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

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

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*

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

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

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

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

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

(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 $\mathbb{Z}$.

CHAPTER 1

Basic commutative ring theory

All rings will be assumed unital, associative and commutative. When R is a ring, we denote by $R^\times$ the multiplicative group consisting of the invertible elements of R. When A is a subring of B, we will sometimes say that $A \subset B$ is a ring extension.

1. Prime and maximal ideals

Recall that a nonzero ring A is called a *domain*, or integral domain, if for every $x, y \in A$ we have

$$xy = 0 \in A \quad \Longrightarrow \; x = 0 \text{ or } y = 0.$$

The *fraction field* K of a domain A is a field containing A, which is minimal (with respect to field inclusions) among such fields. Its elements are the fractions a/b for $a, b \in A$ with $b \neq 0$, subject to the relations $a/b = a'/b'$ whenever $ab' = a'b$. In particular every element of K is of the form ab^{-1} with $a, b \in A$.

Let A be a ring. We recall that an ideal $\mathfrak{p}$ of A is called *prime* if it satisfies any of the following equivalent conditions:

(i) $\mathfrak{p} \neq A$, and for all $x, y \in A$ such that $xy \in \mathfrak{p}$, we have $x \in \mathfrak{p}$ or $y \in \mathfrak{p}$.
(ii) the ring $A/\mathfrak{p}$ is a domain.

An ideal $\mathfrak{m}$ of A is called *maximal* if it satisfies any of the following equivalent conditions:

(i') $\mathfrak{m} \neq A$, and for all ideals I of A such that $\mathfrak{m} \subset I$, we have $\mathfrak{m} = I$ or $A = I$.
(ii') the ring $A/\mathfrak{m}$ is a field.

Remark 1.1.1. Since a field is a domain, every maximal ideal is prime. The converse does not hold; for instance the zero ideal in $\mathbb{Z}$ is prime but not maximal.

We now prove a few lemmas on prime ideals that will be useful.

Lemma 1.1.2. *Let $A \subset B$ be a ring extension. If $\mathfrak{q}$ is a prime ideal of B, then $\mathfrak{q} \cap A$ is a prime ideal of A.*

Proof. Indeed, the morphism $A/(\mathfrak{q} \cap A) \to B/\mathfrak{q}$ is injective, and $B/\mathfrak{q}$ is a domain. Thus $A/(\mathfrak{q} \cap A)$ is a subring of domain, and therefore it is a domain. Equivalently $\mathfrak{q} \cap A$ is a prime ideal of A. □

Lemma 1.1.3. *Let A be a ring, and $\mathfrak{p}$ a prime ideal of A. If $I_1, \dots, I_n$ are ideals of A such that $I_1 \cdots I_n \subset \mathfrak{p}$, then there exists $i \in \{1, \dots, n\}$ such that $I_i \subset \mathfrak{p}$.*

Proof. Assume the contrary, so that $\mathfrak{p}$ contains no I_i. Then there for each $i \in \{1, \dots, n\}$ there exists an element $a_i \in I_i$ such that $a_i \notin \mathfrak{p}$. Then $a_1 \cdots a_n \notin \mathfrak{p}$ because $\mathfrak{p}$ is prime. But $a_1 \cdots a_n \in I_1 \cdots I_n$, a contradiction. □

The next lemma might seem similar, but will have somewhat deeper consequences:

Lemma 1.1.4 (Prime avoidance). *Let $I, \mathfrak{p}_1, \ldots, \mathfrak{p}_n$ be ideals in a ring A. Assume that the ideal $\mathfrak{p}_i$ is prime for $i \geq 3$. If $I \subset \mathfrak{p}_1 \cup \cdots \cup \mathfrak{p}_n$, then $I \subset \mathfrak{p}_i$ for some $i \in \{1, \ldots, n\}$.*

Proof. We assume that I is contained in no $\mathfrak{p}_i$ and find $x \in I$ belonging to no $\mathfrak{p}_i$. This is clear for $n \in \{0, 1\}$. If $n = 2$, we find for $i = 1, 2$ elements $x_i \in I$ such that $x_i \not\in \mathfrak{p}_i$. We may assume that $x_1 \in \mathfrak{p}_2$ and $x_2 \in \mathfrak{p}_1$ (otherwise the statement is proved, by taking $x = x_1$ or $x = x_2$). Then $x = x_1 + x_2$ works.

We now assume that $n > 2$, and proceed by induction on n. For each $j = 1, \ldots, n$, we can find by induction an element $x_j \in I$ which is in none of the ideals $\mathfrak{p}_i$ for $i \neq j$. As above, we may assume that $x_j \in \mathfrak{p}_j$, for all $j \in \{1, \ldots, n\}$ (otherwise $x = x_j$ works). Then we claim

$$x = x_n + x_1 \cdots x_{n-1} \in I$$

does the job (here $x_1 \cdots x_{n-1}$ denotes the product). Indeed assume that $x \in \mathfrak{p}_j$ for some $j \in \{1, \ldots, n\}$. If $j \neq n$, then $x_1 \cdots x_{n-1} \in \mathfrak{p}_j$ (because $x_j \in \mathfrak{p}_j$), and thus $x_n = x - x_1 \cdots x_{n-1} \in \mathfrak{p}_j$, contradicting the choice of x_n. If $j = n$, then $x_1 \cdots x_{n-1} = x - x_n \in \mathfrak{p}_n$, and as the ideal $\mathfrak{p}_n$ is prime by assumption (because $n \geq 3$), we deduce that $x_i \in \mathfrak{p}_n$ for some $i \in \{1, \ldots, n-1\}$, contradicting the choice of x_i. □

We will also need the so-called Chinese remainder theorem:

Lemma 1.1.5. *Let A be a ring, and $I_1, \ldots, I_n$ ideals of A such that $I_i + I_j = A$ for all $i \neq j$.*

(i) We have

$$I_1 \cdots I_n = I_1 \cap \cdots \cap I_n.$$

(ii) The natural ring morphism

$$A/(I_1 \cdots I_n) \to (A/I_1) \times \cdots \times (A/I_n)$$

is bijective.

Proof. (i): Clearly $I_1 \cdots I_n \subset I_1 \cap \cdots \cap I_n$. We prove the other inclusion by induction on n, the case $n = 1$ being trivial. Assume that $n = 2$. Pick $a_1 \in I_1, a_2 \in I_2$ such that $a_1 + a_2 = 1$. Then for any $x \in I_1 \cap I_2$ we have

$$x = x(a_1 + a_2) \in (I_1 \cap I_2)I_1 + (I_1 \cap I_2)I_2 \subset I_1 I_2,$$

proving (i) for $n = 2$. Assume now that $n \geq 3$. Let $I = I_1 \cdots I_{n-1}$. By induction, we know that $I = I_1 \cap \cdots \cap I_{n-1}$. For each $i \in \{1, \ldots, n-1\}$, as $I_i + I_n = A$, we find elements $x_i \in I_i, y_i \in I_n$ such that $x_i + y_i = 1$. Thus

$$x_1 \cdots x_{n-1} = (1 - y_1) \cdots (1 - y_{n-1}) = 1 \mod I_n.$$

As $x_1 \cdots x_{n-1} \in I$, this shows that $I_n + I = A$, hence by the case $n = 2$ considered above, we have

$$I_1 \cap \cdots \cap I_n = I \cap I_n = II_n = I_1 \cdots I_n.$$

(ii): Consider the natural ring morphism

$$A \to (A/I_1) \times \cdots \times (A/I_n) \quad a \mapsto (a \mod I_1, \ldots, a \mod I_n). \tag{1.1.a}$$

Its kernel is $I_1 \cap \cdots \cap I_n$, hence it follows from (i) that the morphism of (ii) is injective. For all $i, j \in \{1, \dots, n\}$ with $i \neq j$, using the relations $I_i + I_j = A$ we find elements $e_{ij} \in I_j$ such that $e_{ij} = 1 \mod I_i$. We set, for all $i \in \{1, \dots, n\}$

$$e_i = \prod_{j \neq i} e_{ij}.$$

Then $e_i = 1 \mod I_i$, and $e_i \in I_j$ for all $j \neq i$. Now if $(x_1, \dots, x_n) \in A^n$, the element

$$\sum_{i=1}^{n} e_i x_i \in A$$

maps to $(x_1 \mod I_1, \dots, x_n \mod I_n)$ under the map (1.1.a). We have proved that the map (ii) is surjective. □

2. Noetherian rings

Proposition 1.2.1. *Let A be a ring, and M an A-module. The following conditions are equivalent:*

(i) every nonempty family of A-submodules of M admits a maximal element (for the relation of inclusion),

(ii) if P_n for $n \in \mathbb{N}$ are A-submodules of M satisfying $P_n \subset P_{n+1}$ for all n, there exists $s \in \mathbb{N}$ such that $P_n = P_s$ for all $n \geq s$,

(iii) every A-submodule of M is finitely generated.

Proof. (i) $\Rightarrow$ (iii) : Let N be an A-submodule of M. Consider the set Σ of all finitely generated A-submodules of M which are contained in N. The set Σ is nonempty, because it contains the zero ideal, so by (i) we may find a maximal element N in the set Σ (ordered by inclusion). Let $x \in N$. As $N' \subset N' + Ax \subset N$, we must have $N' = N' + Ax$ by maximality of N', and so $x \in N'$. We have proved that $N = N'$, and in particular the A-module N is finitely generated.

(ii) $\Rightarrow$ (i) : Let E be a nonempty set of A-submodules of M. If the set E has no maximal element (for the relation of inclusion), we can find inductively elements $P_n \in E$ for all $n \in \mathbb{N}$, in such a way that $P_n \subsetneq P_{n+1}$ for all n. This contradicts (ii).

(iii) $\Rightarrow$ (ii) : Consider a family of A-submodules P_n of M, for $n \in \mathbb{N}$, which satisfies $P_n \subset P_{n+1}$ for all $n \in \mathbb{N}$. Then $P = \bigcup_{n \in \mathbb{N}} P_n$ is an A-submodule of M, it is thus finitely generated by (iii), say by the elements $x_1, \dots, x_m \in P_n$. For s large enough, we have $x_1, \dots, x_m \in P_s$, and so $P_s = P$. In particular for $n \geq s$, we have $P_s \subset P_n \subset P = P_s$, and so $P_n = P_s$. □

Definition 1.2.2. Let A be a ring. An A-module M will be called *noetherian* if it satisfies the conditions of Proposition 1.2.1. A ring A is called *noetherian* if it is noetherian as a module over itself.

Proposition 1.2.3. *Let A be a ring.*

(i) Let $f\colon M \to P$ be a surjective morphism of A-modules. If the A-module M is noetherian, then so is P.

(ii) If M and N are noetherian A-modules, then so is $M \oplus N$.

Proof. (i): Consider a family of A-submodules P_n of P, for $n \in \mathbb{N}$, such that $P_n \subset P_{n+1}$ for all $n \in \mathbb{N}$. For each $n \in \mathbb{N}$, consider the A-submodule $M_n = f^{-1}P_n$ in M. Then $M_n \subset M_{n+1}$ for all $n \in \mathbb{N}$, and $f(M_n) = P_n$ because f is surjective.

As M is noetherian we may find $s \in \mathbb{N}$ such that $M_n = M_s$ for $n \geq s$, and thus $P_n = f(M_n) = f(M_s) = P_s$ for $n \geq s$. We have proved that P is noetherian.

(ii): Let $P_n \subset M \oplus N$ for $n \in \mathbb{N}$ be a family of A-submodules such that $P_n \subset P_{n+1}$ for all $n \in \mathbb{N}$. Consider the second projection $\pi \colon M \oplus N \to N$. Then the family $\pi(P_n)$ for $n \in \mathbb{N}$ satisfies $\pi(P_n) \subset \pi(P_{n+1})$ for all n, and as N is a noetherian A-module, we find an integer $s \in \mathbb{N}$ such that $\pi(P_n) = \pi(P_s)$ for all $n \geq s$.

Let $n \geq s$, and $x \in P_n$. As $\pi(P_n) = \pi(P_s)$, we find $y \in P_s$ such that $\pi(x) = \pi(y)$, or equivalently $z = x - y \in M$ (we view M as an A-submodule of $M \oplus N$ via $m \mapsto (m, 0)$). Thus $x = z + y \in M + P_s$, and thus

$$P_n \subset M + P_s \subset M \oplus N \quad \text{for all } n \geq s. \tag{1.2.a}$$

For $m \in \mathbb{N}$, consider that A-submodule $Q_m = P_{m+s}/P_s$ of $(M \oplus N)/P_s$. It follows from (1.2.a) for all $m \in \mathbb{N}$, the A-submodule Q_m is contained in $(M + P_s)/P_s = M/(P_s \cap M)$. But the A-module $M/(P_s \cap M)$ is noetherian by (i) (because M is assumed noetherian), and as $Q_m \subset Q_{m+1}$ for $m \in \mathbb{N}$, we find $r \in \mathbb{N}$ such that $Q_m = Q_r$ for $m \geq r$. Thus $P_n/P_s = P_{r+s}/P_s$ for all $n \geq r + s$, which implies that $P_n = P_{r+s}$. We have proved that the A-module $M \oplus N$ is noetherian. □

Corollary 1.2.4. *Let A be a noetherian ring, and M a finitely generated A-module. Then every A-submodule of M is finitely generated.*

Proof. Let $x_1, \dots, x_n$ be a set of generators for the A-module M. We define a morphism of A-modules $A^{\oplus n} \to M$ by mapping the i-th element of the canonical A-basis of $A^{\oplus n}$ to x_i, for $i = 1, \dots, n$. This morphism is surjective (because $x_1, \dots, x_n$ generate M), the A-module $A^{\oplus n}$ is noetherian by Proposition 1.2.3 (ii) (applied $n - 1$ times), and thus the A-module M is noetherian by Proposition 1.2.3 (i). This proves the corollary, in view of Proposition 1.2.1. □

Proposition 1.2.5. *Every principal ideal domain is a noetherian ring.*

Proof. Indeed, every ideal is generated by a single element, and is thus finitely generated. □

Lemma 1.2.6. *Let A be a noetherian ring, and I an ideal of A. If $I \neq A$, then I is contained in a maximal ideal.*

Proof. The set of ideals of A containing I and distinct from A is nonempty (it contains the element I), hence as A is noetherian it admits a maximal element. Such an element is a maximal ideal of A which contains I. □

Remark 1.2.7. In fact, in any ring every proper ideal is contained in a maximal ideal. This is a consequence of the so-called Zorn's Lemma. We will not use this fact.

Bibliography

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