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*

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

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 $I = \beta \cdot \mathbb{Z}[i]$. $\square$

Recall that an element x in a ring R is called *irreducible* if $x \notin R^\times \cup \{0\}$, and for all $a, b \in R$

$$x = ab \implies a \in R^\times \text{ or } b \in R^\times.$$

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

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

(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

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

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.

Example 1.2.3. Let k be a field, and A a k-algebra. If A is of finite dimension as a k-vector space, then the ring A is noetherian; indeed, a chain of ideals of A is in particular a chain of k-vector spaces.

Proposition 1.2.4. *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 1.2.5. *Let A be a noetherian ring, and M a finitely generated A-module. Then every A-submodule of M is finitely generated.*

Proof. Let $x_1, \ldots, x_n$ 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 $i = 1, \ldots, n$. This morphism is surjective (because $x_1, \ldots, x_n$ generate M), the A-module $A^{\oplus n}$ is noetherian by Proposition 1.2.4 (ii) (applied $n - 1$ times), and thus the A-module M is noetherian by Proposition 1.2.4 (i). This proves the corollary, in view of Proposition 1.2.1. □

Proposition 1.2.6. *Every principal ideal domain is a noetherian ring.*

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

Lemma 1.2.7. *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 1.2.8. 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.

Lemma 1.2.9. *Let A be a noetherian ring.*

(i) Every ideal of A contains a product of prime ideals.

(ii) Assume that A is a domain. Then every nonzero ideal of A contains a product of nonzero prime ideals of A.

Repetitions are allowed in those products (i.e. the prime ideals need not be pairwise distinct), and those products are finite. Moreover, the ideal A itself is considered a product of prime ideals (over the empty family).

Proof. In case (i), we let Φ be the set of ideals of A which contain no product of prime ideals. In case (ii), we let Φ be the set of nonzero ideals of A which contain no product of nonzero prime ideals. To prove the lemma, it suffices to show that the set Φ is empty. So we assume $\Phi \neq \varnothing$ and find a contradiction. As the ring A is noetherian, the set Φ contains a maximal element I (for the inclusion of ideals). The ideal I is certainly not prime, as otherwise it would be a product of prime ideals (resp. nonzero prime ideals in case (ii)). Also $A \notin \Phi$ (because it is the product of the empty family of nonzero prime ideals), and thus $I \neq A$. So we may find $x, y \in A \smallsetminus I$ such that $xy \in I$. The ideals $I' = I + xA$ and $I'' = I + yA$ contain strictly I, hence by the choice of the ideal I, each of these ideals contains a product of prime ideals (resp. nonzero prime ideals). Then their product $I'I''$ contains a product of prime ideals (resp. nonzero prime ideals). Now

$$I'I'' = (I + xA)(I + yA) \subset I^2 + xI + yI + xyA \subset I,$$

which implies that the ideal I itself contains a product of prime ideals (resp. nonzero prime ideals). We have obtained a contradiction. □

Lemma 1.2.10. *Let A be a noetherian ring, and I an ideal of A. Then the set of prime ideals of A which are minimal (for the relation of inclusion) among those containing I, is finite.*

Proof. For every ideal J of A, let us denote by $\mathcal{M}(J)$ the set of prime ideals of A, which are minimal among those containing J. Let Φ be the set of ideals J of A such that the set $\mathcal{M}(J)$ is infinite. It will suffice to prove that the set Φ is empty. So we assume $\Phi \neq \varnothing$ and find a contradiction. As the ring A is noetherian, the set Φ admits a maximal element J. The ideal J is not prime, as otherwise the set $\mathcal{M}(J) = \{J\}$ would be finite. Also $J \neq A$, because $\mathcal{M}(A) = \varnothing$ is finite. Thus we may find $x, y \in A \smallsetminus J$ such that $xy \in J$. The ideals $J + xA$ and $J + yA$ both strictly contain J, hence $\mathcal{M}(J + xA)$ and $\mathcal{M}(J + yA)$ are both finite (by the choice of the ideal J). Now for any $\mathfrak{p} \in \mathcal{M}(J)$, we have $xy \in J \subset \mathfrak{p}$, hence $x \in \mathfrak{p}$ or $y \in \mathfrak{p}$ (as the ideal $\mathfrak{p}$ is prime). It follows that

$$\mathcal{M}(J) \subset \mathcal{M}(J + xA) \cup \mathcal{M}(J + yA)$$

(here we use the following fact: if $\mathfrak{p}$ is a prime ideal of A minimal among those containing J, and J' is an ideal of A such that $J \subset J' \subset \mathfrak{p}$, then $\mathfrak{p}$ is minimal among the prime ideals containing J'). In particular the set $\mathcal{M}(J)$ must be finite, a contradiction. □

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 $e_1, \ldots, e_n \in M$ such that

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

The family $(e_1, \ldots, e_n)$ 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 a principal ideal domain will

follow from Lemma 1.3.8 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 $(a_1 e_1, \dots, a_q e_q)$ is an A-basis of M, and $a_i \mid a_{i+1}$ for $i = 1, \dots, q-1$.

Before proving Theorem 1.3.2, we discuss some classical consequences.

Corollary 1.3.3. *Let A be a principal ideal domain, and M a finitely generated A-module. Then*

$$M \simeq (A/a_1 A) \oplus \cdots \oplus (A/a_n A),$$

for some $a_1, \dots, a_n \in A$ such that $a_i \mid a_{i+1}$ for $i = 1, \dots, n-1$.

Proof. As M is finitely generated, we may find a surjective morphism of A-modules $f \colon A^{\oplus n} \to M$, for some integer n (by mapping the canonical basis of $A^{\oplus n}$ to a system of n generators of M). We apply Theorem 1.3.2 to the free A-module $A^{\oplus n}$ of rank n, and its submodule $\ker f$. Then

$$\begin{aligned} M \simeq A^{\oplus n}/(\ker f) &= (Ae_1 \oplus \cdots \oplus Ae_q \oplus \cdots \oplus Ae_n)/(Aa_1 e_1 \oplus \cdots \oplus Aa_q e_q) \\ &\simeq (A/a_1 A) \oplus \cdots \oplus (A/a_q A) \oplus A^{\oplus(n-q)}. \end{aligned}$$

Here we have used the following fact: if M_1, M_2 are A-modules and $N_1 \subset M_1, N_2 \subset M_2$ submodules, we have an isomorphism

$$(M_1 \oplus M_2)/(N_1 \oplus N_2) \simeq (M_1/N_1) \oplus (M_2/N_2).$$

To conclude, we set $a_i = 0$ for $i = q, \dots, n$. □

When A is a ring, an A-module M is called *torsion-free* if for all $a \in A$ and $m \in M$

$$am = 0 \implies m = 0 \text{ or } a = 0.$$

Corollary 1.3.4. *Every finitely generated, torsion-free module over a principal ideal domain is free of finite rank.*

Proof. Let A be a principal ideal domain. Assume that M is a finitely generated, torsion-free A-module. We apply Corollary 1.3.3 to obtain elements $a_1, \dots, a_n$ and an isomorphism of A-modules $\varphi \colon M \xrightarrow{\sim} (A/a_1 A) \oplus \cdots \oplus (A/a_n A)$. Assume that $i \in \{1, \dots, n\}$ is such that a_i is not a unit in A. Then the element $x = \varphi^{-1}(0, \dots, 0, 1, 0, \dots, 0) \in M$ (where the i-th entry is 1) is nonzero (because $a_i \notin A^\times$) and satisfies $a_i x = 0$. As M is assumed to be torsion-free, this implies that $a_i = 0$. We have proved that each a_i is either a unit (in which case $A/a_i A = 0$), or zero (in which case $A/a_i A = A$). This implies that M is free of rank r, for some $r \in \mathbb{N}$ (equal to the number of indices i such that $a_i = 0$). □

Proposition 1.3.5. *Let A be an integral domain. Then any finite subgroup of $A^\times$ is cyclic.*

Proof. Let $G \subset A^\times$ be a finite subgroup. By Corollary 1.3.3, we have a group isomorphism $\varphi \colon G \xrightarrow{\sim} (\mathbb{Z}/a_1\mathbb{Z}) \times \cdots \times (\mathbb{Z}/a_n\mathbb{Z})$, where $a_1, \dots, a_n \in \mathbb{Z}$, and $a_i \mid a_{i+1}$ for $i = 1, \dots, n-1$. Set $m = a_n$. Since G is finite, the integer m is nonzero (otherwise G would

contain a subgroup isomorphic to $\mathbb{Z}$, and would thus be infinite). Since $a_i \mid m$ for each $i \in \{1, \dots, n\}$, every element $g \in G$ satisfies $g^m = 1$ (to see this, consider the components of the element $\varphi(g)$). On the other hand, the element $x = \varphi^{-1}(0, \dots, 0, 1) \in G$ has order m.

Let now K be the fraction field of A. Then in the field K, the polynomial $X^m - 1$ has at most m distinct roots. We have just seen that every element of G is a root of that polynomial, and so $\operatorname{card} G \leq m$. The m-elements $1, x, \dots, x^{m-1}$ of G are pairwise distinct (as x has order m), so that G must coincide with the set $\{1, x, \dots, x^{m-1}\}$, and in particular the group G is cyclic. □

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 1.3.6. *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 1.3.7. 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 1.3.8. *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 1.3.6), 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 1.3.9. *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 1.3.6 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 $x = a^{-1} a x = 0 \in V$. □

We will denote by $\mathrm{Hom}_A(F, A)$ the set of morphisms of A-modules $F \to A$. Let us choose $\varphi \in \mathrm{Hom}_A(F, A)$ 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 1.2.6). 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 $\pi_1, \ldots, \pi_n \in \mathrm{Hom}_A(F, A)$ 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 1.3.10. *For all $\psi \in \mathrm{Hom}_A(F, A)$, 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 $\rho = u\psi + v\varphi \in \mathrm{Hom}_A(F, A)$, 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 1.3.10 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 1.3.11. *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 1.3.12. *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 1.3.8, 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 1.3.11 (ii) and Lemma 1.3.9 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 1.3.11 (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 1.3.12, applied to the submodule $\ker\varphi \subset F$, that the A-modules $\ker\varphi$ is free of rank $m \leq n$. By Lemma 1.3.11 (i), Lemma 1.3.8 and Lemma 1.3.9, 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 1.3.11 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 $\xi \in \mathrm{Hom}_A(F, A)$ 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 1.3.13. *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) $\Rightarrow$ (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 1.3.8.

(ii) $\Rightarrow$ (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 1.3.8 that $m = q$.

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

CHAPTER 2

Integral extensions

1. Integral dependence

DEFINITION 2.1.1. Let R be a ring and $A \subset R$ a subring. An element $x \in R$ is called *integral over* A if there exist elements $a_0, \ldots, a_{n-1} \in A$ such that

$$x^n + a_{n-1}x^{n-1} + \cdots + a_0 = 0.$$

A polynomial $P \in A[X]$ whose leading term is equal to 1 will be called *monic*. Thus an element of R is integral over A if it is a zero of a monic polynomial with coefficients in A.

REMARK 2.1.2. When $A \subset R$ is a subring, every element of $a \in A$ is integral over A, being a zero of the monic polynomial $X - a$.

EXAMPLE 2.1.3. Consider the subring $\mathbb{Z} \subset \mathbb{R}$. Then $\sqrt{2}$ is integral over $\mathbb{Z}$, while $1/2$ is not.

LEMMA 2.1.4. *Let B be a ring, and A a subring. Assume that B is finitely generated as an A-module. Then every finitely generated B-module is also finitely generated as an A-module.*

PROOF. Let M be a finitely generated B-module. Let $(b_1, \ldots, b_n)$ be a finite system of generators for the A-module B, and $(m_1, \ldots, m_s)$ a finite system of generators for the B-module M. Then

$$(b_i m_j) \quad \text{for } 1 \leq i \leq n \text{ and } 1 \leq j \leq s$$

is a finite system of generators for the A-module M. □

Let R be a ring and $A \subset R$ a subring. Let $x \in R$. We will denote by $A[x] \subset R$ the A-subalgebra generated by x. This is the smallest (for the inclusion) subring of R containing A and x. Its elements are those elements of R of the form $a_n x^n + \cdots + a_0$, where $a_0, \ldots, a_n \in A$. We warn the reader that, despite the notation, the ring $A[x]$ depends on the extension $A \subset R$, and will not necessarily isomorphic to the polynomial ring in one variable over A. We will reserve the notation $A[X]$ for the polynomial ring (using capital letters for indeterminates). More generally, we will denote by $A[x_1, \ldots, x_n]$ the A-subalgebra of R generated by the elements $x_1, \ldots, x_n \in R$.

We will need the following observation:

LEMMA 2.1.5. *Let R be a ring, and elements $x_1, \ldots, x_n \in R$. Assume that $1 \in R$ is an R-linear combination of the elements $x_1, \ldots, x_n$. If $M \in M_n(R)$ is such that the column vector $(x_1, \ldots, x_n)$ lies in the kernel of M, then $\det M = 0 \in R$.*

PROOF. Consider the *adjugate matrix* N to M, i.e. the transpose of the comatrix of M (the (i,j)-th entry of the comatrix is $(-1)^{i+j}$ times the determinant of the matrix obtained from M by deleting the i-th row and j-th column). Then a basic property of the determinant (namely, the Laplace expansion) can be expressed as

$$NM = (\det M) \cdot I_n \in M_n(R),$$

where I_n is the $n \times n$ identity matrix. We deduce that for each $i \in \{1, \dots, n\}$, the element x_i is annihilated in R by the element $\det M$. Since by assumption we have

$$1 = \sum_{i=1}^{n} a_i x_i, \quad \text{for some } a_1, \dots, a_n \in R,$$

it follows that

$$\det M = (\det M) \cdot 1 = (\det M) \sum_{i=1}^{n} a_i x_i = \sum_{i=1}^{n} a_i (\det M) x_i = 0. \qquad \square$$

PROPOSITION 2.1.6. *Let R be a ring and $A \subset R$ a subring. Let $x \in R$. The following conditions are equivalent:*

(i) the element x is integral over A,
(ii) the A-module $A[x]$ is finitely generated,
(iii) the subring $A[x]$ is contained in a subring C of R, and C is finitely generated as an A-module.

PROOF. (i) $\Rightarrow$ (ii) : By assumption, we have an equation

$$x^n = -a_{n-1}x^{n-1} - \cdots - a_0, \quad \text{where } a_0, \dots, a_{n-1} \in A.$$

Multiplying with x^j for $j \geq 0$, we obtain

$$x^{n+j} = -a_{n-1}x^{n+j-1} - \cdots - a_0 x^j, \quad \text{where } a_0, \dots, a_{n-1} \in A.$$

We deduce by induction on j that x^{n+j} belongs to the A-submodule of R generated by $1, \dots, x^{n-1}$, for all $j \in \mathbb{N}$. Since $A[x]$ is the A-submodule of R generated by the elements x^i for $i \in \mathbb{N}$, we have proved that $A[x]$ is generated by $1, \dots, x^{n-1}$.

(ii) $\Rightarrow$ (iii) : Take $C = A[x]$.

(iii) $\Rightarrow$ (i) : Let $(y_1, \dots, y_n)$ be a generating system for the A-module C. As $x \in A[x] \subset C$, and C is a subring of R, we have $xy_i \in C$ for all $i \in \{1, \dots, n\}$. Therefore we may write, for each $i \in \{1, \dots, n\}$

$$xy_i = \sum_{j=1}^{n} a_{ij} y_j, \quad \text{with } a_{ij} \in A. \tag{2.1.a}$$

So we have equations in R, for $i = 1, \dots, n$

$$\sum_{j=1}^{n} (\delta_{ij} x - a_{ij}) y_j = 0, \tag{2.1.b}$$

where δ_{ij} is the Kronecker symbol (see (1.3.b)).

Consider the $n \times n$ matrix $M \in M_n(R)$, whose coefficients are $\delta_{ij}x - a_{ij} \in R$. Then (2.1.b) expresses the fact that the column vector $(y_1, \dots, y_n) \in R^n$ lies in the kernel of M. In addition 1 is an A-linear combination of the elements $y_1, \dots, y_n$, as is any element of

C by the choice of the family $y_1, \dots, y_n$. Therefore by Lemma 2.1.5, we have $\det M = 0$. Expanding the determinant $\det M$, we obtain

$$0 = \det M = x^n + a_{n-1}x^{n-1} + \cdots + a_0, \quad \text{where } a_0, \dots, a_{n-1} \in A.$$

(If $P \in A[X]$ is the characteristic polynomial of the matrix $(a_{ij}) \in M_n(A)$, then $\det M = P(x) \in R$, and $1, a_{n-1}, \dots, a_0$ are the coefficients of P.) This is the required equation of integral dependence to prove that x is integral over A. □

COROLLARY 2.1.7. *Let R be a ring, and $A \subset R$ a subring. If $x_1, \dots, x_n \in R$ are all integral over A, then the A-module $A[x_1, \dots, x_n]$ is finitely generated.*

PROOF. We proceed by induction on n, the case $n = 0$ being Remark 2.1.2. Assume that $n \geq 1$. Set $A' = A[x_1, \dots, x_{n-1}]$. Then by induction the A-module A' is finitely generated. Since x_n is integral over A, it is also integral over A' (because $A \subset A'$). Therefore by the implication (i) $\Rightarrow$ (ii) in Proposition 2.1.6, the A'-module $A'[x_n] = A[x_1, \dots, x_n]$ is finitely generated. We conclude using Lemma 2.1.4 that the A-module $A[x_1, \dots, x_n]$ is finitely generated. □

PROPOSITION 2.1.8. *Let R be a ring and $A \subset R$ a subring. If $x, y \in R$ are both integral over A, then so are xy and $x + y$.*

PROOF. By Corollary 2.1.7, the subring $A[x, y] \subset R$ is finitely generated as an A-module. For $z \in \{xy, x+y\}$, the subring $A[z]$ is contained in $A[x, y]$, and so the statement follows from the implication (iii) $\Rightarrow$ (i) in Proposition 2.1.6. □

DEFINITION 2.1.9. Let R be a ring, and $A \subset R$ a subring. By Proposition 2.1.8 and Remark 2.1.2, the set of elements of R which are integral over A is a subring of R which contains A, called the *integral closure of A in R*. If A coincides with its integral closure in R, we say that A is *integrally closed* in R.

When A is a domain, the integral closure of A in its fraction field K is simply called the integral closure of A, and we say that A is integrally closed when it coincides with its integral closure.

DEFINITION 2.1.10. A *number field* is a field extension of $\mathbb{Q}$ having finite degree. When K is a number field, the integral closure of $\mathbb{Z}$ in K is called the *ring of integers* of K, and will be denoted by $\mathcal{O}_K \subset K$.

PROPOSITION 2.1.11. *Every principal ideal domain is integrally closed.*

PROOF. Let A be a principal ideal domain, with fraction field K. Let $x \in K$ be integral over A. So we have an equation in K

$$x^n + a_{n-1}x^{n-1} + \cdots + a_0 = 0, \tag{2.1.c}$$

with $a_0, \dots, a_{n-1} \in A$. Now we find elements $a, b \in A$ with $b \neq 0$ such that $x = ab^{-1}$. The ideal $aA + bA$ in the principal ideal domain A must be of the form dA, for some $d \in A$. In particular $a = da'$ and $b = db'$ for some $a', b' \in A$. Replacing (a, b) with (a', b'), we may assume that $d = 1$, which means that there exist $u, v \in A$ such that $au + bv = 1$. Multiplying (2.1.c) with b^n and using the relation $bx = a$, we obtain in $A \subset K$

$$a^n + a_{n-1}ba^{n-1} + \cdots + a_0b^n = 0,$$

and therefore

$$a^n = b(-a_{n-1}a^{n-1} - \cdots - a_0b^{n-1}).$$

Thus b divides a^n. It follows that b divides

$$a^n u^n = (au)^n = (1 - bv)^n = 1 \mod bA,$$

and thus b divides 1, which means that $b \in B^\times$. This implies that $a = ab^{-1} \in A \subset K$. □

Remark 2.1.12. In particular, it follows from Proposition 2.1.11 that the domain $\mathbb{Z}$ is integrally closed (in $\mathbb{Q}$), a fact the will be used repeatedly.

Definition 2.1.13. Let R be a ring, and $A \subset R$ a subring. If every element of R is integral over A, we say that R is *integral over* A, or that the extension $A \subset R$ is integral.

Example 2.1.14. Let k be a field and A a nonzero k-algebra. Then we claim that the associated morphism $\varphi\colon k \to A$ (mapping $\lambda \in k$ to $\lambda \cdot 1 \in A$) is injective. Indeed its kernel is an ideal of k, and there are only two such ideals in the field k, namely 0 and k. As 1 belongs to the image of φ, and $1 \neq 0$ as A is nonzero, the kernel of φ can only be zero. This proves the claim.

If in addition, the k-vector space A has finite dimension, then A is integral over k, by the second criterion of Proposition 2.1.6.

Proposition 2.1.15. *Let C be a ring, and $A \subset B \subset C$ subrings. If B is integral over A and C is integral over B, then C is integral over A.*

Proof. Let $x \in C$. As C is integral over B, we can find elements $b_0, \dots, b_{n-1} \in B$ such that

$$0 = x^n + b_{n-1}x^{n-1} + \cdots + b_0. \tag{2.1.d}$$

Let $A' = A[b_0, \dots, b_{n-1}] \subset B$. As B is integral over A, the elements $b_0, \dots, b_{n-1}$ are integral over A. Therefore by Corollary 2.1.7, the A-module A' is finitely generated. On the other hand, the relation (2.1.d) shows that x is integral over A', so that by the implication (i) ⇒ (ii) in Proposition 2.1.6 the A'-module $A'[x]$ is finitely generated. We conclude using Lemma 2.1.4 that the A-module $A'[x]$ is finitely generated. Since $A[x] \subset A'[x]$ it follows from the implication (iii) ⇒ (i) in Proposition 2.1.6 that x is integral over A. □

Lemma 2.1.16. *Let $A \subset R$ be a subring, and $\sigma\colon R \to S$ a ring morphism. Consider the subring $B = \sigma(A) \subset S$. If $x \in R$ is integral over A, then $\sigma(x) \in S$ is integral over B.*

Proof. If $P \in A[X]$ is a monic polynomial such that $P(x) = 0$, then its image $Q = \sigma(P) \in B[X]$ is a monic polynomial such that $Q(\sigma(x)) = 0$. □

Lemma 2.1.17. *Let $A \subset R$ be an integral ring extension. Then for any ideal J of R, the ring extension $A/(J \cap A) \subset R/J$ is integral.*

Proof. Consider the quotient morphism $\sigma\colon R \to R/J$. Then any element $y \in R/J$ is the image of some element $x \in R$ under σ. The element x is integral over A by assumption, hence it follows from Lemma 2.1.16 that $\sigma(x) = y$ is integral over $\sigma(A) = A/(J \cap A) \subset R/J$. □

Lemma 2.1.18. *Let $A \subset R$ be an integral ring extension. Assume that the ring R is a domain. Then for any nonzero ideal J of R, the ideal $J \cap A$ of A is nonzero.*

PROOF. Let $x \in J$ be a nonzero element. Since x is integral over A, we have

$$x^n + a_{n-1}x^{n-1} + \cdots + a_0 = 0, \quad \text{for some } a_0, \ldots, a_{n-1} \in A.$$

We may arrange that the integer $n \in \mathbb{N} \smallsetminus \{0\}$ is minimal among those appearing in such an equation (i.e. the integer n is the minimal degree of a monic polynomial with coefficients in A admitting x as a zero). If $a_0 = 0$, as R is a domain and $x \neq 0$, we obtain an equation

$$x^{n-1} + a_{n-1}x^{n-2} + \cdots + a_1 = 0,$$

which contradicts the minimality of the integer n. We thus have $a_0 \neq 0$. Then

$$a_0 = x(-x^{n-1} - a_{n-2}x^{n-2} - \cdots - a_1) \in xR \subset J$$

is a nonzero element of $J \cap A$. □

PROPOSITION 2.1.19. *Let $A \subset R$ be an integral ring extension. Assume that R is a domain. Then R is a field if and only if A is a field.*

PROOF. Assume that R is a field. Let $x \in A$. Then by assumption the element $x^{-1} \in R$ is integral over A, hence satisfies an equation of the form

$$x^{-n} + a_{n-1}x^{1-n} + \cdots + a_0 = 0,$$

with $a_0, \ldots, a_{n-1} \in A$. Multiplying with x^{1-n}, we obtain

$$x^{-1} = -a_{n-1} - \cdots - a_0 x^{n-1} \in R,$$

which visibly belongs to A. We have proved that A is a field.

Recall that a domain D is a field if and only if its only ideals are $0, D$. Assume that A is a field, and let J be a nonzero ideal of R. Then the ideal $I = J \cap R$ of A is nonzero by Lemma 2.1.18. As A is a field, we must have $I = A$. Then $1 \in J \cap A \subset J$, hence $J = R$. We have proved that R is a field. □

COROLLARY 2.1.20. *Let k be a field, and A a finite-dimensional k-algebra. Then every prime ideal of A is maximal.*

PROOF. Let $\mathfrak{p}$ be a prime ideal of A. Then the ring $A/\mathfrak{p}$ is nonzero by definition of a prime ideal, so that the ring morphism $k \to A/\mathfrak{p}$ is injective, and makes the ring $A/\mathfrak{p}$ integral over k (see Example 2.1.14). Therefore the ring $A/\mathfrak{p}$ is a field by Proposition 2.1.19, which means that the ideal $\mathfrak{p}$ is maximal. □

2. Integers in quadratic fields

When $\alpha \in \mathbb{C}$ and $K \subset \mathbb{C}$ is a subfield, we denote by $K(\alpha)$ the subset of $\mathbb{C}$ consisting of the elements $P(\alpha)/Q(\alpha)$, with $P, Q \in K[X]$, and $Q(\alpha) \neq 0$. Then $K(\alpha)$ is the smallest subfield of $\mathbb{C}$ containing α and K. When α is algebraic over K, then we have $K(\alpha) = K[\alpha]$.

DEFINITION 2.2.1. A *quadratic field* is a field extension of degree 2 of the field of rational numbers $\mathbb{Q}$. A quadratic field is called *real* if it admits an embedding into $\mathbb{R}$ as a subfield, and *imaginary* otherwise.

Examples of quadratic fields include the fields $\mathbb{Q}(\sqrt{d})$, where $d \in \mathbb{Z}$ is not a square.[1] This quadratic field is real if $d > 0$ and imaginary if $d < 0$.

[1] By $\sqrt{d}$ we denote one of the two elements of $\mathbb{C}$ whose square is d; this choice does not affect the field $\mathbb{Q}(\sqrt{d}) = \mathbb{Q}(-\sqrt{d})$.

We will say that an integer $d \in \mathbb{Z}$ is *square-free* when 1 is the only square dividing d. An equivalent condition is that either d or $-d$ can be written as a product of pairwise distinct primes.

Proposition 2.2.2. *Every quadratic field is isomorphic to $\mathbb{Q}(\sqrt{d})$ for some $d \in \mathbb{Z} \smallsetminus \{1\}$, where d is square-free.*

Proof. Let K be a quadratic field. Pick an element $x \in K \smallsetminus \mathbb{Q}$. Then x generates K as a $\mathbb{Q}$-algebra. Its minimal polynomial has degree 2 (its degree is at most 2 because $\dim_{\mathbb{Q}} K = 2$, and is not equal to 1 because $x \notin K$), hence we have an equation of the form

$$x^2 + bx + c = 0 \in \mathbb{Q}[X], \quad \text{with } b, c \in \mathbb{Q}. \tag{2.2.a}$$

Let $e = b^2 - 4c \in \mathbb{Q}$. Then (2.2.a) implies that

$$(2x + b)^2 = e.$$

In particular $\sqrt{e} \in K$, and moreover

$$x \in \left\{ \frac{-b + \sqrt{e}}{2}, \frac{-b - \sqrt{e}}{2} \right\} \subset \mathbb{Q}(\sqrt{e}).$$

We deduce that $K = \mathbb{Q}(\sqrt{e})$. Writing $e = u/v$ with $u, v \in \mathbb{Z}$, the element $f = v^2 e$ belongs to $\mathbb{Z}$. Then f may be written as $f = dg^2$, where $g \in \mathbb{Z}$ and d is square-free. Then $d = (v/g)^2 e$, so that $\mathbb{Q}(\sqrt{e}) = \mathbb{Q}(\sqrt{d})$. Note that the case $d = 1$ is excluded, as then $\mathbb{Q}(\sqrt{d}) = \mathbb{Q}$ is not a quadratic field. □

Theorem 2.2.3. *Let K be a quadratic field, and write $K = \mathbb{Q}(\sqrt{d})$ where $d \in \mathbb{Z} \smallsetminus \{1\}$ is square-free (see Proposition 2.2.2), and in particular $d \neq 0 \mod 4$. Then a $\mathbb{Z}$-basis of the ring of integers $\mathcal{O}_K$ (see Definition 2.1.10) is given by*

$$\begin{cases} (1, \sqrt{d}) & \text{if } d \text{ is congruent to } 2 \text{ or } 3 \text{ modulo } 4, \\ \left(1, \dfrac{1 + \sqrt{d}}{2}\right) & \text{if } d \text{ is congruent to } 1 \text{ modulo } 4. \end{cases}$$

Proof. The $\mathbb{Q}$-algebra K is isomorphic to $\mathbb{Q}[X]/(X^2 - d)$. In particular, every element of K is of the form $a + b\sqrt{d}$, for unique elements $a, b \in \mathbb{Q}$. Moreover, the morphism of $\mathbb{Q}$-algebras $\mathbb{Q}[X]/(X^2 - d) \to \mathbb{Q}[X]/(X^2 - d)$ given by $X \mapsto -X$ yields a morphism of $\mathbb{Q}$-algebras

$$\sigma \colon K \to K, \quad a + b\sqrt{d} \mapsto a - b\sqrt{d} \quad (\text{where } a, b \in \mathbb{Q}).$$

It follows that $\mathbb{Q} \subset K$ is the subset of elements fixed by the endomorphism $\sigma \colon K \to K$. In particular for any $x \in K$, the elements $x + \sigma(x)$ and $x\sigma(x)$ belong to $\mathbb{Q}$. If $x \in \mathcal{O}_K$, then $\sigma(x) \in \mathcal{O}_K$ by Lemma 2.1.16, and therefore (by Proposition 2.1.8) the elements $x + \sigma(x)$ and $x\sigma(x)$ are integral over $\mathbb{Z}$. Since $\mathbb{Z}$ is integrally closed (in $\mathbb{Q}$) by Remark 2.1.12, we deduce that $x + \sigma(x) \in \mathbb{Z}$ and $x\sigma(x) \in \mathbb{Z}$. In other words, if $a, b \in \mathbb{Q}$ are the elements such that $x = a + b\sqrt{d}$, we have

$$2a \in \mathbb{Z} \quad \text{and} \quad a^2 - db^2 \in \mathbb{Z}. \tag{2.2.b}$$

Conversely, assume that $a, b \in \mathbb{Q}$ satisfy the conditions given in (2.2.b). Then the element $a + b\sqrt{d} \in K$ is a root of the monic polynomial

$$X^2 - 2aX + (a^2 - db^2) \in \mathbb{Z}[X],$$

hence belongs to $\mathcal{O}_K$. We have proved that, for any $a, b \in \mathbb{Q}$

$$a + b\sqrt{d} \in \mathcal{O}_K \iff \text{(2.2.b)}.$$

Now the condition (2.2.b) implies that $4db^2 \in \mathbb{Z}$. Writing $2b = f/g$ with $f, g \in \mathbb{Z}$ relatively prime, we have $df^2 \in g^2\mathbb{Z}$, and so $d \in g^2\mathbb{Z}$ (as f^2 is prime to g^2). As d is square-free, we must have $g^2 = 1$, which implies that $2b \in \mathbb{Z}$. Therefore we may write $a = u/2$ and $b = v/2$ with $u, v \in \mathbb{Z}$, and The condition (2.2.b) becomes

$$u^2 - dv^2 \in 4\mathbb{Z}. \tag{2.2.c}$$

If u is even, the condition (2.2.c) implies that v is also even (recall that d is not divisible by 4, being square-free); then we have $a, b \in \mathbb{Z}$. If u is odd, then $u^2 = 1 \mod 4$ and thus (2.2.c) implies that

$$dv^2 = 1 \mod 4. \tag{2.2.d}$$

Thus the integer v^2 is not divisible by 4, and as observed in (0.a) this implies that $v^2 = 1 \mod 4$. In particular v is odd, and moreover the relation (2.2.d) implies that $d = 1 \mod 4$.

Conversely, assume that $d = 1 \mod 4$. If $u, v \in \mathbb{Z}$ have the same parity, then $u^2 - dv^2 = u^2 - v^2$ is divisible by 4 (see (0.a)), and so (2.2.c) holds. We have proved that

$$\mathcal{O}_K = \begin{cases} \{a + b\sqrt{d}, \text{ where } a, b \in \mathbb{Z}\} & \text{if } d = 2, 3 \mod 4, \\ \left\{ \dfrac{u + v\sqrt{d}}{2}, \text{ where } u, v \in \mathbb{Z} \text{ and } u = v \mod 2 \right\} & \text{if } d = 1 \mod 4. \end{cases}$$

The system $(1, \sqrt{d})$, resp. $(1, (1+\sqrt{d})/2)$, is $\mathbb{Z}$-linearly independent in K (being $\mathbb{Q}$-linearly independent), and is contained in $\mathcal{O}_K$ when d is congruent to 2 or 3 modulo 4, resp. 1 modulo 4. If $u, v \in \mathbb{Z}$ have the same parity, then

$$\frac{u + v\sqrt{d}}{2} = \frac{u - v}{2} + v\frac{1 + \sqrt{d}}{2}$$

is a $\mathbb{Z}$-linear combination of 1 and $(1 + \sqrt{d})/2$. This concludes the proof of the statement. □

CHAPTER 3

Trace, norm and discriminant

1. The characteristic polynomial

In this section, we consider a ring B and a subring $A \subset B$. We assume that the A-module B is free of rank $n \in \mathbb{N}$, in other words that there exists an isomorphism of A-modules $B \simeq A^{\oplus n}$.

DEFINITION 3.1.1. Let $b \in B$. Consider the morphism of A-modules

$$l_b \colon B \to B, \quad x \mapsto bx.$$

The *characteristic polynomial* of b is the polynomial[1]

$$\chi_{B/A}(b) = \det(X \operatorname{id}_B - l_b) \in A[X].$$

Observe that $\chi_{B/A}(b)$ is a monic polynomial of degree n with coefficients in A.

LEMMA 3.1.2. *If $\varphi \colon B \xrightarrow{\sim} B'$ is an isomorphism of A-algebras, then for any $b \in B$ we have*

$$\chi_{B/A}(b) = \chi_{B'/A}(\varphi(b)).$$

PROOF. Indeed we have $l_{\varphi(b)} = \varphi \circ l_b \circ \varphi^{-1}$, and the lemma follows from a standard property of the determinant. □

We recall that a element x of a ring R is called nilpotent if there exists an integer $n \in \mathbb{N}$ such that $x^n = 0$.

PROPOSITION 3.1.3. *Assume that the ring A is a domain. If $b \in B$ is a nilpotent element, then $\chi_{B/A}(b) = X^n$.*

PROOF. Assume that $b^{k+1} = 0$. Let $\varphi = l_b$, so that $\varphi^{k+1} = 0$. We have

$$(X \operatorname{id}_B - \varphi)(X^k \operatorname{id}_B + \varphi x^{k-1} + \cdots + \varphi^k) = X^{k+1} \operatorname{id}_B .$$

Taking the determinants, we deduce that $\chi_{B/A}(b) = \det(X \operatorname{id}_B - \varphi)$ divides $\det(X^{k+1} \operatorname{id}_B) = X^{n(k+1)}$. We conclude the proof using Lemma 3.1.4 below. □

LEMMA 3.1.4. *Let A be a domain, and $q \in \mathbb{N}$. Then the only monic polynomials dividing X^n in $A[X]$ are the polynomials X^k for $k \leq q$.*

PROOF. Assume that $X^q = PQ$ with $P, Q \in A[X]$. Then we may write

$$P = X^m(p_r X^r + \cdots + p_0) \quad \text{and} \quad P = X^{m'}(q_s X^s + \cdots + q_0),$$

where $p_0, \ldots, p_r, q_0, \ldots, q_s \in A$, and moreover $p_0 \neq 0$ and $q_0 \neq 0$. Then the $(X^{m+m'})$-coefficient of PQ is $p_0 q_0$. If either P or Q is not a power of X (i.e. if $r + s > 0$), we must

[1] We commit a slight abuse of notation, and use the same notation of endomorphisms of the A-module B and the induced endomorphisms of the $A[X]$-module $B[X]$.

have $p_0 q_0 = 0$ (because $PQ = X^q = X^{m+m'+r+s}$). Since the ring A is a domain, this implies that $p_0 = 0$ or $q_0 = 0$, a contradiction. □

Lemma 3.1.5. *Let B_1, B_2 be rings such that $A \subset B_1$ and $A \subset B_2$. Assume that B_1, B_2 are free of respective ranks $n_1, n_2 \in \mathbb{N}$ as A-modules. Then the A-algebra $B_1 \times B_2$ is free of rank $n_1 + n_2$ as an A-module, and for any $b_1 \in B_2$ and $b_2 \in B_2$, we have*

$$\chi_{(B_1 \times B_2)/A}((b_1, b_2)) = \chi_{B_1/A}(b_1) \cdot \chi_{B_2/A}(b_2).$$

Proof. If $(e_1, \dots, e_{n_1})$ is an A-basis of B_1 and $(f_1, \dots, f_{n_2})$ an A-basis of B_2, then

$$((e_1, 0), \dots, (e_{n_1}, 0), (0, f_1), \dots, (0, f_{n_2})) \tag{3.1.a}$$

is an A-basis of $B_1 \times B_2$. Let $M_1 \in M_{n_1}(A), M_2 \in M_{n_2}(A)$ be the matrices of l_{b_1}, l_{b_2} in the above basis of B_1, B_2. Then the matrix of $l_{(b_1, b_2)}$ in the basis (3.1.a) of $B_1 \times B_2$ is the block matrix

$$M = \begin{pmatrix} M_1 & 0 \\ 0 & M_2 \end{pmatrix} \in M_{n_1+n_2}(A)$$

and the properties of determinant of block matrices show that, denoting by $I_k \in M_k(A)$ the identity matrix,

$$\det(XI_{n_1+n_2} - M) = \det(XI_{n_1} - M_1) \cdot \det(XI_{n_2} - M_2),$$

which gives the required formula. □

Proposition 3.1.6 (Cayley–Hamilton Theorem). *For any $b \in B$ we have*

$$\big(\chi_{B/A}(b)\big)(b) = 0.$$

Proof. Let $(e_1, \dots, e_n)$ be an A-basis of B. Let us write for $i = 1, \dots, n$

$$be_i = \sum_{j=1}^{n} b_{ij} e_j, \quad \text{with } b_{ij} \in A. \tag{3.1.b}$$

Then $(b_{ij}) \in M_n(A)$ is the matrix of the endomorphism l_b in the above A-basis of B. Let us consider the matrix (using the notation of (1.3.b))

$$N = (\delta_{ij} b - b_{ij}) \in M_n(B).$$

The equation (3.1.b) asserts that the column vector $(e_1, \dots, e_n) \in B^n$ belongs to the kernel of N. Since $(e_1, \dots, e_n)$ is an A-basis of B, the element 1 is an A-linear combination of the elements $e_1, \dots, e_n$, and in particular a B-linear combination of those. It thus follows from Lemma 2.1.5 that $\det N = 0 \in B$. On the other hand, we have

$$\chi_{B/A}(b) = \det(\delta_{ij} X - b_{ij}) \in A[X].$$

This formula also holds in $B[X]$ (here we use that the following fact: if $M \in M_n(A[X])$ has image $M' \in M_n(B[X])$, then $\det M' \in B[X]$ is the image of $\det M \in A[X]$). Evaluating at $b \in B$ shows that $\chi_{B/A}(b)(b) = \det N \in B$, and we have seen above that this element vanishes. □

Two particular coefficients of the characteristic polynomial will be especially significant:

DEFINITION 3.1.7. We define the *norm* and *trace* of an element $b \in B$ as the determinant and trace of the endomorphism l_b of the free A-module B of rank n (see Definition 3.1.1):

$$\mathrm{N}_{B/A}(b) = \det(l_b) \in A \quad \text{and} \quad \mathrm{Tr}_{B/A}(b) = \mathrm{Tr}(l_b) \in A.$$

LEMMA 3.1.8. *For $b \in B$, let us write*

$$\chi_{B/A}(b) = X^n + a_{n-1}X^{n-1} + \cdots + a_0 \in A[X],$$

where $a_0, \ldots, a_{n-1} \in A$. Then

$$\mathrm{N}_{B/A}(b) = (-1)^n a_0 \quad \textit{and} \quad \mathrm{Tr}_{B/A}(b) = -a_{n-1}.$$

PROOF. Let us choose a basis of the A-module B consisting of n elements of B, and denote by $b_{ij} \in A$ the coefficients of the matrix of the endomorphism l_b in that basis. Then (using the notation of (1.3.b))

$$\chi_{B/A}(b) = \det(\delta_{ij}X - b_{ij}) \in A[X].$$

Then we set $m_{ij} = \delta_{ij}X - b_{ij} \in A[X]$, and consider the formula (where $\mathfrak{S}_n$ denotes the symmetric group on n elements, and $\mathrm{sgn}\colon \mathfrak{S}_n \to \{1, -1\}$ is the signature morphism)

$$\det(m_{ij}) = \sum_{\sigma \in \mathfrak{S}_n} \mathrm{sgn}(\sigma) m_{1\sigma(1)} \cdots m_{n\sigma(n)} \in A[X]. \tag{3.1.c}$$

This polynomial has constant coefficient

$$\sum_{\sigma \in \mathfrak{S}_n} \mathrm{sgn}(\sigma)(-b_{1\sigma(1)}) \cdots (-b_{n\sigma(n)}) = (-1^n)\det(b_{ij}) \in A.$$

In the formula (3.1.c), the term $\mathrm{sgn}(\sigma)m_{1\sigma(1)} \cdots m_{n\sigma(n)}$ can contribute to the X^{n-1}-coefficient only when $\sigma(i) = i$ for at least $n-1$ values of $i \in \{1, \ldots, n\}$, in which case we must also have $\sigma(i) = i$ for the single remaining value of i, and so $\sigma = \mathrm{id}$. Therefore the X^{n-1}-coefficient of (3.1.c) coincides with the X^{n-1}-coefficient of the polynomial

$$\prod_{i=1}^{n} m_{ii} = \prod_{i=1}^{n} (X - b_{ii}) \in A[X],$$

and is thus equal to

$$\sum_{i=1}^{n} (-b_{ii}) = -\mathrm{Tr}(l_b) \in A. \qquad \square$$

PROPOSITION 3.1.9. *The following hold:*

(i) We have

$$\mathrm{Tr}_{B/A}(0) = 0 \quad \textit{and} \quad \mathrm{N}_{B/A}(1) = 1.$$

(ii) For any $x, y \in B$, we have

$$\mathrm{Tr}_{B/A}(x+y) = \mathrm{Tr}_{B/A}(x) + \mathrm{Tr}_{B/A}(y) \quad \textit{and} \quad \mathrm{N}_{B/A}(xy) = \mathrm{N}_{B/A}(x)\,\mathrm{N}_{B/A}(y).$$

(iii) For any $a \in A$, we have $\chi_{B/A}(a) = (X-a)^n$. In particular

$$\mathrm{Tr}_{B/A}(a) = na \quad \textit{and} \quad \mathrm{N}_{B/A}(a) = a^n.$$

PROOF. (i) and (ii) are clear from the definitions.

(iii) : This follows from the fact that, in any A-basis of B, the matrix of $l_a\colon B \to B$ is diagonal with coefficients $(a, \ldots, a)$. $\square$

Lemma 3.1.10. *For any $b \in B$, we have*

$$b \in B^\times \iff \mathrm{N}_{B/A}(b) \in A^\times.$$

Proof. It follows from Proposition 3.1.9 (i) and (ii) that $\mathrm{N}_{B/A}(b) \in A^\times$ when $b \in B^\times$. Conversely if $\mathrm{N}_{B/A}(b) \in A^\times$, the morphism of A-modules $l_b \colon B \to B$ has invertible determinant, hence is bijective. Its surjectivity yields an element $c \in B$ such that $bc = 1$, which shows that $b \in B^\times$. □

Remark 3.1.11. It follows from Proposition 3.1.9 and Lemma 3.1.10 that the norm map induces a group morphism

$$\mathrm{N}_{B/A} \colon B^\times \to A^\times.$$

2. The discriminant

In this section B will be a ring and $A \subset B$ a subring such that the A-module B is free of rank $n \in \mathbb{N}$.

Definition 3.2.1. The *discriminant* of a system $(x_1, \dots, x_n) \in B^n$ is defined as the element

$$\mathrm{D}_{B/A}(x_1, \dots, x_n) = \det(\mathrm{Tr}_{B/A}(x_i x_j)) \in A,$$

where (i, j) runs over $\{1, \dots, n\}^2$.

Lemma 3.2.2. *Assume that $(e_1, \dots, e_n)$ is an A-basis of B. Let $\varphi \colon B \to B$ be a morphism of A-modules. Then*

$$\mathrm{D}_{B/A}(\varphi(e_1), \dots, \varphi(e_n)) = (\det \varphi)^2 \cdot \mathrm{D}_{B/A}(e_1, \dots, e_n).$$

Proof. Let us denote by $a_{ij} \in A$ for $1 \leq i, j \leq n$ the coefficients of the matrix of φ in the basis $(e_1, \dots, e_n)$. Then

$$\mathrm{Tr}(\varphi(e_i)\varphi(e_j)) = \mathrm{Tr}\Big(\Big(\sum_{p=1}^n a_{pi} e_p\Big)\Big(\sum_{q=1}^n a_{qj} e_q\Big)\Big) = \sum_{p,q=1}^n a_{pi} a_{qj} \,\mathrm{Tr}(e_p e_q).$$

We thus have equalities between matrices in $M_n(A)$

$$(\mathrm{Tr}(\varphi(e_i)\varphi(e_j))) = (a_{pi}) \cdot (\mathrm{Tr}(e_p e_q)) \cdot {}^t(a_{qj}),$$

where ${}^tM$ denotes the transpose of the matrix M. Taking determinants yields the statement (as transposing a matrix does not change its determinant). □

Definition 3.2.3. The *discriminant ideal* $\mathfrak{D}_{B/A}$ is defined as the ideal of A generated by the elements $\mathrm{D}_{B/A}(x_1, \dots, x_n)$, where $(x_1, \dots, x_n)$ runs over B^n.

Proposition 3.2.4. *Assume that $\mathfrak{D}_{B/A} \neq 0$ and that the ring A is a domain. Then a system $(x_1, \dots, x_n) \in B^n$ is an A-basis of B if and only if the element $\mathrm{D}_{B/A}(x_1, \dots, x_n)$ generates the ideal $\mathfrak{D}_{B/A}$ in A.*

Proof. Let $(e_1, \dots, e_n)$ be an A-basis of B. Then there exists an A-linear map $\varphi \colon B \to B$ such that $\varphi(e_i) = x_i$ for all $i \in \{1, \dots, n\}$, and by Lemma 3.2.2 we have

$$\mathrm{D}_{B/A}(x_1, \dots, x_n) = (\det \varphi)^2 \cdot \mathrm{D}_{B/A}(e_1, \dots, e_n). \tag{3.2.a}$$

As $(\det \varphi)^2 \in A$, this implies that the element $\mathrm{D}_{B/A}(e_1, \dots, e_n)$ generates the ideal $\mathfrak{D}_{B/A}$ in A, proving one implication.

Now let $d = \mathrm{D}_{B/A}(x_1, \dots, x_n)$, and assume that d generates the ideal $\mathfrak{D}_{B/A}$ in A. Then $\mathrm{D}_{B/A}(e_1, \dots, e_n) = ad$ for some $a \in A$, hence (3.2.a) yields $d = (\det \varphi)^2 ad$. Now $d \neq 0$ (because by the ideal $\mathfrak{D}_{B/A}$ is nonzero by assumption), and as A is assumed to be a domain, we deduce that $1 = (\det \varphi)^2 a$. Therefore the element $\det \varphi$ is invertible in A. Thus φ is an isomorphism of A-modules, and so $(x_1, \dots, x_n)$ is an A-basis of B, being the image under φ of an A-basis of B. □

The following complement is sometimes useful to study integers in number fields:

LEMMA 3.2.5. *Assume that $A = \mathbb{Z}$, and let $(x_1, \dots, x_n) \in B^n$ be a system such that the integer $\mathrm{D}_{B/\mathbb{Z}}(x_1, \dots, x_n) \in \mathbb{Z}$ is square-free. Then $(x_1, \dots, x_n)$ is a $\mathbb{Z}$-basis of B.*

PROOF. Indeed, let $(e_1, \dots, e_n)$ be a $\mathbb{Z}$-basis of B. Then there exists a morphism of $\mathbb{Z}$-modules $\varphi\colon B \to B$ such that $\varphi(e_i) = x_i$ for each $i \in \{1, \dots, n\}$. By Lemma 3.2.2 we have

$$\mathrm{D}_{B/\mathbb{Z}}(x_1, \dots, x_n) = \det(\varphi)^2 \cdot \mathrm{D}_{B/\mathbb{Z}}(e_1, \dots, e_n).$$

As this integer is assumed to be square-free, we must have $\det(\varphi) \in \{1, -1\} = \mathbb{Z}^\times$, and thus φ is an isomorphism. This implies that $(x_1, \dots, x_n)$ is a $\mathbb{Z}$-basis of B. □

REMARK 3.2.6. Lemma 3.2.5 merely provides a sufficient condition for a given system to be a $\mathbb{Z}$-basis, which is not always necessary, as shown by Example 3.2.7 below.

EXAMPLE 3.2.7. Let $K = \mathbb{Q}(\sqrt{d})$, with $d \in \mathbb{Z} \smallsetminus \{1\}$ square-free. We set $A = \mathbb{Z}$ and $B = \mathcal{O}_K$. Let us compute the discriminant d_K of the $\mathbb{Z}$-basis of $\mathcal{O}_K$ given by Theorem 2.2.3.

Assume that d is congruent to 2 or 3 modulo 4. Then a $\mathbb{Z}$-basis of $\mathcal{O}_K$ is given by $(x_1, x_2) = (1, \sqrt{d})$. We have

$$\mathrm{Tr}(l_1) = \mathrm{Tr}\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = 2, \quad \mathrm{Tr}(l_{\sqrt{d}}) = \mathrm{Tr}\begin{pmatrix} 0 & d \\ 1 & 0 \end{pmatrix} = 0, \quad \mathrm{Tr}(l_d) = \mathrm{Tr}\begin{pmatrix} d & 0 \\ 0 & d \end{pmatrix} = 2d,$$

so that

$$\mathrm{Tr}_{\mathcal{O}_K/\mathbb{Z}}(x_i x_j) = \begin{pmatrix} \mathrm{Tr}(l_1) & \mathrm{Tr}(l_{\sqrt{d}}) \\ \mathrm{Tr}(l_{\sqrt{d}}) & \mathrm{Tr}(l_d) \end{pmatrix} = \begin{pmatrix} 2 & 0 \\ 0 & 2d \end{pmatrix}.$$

Taking determinants we obtain $d_K = 4d$.

Assume now that $d = 1 \mod 4$, and let $e \in \mathbb{Z}$ be the integer such that $d - 1 = 4e$. Then a $\mathbb{Z}$-basis of $\mathcal{O}_K$ is given by $(x_1, x_2) = (1, \alpha)$, where $\alpha = (1 + \sqrt{d})/2$. We have

$$\alpha^2 = \frac{(1 + \sqrt{d})^2}{4} = \frac{d-1}{4} + \frac{1 + \sqrt{d}}{2} = e + \alpha$$

and thus

$$\alpha^3 = e\alpha + \alpha^2 = e + (e+1)\alpha.$$

We have

$$\mathrm{Tr}(l_1) = \mathrm{Tr}\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = 2, \quad \mathrm{Tr}(l_\alpha) = \mathrm{Tr}\begin{pmatrix} 0 & e \\ 1 & 1 \end{pmatrix} = 1, \quad \mathrm{Tr}(l_{\alpha^2}) = \mathrm{Tr}\begin{pmatrix} e & e \\ 1 & e+1 \end{pmatrix} = 2e+1,$$

hence

$$\mathrm{Tr}_{\mathcal{O}_K/\mathbb{Z}}(x_i x_j) = \begin{pmatrix} \mathrm{Tr}(l_1) & \mathrm{Tr}(l_\alpha) \\ \mathrm{Tr}(l_\alpha) & \mathrm{Tr}(l_{\alpha^2}) \end{pmatrix} = \begin{pmatrix} 2 & 1 \\ 1 & 2e+1 \end{pmatrix}.$$

Taking determinants yields $d_K = 4e + 1 = d$.

CHAPTER 4

Étale algebras

1. Separable field extensions

When k is a field, recall that a *k-algebra* is a ring A together with a ring morphism $\iota_A\colon k \to A$. A morphism of k-algebras $\varphi\colon A \to B$ is a ring morphism such that $\varphi \circ \iota_A = \iota_B$.

When a k-algebra F is a field, we say that F/k is a *field extension*. Note that in this case the ring morphism $k \to F$ is automatically injective, and so we will view k as a subfield of F.

Definition 4.1.1. A field extension F/k is called *finite*, or *of finite degree*, if the inclusion $k \subset F$ makes F a finite-dimensional k-vector space. The *degree* of the extension is $\dim_k L$, denoted $[L : k]$.

Remark 4.1.2. If the field extensions F/k and L/F are both finite, then so is L/k, and

$$[L : k] = [L : F][F : k].$$

Definition 4.1.3. Let F/k be a field extension. An element $x \in F$ is called *algebraic over k* if it is the root of a nonzero polynomial with coefficients in k. The extension F/k is called *algebraic* when all elements of F are algebraic over k.

Note that a field extension F/k is algebraic if and only if the ring F is integral over its subring k.

Remark 4.1.4. A finite field extension F/k is always algebraic. Indeed, if $x \in F$, then the family $x^i, i \in \mathbb{N}$ is linearly dependent over k (as $\dim_k F < \infty$), which provides a nonzero polynomial in $k[X]$ having x as a root. (Alternatively this follows from Example 2.1.14.) There exist algebraic extensions which are not finite.

Lemma 4.1.5. *Let $P \in k[X]$ be an irreducible polynomial, and set $F = k[X]/P$. Then F is a field and $[F : k] = \deg P$.*

Proof. Let $d = \deg P$, and $x \in F$ the class of X. A k-basis of F is given by $1, x, \ldots, x^{d-1}$, and so $\dim_k F = d$. As P is irreducible, it follows that the ring F is a domain. The ring extension $k \subset F$ is integral by Example 2.1.14, hence F is a field by Proposition 2.1.19. □

Definition 4.1.6. When F/k is a field extension and $x \in F$ is algebraic over k, the *minimal polynomial of x over k* is the unique monic generator of the ideal of polynomial P in $k[X]$ such that $P(x) = 0 \in F$.

Remark 4.1.7. Let F/k be a field extension, and $x \in F$ an algebraic element. Let $P \in k[X]$ be the minimal polynomial of x over k. Then $X \mapsto x$ induces an isomorphism of k-algebras $k[X]/P \simeq k[x]$. Since the ring $k[x]$ is a domain (being contained in the field

F), so is the ring $k[X]/P$, which implies that the polynomial P is irreducible. Thus by Lemma 4.1.5 the subalgebra $k[x] \subset F$ is a field. We will call the field extension $k[x]/k$ the subextension of F/k generated by x.

PROPOSITION 4.1.8. *Let k be a field and $P_1, \dots, P_n \in k[X]$ be monic polynomials. Then there exists a field extension L/k of finite degree such that each polynomial $P_1, \dots, P_n$ splits into linear factors in $L[X]$.*

PROOF. We proceed by induction on $d = (\deg P_1) + \cdots + (\deg P_n)$ (allowing k to vary). The proposition is clear if $d = 0$, so we assume that $d \geq 1$. Then $\deg P_j > 0$ for some $j \in \{1, \dots, n\}$, and we let Q be an irreducible factor of P_j. Consider k-algebra $E = k[Y]/Q(Y)$. Then E/k is a field extension of finite degree by Lemma 4.1.5. The polynomial P_j has a root in E, namely (the class of) Y. Thus $P_j = (X - Y)R_j$ in $E[X]$ for some polynomial $R_j \in E[X]$. Setting $R_i = P_i \in E[X]$ for every $i \in \{1, \dots, n\} \smallsetminus \{j\}$, we have

$$(\deg R_1) + \cdots + (\deg R_n) = d - 1,$$

and so by induction we may find a field extension L/E of finite degree where each R_i splits into linear factors. Then each P_i splits into linear in $L[X]$, completing the proof. □

PROPOSITION 4.1.9. *Let E/k be a field extension, and L/k a field extension of finite degree. Then there exist a field extension F/E of finite degree, and a morphism of k-algebras $L \to F$.*

PROOF. We proceed by induction on the degree $[L : k]$, the case $[L : k]$ being clear. Assume that $L \neq k$, and pick $x \in L \smallsetminus k$. Let K/k be the subextension of L/k generated by x. Then x is the root of an irreducible polynomial $P \in k[X]$ (its minimal polynomial over k, recall that the field extension L/k is assumed to be of finite degree), and the k-algebra K isomorphic to $k[X]/P$. If Q is any irreducible divisor of P in $E[X]$, then $E' = E[Y]/Q(Y)$ is a field extension of E having finite degree (Lemma 4.1.5), which admits a morphism of k-algebras $K \to E'$ (corresponding to $X \mapsto Y$). By induction, we find a field extension F/E' of finite degree and a morphism of K-algebras $L \to F$, concluding the proof. □

DEFINITION 4.1.10. Let k be a field. A polynomial $P \in k[X]$ is called *separable* if, for every field extension L/k, the polynomial $P \in L[X]$ has no multiple root in L.

A field extension F/k is called *separable* if every element of F is the root of an irreducible separable polynomial with coefficients in k. In particular, a separable extension is algebraic by definition.[1]

Note that an algebraic extension is separable if and only if the minimal polynomial of every element is separable.

REMARK 4.1.11. It follows from the definition that any subextension of a separable extension is separable. In addition, if F/k is separable field extension and E/k a subextension of F/k, then the extension F/E is separable: indeed the minimal polynomial over E of an element of F divides its minimal polynomial over k, and so must be separable.

LEMMA 4.1.12. *An irreducible polynomial $P \in k[X]$ is separable if and only if its derivative $P' \in k[X]$ is nonzero.*

[1]There exist more sophisticated definitions of separability, which apply to non-algebraic extensions.

PROOF. First, let F/k be a field extension, and $a \in F$ be such that $P(a) = 0$. Write $P = (X-a)R$, with $R \in F[X]$. Then $P' = R+(X-a)R'$, and so $P'(a) = R(a)$. Therefore

$$a \text{ is a multiple root of } P \iff (P(a) = 0 \text{ and } P'(a) = 0). \tag{4.1.a}$$

Assume now that $P' \neq 0$. Let $Q \in k[X]$ be the greatest common divisor of P and P' in $k[X]$, that is the monic generator of the ideal generated by P and P' in $k[X]$. As P' is nonzero and $Q \mid P'$, we have $\deg Q \leq \deg P' < \deg P$. As P is irreducible and divisible by Q, we must have $Q = 1$. Therefore there exist $U, V \in k[X]$ such that $1 = UP + VP'$. If F/k is a field extension, and $a \in F$ a multiple root of P, then a is root of P' by (4.1.a), so that

$$1 = (UP + VP')(a) = U(a)P(a) + V(a)P'(a) = 0,$$

a contradiction which proves that P is separable.

Conversely assume that P is separable. As P is nonconstant (being irreducible), by Proposition 4.1.8 we may find a field extension F/k, and an element $a \in F$ such that $P(a) = 0$. Then $P'(a) \neq 0$ by (4.1.a), and in particular the polynomial $P' \in k[X]$ is nonzero. □

DEFINITION 4.1.13. A field k is called *perfect* if every finite field extension of k is separable. An equivalent condition is that every irreducible polynomial in $k[X]$ is separable.

PROPOSITION 4.1.14. *Every field of characteristic zero is perfect.*

PROOF. Let k be a field of characteristic zero, and let $P \in k[X]$ be an irreducible polynomial, of degree $n > 1$. Then we write

$$P = a_n X^n + \cdots + a_0, \quad \text{with } a_0, \ldots, a_n \in k,$$

and $a_n \neq 0$. Then

$$P' = n a_n X^{n-1} + \cdots + a_1.$$

As $n \neq 0$ in k (because k has characteristic zero), we deduce that $P' \neq 0$. The proposition thus follows from Lemma 4.1.12. □

PROPOSITION 4.1.15. *Every finite field is perfect.*

PROOF. Let k be a finite field. Then k has characteristic p, when $p > 0$ is a prime number. Let us first recall that if A is any ring where $p = 0$, we have

$$(a + b)^p = a^p + b^p \quad \text{for any } a, b \in A. \tag{4.1.b}$$

(Observe that the binomial coefficients $\binom{p}{i}$ are all divisible by p when $1 < i < p$.)

Let $P \in k[X]$ be an irreducible polynomial such that $P' = 0$. If $a_m \in k$ is the X^m-th coefficient of P, then $m a_m$ is the X^{m-1}-th coefficient of P'. When m is not divisible by p, we have $m \neq 0$ in k and thus $a_m = 0$. Therefore we may $P = B(X^p)$, for some $B \in k[Y]$. Let us write

$$B = b_r Y^r + \cdots + b_0, \quad \text{with } b_0, \ldots, b_r \in k.$$

In view of (4.1.b) (applied to $A = k$), the Frobenius map $\phi\colon k \to k$ given by $x \mapsto x^p$ is a group morphism. As $x^p = 0$ implies $x = 0$ in the field k, the morphism ϕ is injective. But the set k is finite, hence the map ϕ must also be surjective. Thus we can find elements $c_0, \ldots, c_r \in k$ such that $c_i^p = b_i$ for all $i = 0, \ldots, r$. Consider the polynomial

$$C = c_r X^r + \cdots + c_0 \in k[X].$$

Then $C(X)^p = B(X^p) = P$ by (4.1.b) (applied in the ring $A = k[X]$), which contradicts the fact the P is irreducible.

We have proved that every irreducible polynomial in $k[X]$ has a nonzero derivative, and we deduce the proposition from Lemma 4.1.12. □

We now come to a crucial property of separable extensions:

Proposition 4.1.16. *Let F/k be a finite separable field extension, and set $n = [F : k]$. Then there exists a finite field extension ℓ/k and n pairwise distinct morphisms of k-algebras $\sigma_1, \dots, \sigma_n \colon F \to \ell$.*

Proof. We proceed by induction on the integer n. The case $n = 1$ is clear, so we assume that $n > 1$, or equivalently $F \neq k$. Since F/k contains no infinite increasing chain of subextensions (such chains are in particular chains of k-subspaces, and F is finite-dimensional over k), we may find a subextension $E \subset F$ and an element $x \in F \smallsetminus E$ such that $F = E[x]$ (recall from Remark 4.1.7 that $E[x]$ is a field). Let $P \in E[X]$ be the minimal polynomial of x over E. Since the field extension F/E is separable by Remark 4.1.11, the polynomial P is separable. Mapping X to x induces an isomorphism of E-algebras $E[X]/P \simeq F$. Recall that the extension E/k is separable (Remark 4.1.11), and its degree $m = [E : k]$ satisfies $m < [F : k]$ because $E \neq F$. Therefore by induction we may find a field extension ℓ'/k of finite degree, and m distinct morphisms of k-algebras $\sigma'_1, \dots, \sigma'_m \colon E \to \ell'$.

For each $i \in \{1, \dots, n\}$ the polynomial $\sigma'_i(P) \in \ell'[X]$ is separable, being the image of the separable polynomial P under the field extension ℓ'/k given by σ'_i. By Proposition 4.1.8, we may find a field extension ℓ/ℓ' of finite degree such that each polynomial $\sigma'_i(P) \in \ell'[X]$ splits into linear factors in $\ell[X]$, which are pairwise distinct since $\sigma'_i(P)$ is separable.

For each $i \in \{1, \dots, m\}$, the extensions of the composite $E \xrightarrow{\sigma'_i} \ell' \subset \ell$ to a morphism of k-algebras $F \to \ell$ are in bijection with the roots of $\sigma'_i(P)$ in ℓ (because $F \simeq E[X]/P$), of which there are exactly $\deg P = [F : k]$, because the polynomial $\sigma'_i(P)$ is separable over . We have thus found $m[F : k] = n$ morphisms of k-algebras $F \to \ell$, as required. □

Bibliography

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