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

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

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

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

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

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

(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 $\mathbb{Z}$.

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.

Let A be a ring. An A-*algebra* is a ring R equipped with a ring morphism $\iota_R \colon A \to R$. When R, S are A-algebra, a ring morphism $f \colon R \to S$ is called a morphism of A-algebras if $f \circ \iota_R = \iota_S$.

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 $I, \mathfrak{p}_1, \dots, \mathfrak{p}_n$ 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 $i \in \{1,\dots,n\}$.*

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 $x_i \notin \mathfrak{p}_i$. 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 $j = 1, \dots, n$, 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 $j \in \{1,\dots,n\}$ (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 $j \in \{1,\dots,n\}$. 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 $i \in \{1,\dots,n-1\}$, 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 $I_1, \dots, I_n$ 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 $i \in \{1,\dots,n-1\}$, 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

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

(ii): Consider the natural ring morphism

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

Its kernel is $I_1 \cap \cdots \cap I_n$, hence it follows from (i) that the morphism of (ii) is injective. For all $i, j \in \{1, \ldots, n\}$ 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 $i \in \{1, \ldots, n\}$

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

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

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

maps to $(x_1 \mod I_1, \ldots, x_n \mod I_n)$ 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) ⇒ (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) ⇒ (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) ⇒ (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 $x_1, \ldots, x_m \in P_n$. For s large enough, we have $x_1, \ldots, x_m \in P_s$, 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.

3. Modules over principal ideal domains

Let A be a ring, and $n \in \mathbb{N}$. Recall that an A-module M is called *free of rank n* if it there exist elements $e_1, \dots, e_n \in M$ such that

$$M = Ae_1 \oplus \cdots \oplus Ae_n.$$

The family $(e_1, \dots, e_n)$ is then called an A-basis of M.

Remark 1.3.1. Looking at the case $A = 0$ (and thus $M = 0$), it is clear that the integer n such that M is free of rank n is not unique, if it exists. In fact, one may prove that n is unique as soon as $A \neq 0$. The case when A is principal ideal domain will follow from Lemma 1.3.5 below (whose arguments only use the fact that the ring A is a domain; a different argument is required for the general case).

Theorem 1.3.2. *Let A be a principal ideal domain. Let F be a free A-module of rank $n \in \mathbb{N}$, and $M \subset F$ a submodule. Then the A-module M is free of rank q, for some integer $q \in \mathbb{N}$ such that $q \leq n$.*

In addition there exist an A-basis $(e_1, \dots, e_n)$ of F, and elements $a_1, \dots, a_q \in A$ such that $(a_1e_1, \dots, a_qe_q)$ is an A-basis of M, and $a_i \mid a_{i+1}$ for $i = 1, \dots, q-1$.

The proof of Theorem 1.3.2 is quite long, so we break it into a series of lemmas. Let us put ourselves in the situation of Theorem 1.3.2, and let K be the fraction field of A. Let us choose a K-vector space V, such that F is an A-submodule of V. Such V does exist, because the A-module F is free of rank n (for instance, pick a basis $x_1, \dots, x_n$ of F, set $V = K^n$ and define the inclusion $F \subset V$ by mapping x_i to the i-th vector in the canonical basis of K^n). When $N \subset F$ is an A-submodule, we let $\widetilde{N}$ be the K-vector space spanned by N in V.

Lemma 1.3.3. *Let $N \subset F$ be an A-submodule. For all $x \in \widetilde{N}$, there exists a nonzero element $a \in A$ such that $ax \in N$.*

Proof. Let us write

$$x = \sum_{i=1}^{s} \lambda_i y_i, \text{ with } \lambda_1, \dots, \lambda_s \in K \text{ and } y_1, \dots, y_s \in N.$$

For $i \in \{1, \dots, s\}$, write $\lambda_i = a_i/b_i$ with $a_i, b_i \in A$. Then we may take $a = b_1 \cdots b_s$. □

For an A-submodule $N \subset F$, we define

$$r(N) = \dim_K \widetilde{N}. \tag{1.3.a}$$

Remark 1.3.4. The integer $r(N)$ is sometimes called the rank of N (even when N is not free). It is possible to give a (seemingly) more intrinsic definition using the tensor product, by setting $r(N) = \dim_K(N \otimes_A K)$. In particular, one may prove that the integer (1.3.a) is independent of the choice of V.

Lemma 1.3.5. *If the A-module N is free of rank m, then $r(N) = m$.*

Proof. Let $(e_1, \dots, e_m)$ be an A-basis of N. Then the system $(e_1, \dots, e_m) \in V^n$ certainly generates the K-vector space $\widetilde{N}$. Assume that $\lambda_1, \dots, \lambda_n \in K$ are such that

$$\sum_{i=1}^{m} \lambda_i e_i = 0 \in \widetilde{N} \subset V.$$

Letting $b \in A \smallsetminus \{0\}$ be such that $b\lambda_i \in A$ for all $i \in \{1, \dots, m\}$ (the element b is a common denominator of $\lambda_1, \dots, \lambda_m$, see the proof of Lemma 1.3.3), we thus have

$$\sum_{i=1}^{m} (b\lambda_i) e_i = 0.$$

This equality holds in $N \subset V$, hence by A-linear independence of the system $(e_1, \dots, e_m)$, we deduce that $b\lambda_1 = \cdots = b\lambda_m = 0$ in A, and thus in K. As $b \neq 0$, we obtain

$\lambda_1 = \cdots = \lambda_m = 0$ in K. We have proved that the system $(e_1, \ldots, e_m)$ is K-linearly independent. Therefore $(e_1, \ldots, e_m)$ is a K-basis of $\widetilde{N}$, and so $\dim_K \widetilde{N} = m$. □

Lemma 1.3.6. *Let N_1, N_2 be A-modules such that $N_1 \oplus N_2$ is a submodule of F. Then*

$$r(N_1 \oplus N_2) = r(N_1) + r(N_2).$$

Proof. Since the A-module $N_1 \oplus N_2$ is generated by $N_1 \cup N_2$, the K-vector space $\widetilde{N_1 \oplus N_2}$ is generated by $\widetilde{N_1} \cup \widetilde{N_2}$, and thus $\widetilde{N_1 \oplus N_2} = \widetilde{N_1} + \widetilde{N_1}$. To conclude the proof of the lemma, it will suffice to prove that $\widetilde{N_1} \cap \widetilde{N_2} = 0$ in V. If $x \in \widetilde{N_1} \cap \widetilde{N_2}$, then by Lemma 1.3.3 we may find nonzero elements $a_1, a_2 \in A$ such that $a_1 x \in N_1$ and $a_2 x \in N_2$. Setting $a = a_1 a_2$, we have $ax \in N_1 \cap N_2$. Then $ax = 0$ in F, and thus also in V. This yields $x = a^{-1}ax = 0 \in V$. □

We will denote by $\operatorname{Hom}_A(F, A)$ the set of morphisms of A-modules $F \to A$. Let us choose $\varphi \in \operatorname{Hom}_A(F, A)$ such that the subset $\varphi(M)$ is maximal (for the inclusion relation); this is possible because those subsets are ideals of A, and the ring A is noetherian (Proposition 1.2.5). As A is a principal ideal domain, we may find an element $\alpha \in A$ such that $\varphi(M) = \alpha A$.

Let us choose an A-basis $(x_1, \ldots, x_n)$ of F. Let $\pi_1, \ldots, \pi_n \in \operatorname{Hom}_A(F, A)$ be the system defined by the relations

$$\pi_i(x_j) = \delta_{ij} \quad \text{for } 1 \leq i, j \leq n,$$

where we use the *Kronecker symbol*:

$$\delta_{ij} = \begin{cases} 1 & \text{if } i = j, \\ 0 & \text{if } i \neq j. \end{cases} \tag{1.3.b}$$

Let us now assume that the A-module M is nonzero. Then we have $\pi_i(M) \neq 0$ for some $i \in \{1, \ldots, n\}$, and in particular

$$\alpha \neq 0. \tag{1.3.c}$$

Recall that by definition $\alpha A = \varphi(M)$, so let us pick an element

$$e' \in M \text{ such that } \varphi(e') = \alpha.$$

Lemma 1.3.7. *For all $\psi \in \operatorname{Hom}_A(F, A)$, we have $\psi(e') \in \alpha A$.*

Proof. As A is a principal ideal domain, the ideal of A generated by $\psi(e')$ and α in A is of the form dA, for some $d \in A$. Let us write $d = u\psi(e') + v\alpha$, with $u, v \in A$. Set $\rho = u\psi + v\varphi \in \operatorname{Hom}_A(F, A)$, so that $d = \rho(e')$. We have

$$\varphi(M) = \alpha A \subset dA = \rho(e'A) \subset \rho(M),$$

hence by maximality of φ, we deduce that $\varphi(M) = \rho(M)$, and so $\alpha A = dA$. As $\psi(e') \in dA$, the statement follows. □

Lemma 1.3.7 implies in particular that for each $i \in \{1, \ldots, n\}$, we may find an element $b_i \in A$ such that $\pi_i(e') = \alpha b_i$. Set

$$e = \sum_{i=1}^{n} b_i x_i \in F.$$

Then $e' = \alpha e$ (because their components in the basis $(x_1, \dots, x_n)$ coincide). Now

$$\alpha = \varphi(e') = \varphi(\alpha e) = \alpha\varphi(e).$$

Since the ring A is a domain, and $\alpha \neq 0$ (see (1.3.c)), this implies that

$$\varphi(e) = 1.$$

Lemma 1.3.8. *We have*

(i) $F = Ae \oplus \ker\varphi$,

(ii) $M = Ae' \oplus (M \cap \ker\varphi)$.

Proof. Every element $x \in F$ decomposes as

$$x = \varphi(x)e + (x - \varphi(x)e),$$

which shows that $F = Ae + \ker\varphi$. Let now $y \in M$. As $\varphi(M) = \alpha A$, we have $\varphi(y) = b\alpha$ for some $b \in A$. Then

$$y = be' + (y - be'),$$

which shows that $M = Ae' + (M \cap \ker\varphi)$.

Now, if $a \in A$ is such that $ae \in \ker\varphi$, then $0 = a\varphi(e) = a$, and thus $ae = 0$. This shows that $Ae \cap (\ker\varphi) = 0$. As $Ae' \cap (M \cap \ker\varphi) \subset Ae \cap (\ker\varphi)$, we also have $Ae' \cap (M \cap \ker\varphi) = 0$. □

Lemma 1.3.9. *The A-module M is free of rank r, for some integer $r \leq n$.*

Proof. Let $r = r(M)$. As $M \subset F$, we have $\widetilde{M} \subset \widetilde{F}$, and thus

$$r = r(M) = \dim_K \widetilde{M} \leq \dim_K \widetilde{F} = r(F).$$

Since $r(F) = n$ by Lemma 1.3.5, we have proved that $r \leq n$. To conclude, we prove that M is free of rank r.

We proceed by induction on the integer r. If $r = 0$, then $M = 0$ and the statement is true. Assume that $r > 0$, so that $M \neq 0$. Pick φ, α, e, e' as above. Then by Lemma 1.3.8 (ii) and Lemma 1.3.6 we have $r(M \cap \ker\varphi) = r - 1$. Therefore by induction the A-module $M \cap \ker\varphi$ is free of rank $r - 1$, and it follows from Lemma 1.3.8 (ii) that the A-module M is free of rank r. □

Proof of Theorem 1.3.2. We proceed by induction on n. The statement is clear when $n = 0$, so we assume that $n > 0$. We use the notation φ, α, e, e' given above. We know by Lemma 1.3.9, applied to the submodule $\ker\varphi \subset F$, that the A-modules $\ker\varphi$ is free of rank $m \leq n$. By Lemma 1.3.8 (i), Lemma 1.3.5 and Lemma 1.3.6, we have

$$m = r(\ker\varphi) = r(F) - 1 = n - 1.$$

Thus we may apply the inductive hypothesis to the free A-module $\ker\varphi$ and its submodule $M \cap \ker\varphi$. We obtain an A-basis $(e_2, \dots, e_n)$ of $\ker\varphi$, and nonzero elements $a_2, \dots, a_q \in A$ such that $(a_2e_2, \dots, a_qe_q)$ is an A-basis of $M \cap \ker\varphi$, and $a_i \mid a_{i+1}$ for $i = 2, \dots, q - 1$. Here we may assume that $q \geq 1$. Setting $a_1 = \alpha$ and $e_1 = e$, in view of Lemma 1.3.8 we obtain that $(e_1, \dots, e_n)$ is an A-basis of F, and that $(a_1e_1, \dots, a_qe_q)$ is an A-basis of M.

If $q = 1$, this concludes the proof of Theorem 1.3.2. Let us assume that $q \geq 2$, and prove that $a_1 \mid a_2$. Consider the linear form $\xi \in \operatorname{Hom}_A(F, A)$ defined by $\xi(e_1) = \xi(e_2) = 1$ and $\xi(e_i) = 0$ for $i \in \{3, \dots, n\}$. Then $\xi(e') = \alpha$, hence $\varphi(M) = \alpha A \subset \xi(M)$. By maximality of φ, it follows that $\alpha A = \xi(M)$. As $\xi(a_2e_2) = a_2 \in \xi(M)$, we have $a_1 = \alpha \mid a_2$. This concludes the proof of Theorem 1.3.2. □

Finally, it will be convenient to record now the following complement to Theorem 1.3.2:

Proposition 1.3.10. *In the situation of Theorem 1.3.2, let K be fraction field of A. Let $m \in \mathbb{N}$, and consider the integer $q \in \mathbb{N}$ given by Theorem 1.3.2. Then the following conditions are equivalent:*

(i) the A-module M is free of rank m,

(ii) the A-module F is a submodule of a K-vector space V, in which the set M spans a K-subspace of dimension m,

(iii) $q = m$.

Proof. (i) ⇒ (ii): As observed above, the A-module F is always contained in some K-vector space V. The K-subspace $\widetilde{M}$ spanned by M in V has dimension $r(M)$ (see (1.3.a)), and we have $r(M) = m$ by Lemma 1.3.5.

(ii) ⇒ (iii): The A-module M is free of rank q by Theorem 1.3.2. Using the given K-vector space V to define the integer $r(M)$, we have $r(M) = m$ by definition (see (1.3.a)), and it follows from Lemma 1.3.5 that $m = q$.

(iii) ⇒ (i): Certainly if $(a_1e_1, \ldots, a_qe_q)$ is an A-basis of M, then M is free of rank q. □

Bibliography

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