb{N} \smallsetminus \{0\}$ is minimal. Then for any $\alpha \in A$, by Lemma 0.6 we may write $\alpha = \gamma\beta + \rho$ with $\gamma, \rho \in \mathbb{Z}[i]$ and $\mathrm{N}(\rho) < \mathrm{N}(\beta)$. By minimality of $\mathrm{N}(\beta)$, we must have $\rho = 0$, and thus $\alpha = \gamma\beta$. We have proved that $I = \beta \cdot \mathbb{Z}[i]$. □

PROPOSITION 0.8 (Girard, Dedekind). *Let p be an odd prime number. Then the following conditions are equivalent:*

(i) p is congruent to 1 modulo 4,
(ii) -1 is a square in $\mathbb{Z}/p\mathbb{Z}$,
(iii) p is not irreducible in $\mathbb{Z}[i]$,
(iv) $p = a^2 + b^2$ for some $a, b \in \mathbb{Z}$.

PROOF. (i) ⇒ (ii) : The ring $\mathbb{Z}/p\mathbb{Z}$ is a finite field, and so its group of units $(\mathbb{Z}/p\mathbb{Z})^\times$ is cyclic (we will reprove this classical fact later) of order $p-1$. We thus have an isomorphism $(\mathbb{Z}/p\mathbb{Z})^\times \simeq \mathbb{Z}/(p-1)\mathbb{Z}$; the element $-1 \in (\mathbb{Z}/p\mathbb{Z})^\times$ corresponds to $(p-1)/2 \in \mathbb{Z}/(p-1)\mathbb{Z}$ (those are the unique elements of order 2). If p is congruent to 1 modulo 4, then $(p-1)/2$ is divisible by 2 in $\mathbb{Z}/(p-1)\mathbb{Z}$, which means that -1 is a square in $(\mathbb{Z}/p\mathbb{Z})^\times$.

(ii) ⇒ (iii) : If -1 is a square in $\mathbb{Z}/p\mathbb{Z}$, then we may find an integer $x \in \mathbb{Z}$ such that $p \mid x^2 + 1 = (x+i)(x-i)$. We now assume that p is irreducible in $\mathbb{Z}[i]$, and come to a contradiction. Let $I \subset \mathbb{Z}[i]$ be the ideal generated by p and $x + i$. As the ring $\mathbb{Z}[i]$ is a principal ideal domain (Lemma 0.7), we have $I = \alpha \cdot \mathbb{Z}[i]$ for some $\alpha \in \mathbb{Z}[i]$. Then α divides p in $\mathbb{Z}[i]$. As p is irreducible in $\mathbb{Z}[i]$, the element $\alpha \in \mathbb{Z}[i]$ is either a unit, or divisible by p. But p does not divide $x + i$ in $\mathbb{Z}[i]$ (an element of $\mathbb{Z}$ divides $a + bi$ in $\mathbb{Z}[i]$ if and only if it divides a and b; in our case $b = 1$), hence p does not divide α in $\mathbb{Z}[i]$. We deduce that α must be a unit in $\mathbb{Z}[i]$, and so $I = \mathbb{Z}[i]$. In particular we may find elements $\beta, \gamma \in \mathbb{Z}[i]$ such that

$$1 = p\beta + (x+i)\gamma \in \mathbb{Z}[i].$$

Multiplying with $x - i$ and using the relation $(x+i)(x-i) = p$ shows that $x - i$ is divisible by p in $\mathbb{Z}[i]$, a contradiction (this is the case $b = -1$ in the remark above).

(iii) ⇒ (iv) : Assume that $p = \alpha\beta$, where $\alpha, \beta \in \mathbb{Z}[i]$ are not units. Then

$$p^2 = \mathrm{N}(p) = \mathrm{N}(\alpha) \cdot \mathrm{N}(\beta) \in \mathbb{N}.$$

Since by Lemma 0.2 we have $\mathrm{N}(\alpha) \neq 1$ and $\mathrm{N}(\beta) \neq 1$, and as p is prime, we must have $p = \mathrm{N}(\alpha)$. Writing $\alpha = a + bi$ with $a, b \in \mathbb{Z}$, yields the required pair (a, b).

(iv) ⇒ (i) : Observe that for any $x \in \mathbb{Z}$, we have

$$x^2 = \begin{cases} 0 \mod 4 & \text{if } x = 0 \mod 2, \\ 1 \mod 4 & \text{if } x = 1 \mod 2. \end{cases}$$

Therefore for any $a, b \in \mathbb{Z}$, the integer $a^2 + b^2$ is congruent modulo 4 to $0, 1$ or 2. If $a^2 + b^2$ is an odd prime, the only possibility is 1 modulo 4. □

REMARK 0.9. Beside the norm function, the *trace* function

$$\mathrm{Tr}\colon \mathbb{Z}[i] \to \mathbb{Z}, \quad a + bi \mapsto 2a$$

can be useful. In particular, for any $\alpha \in \mathbb{Z}[i]$, we have

$$\alpha^2 - \alpha\,\mathrm{Tr}(\alpha) + \mathrm{N}(\alpha) = 0$$

(this may be verified using by a direct computation, writing $\alpha = a + bi$). Thus the elements of $\mathbb{Z}[i]$ are always the solutions of a monic polynomial equation with coefficients in $\mathbb{Z}$.

Bibliography

[Sam70] Pierre Samuel. *Algebraic theory of numbers*. Houghton Mifflin Co., Boston, Mass., 1970. Translated from the French by Allan J. Silberger.