

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

Foreword	1
Introduction	5
Chapter 1. Basic commutative ring theory	9
1. Prime and maximal ideals	9
2. Noetherian rings	11
3. Modules over principal ideal domains	13
Chapter 2. Integral extensions	19
1. Integral dependence	19
2. Integers in quadratic fields	23
Chapter 3. Trace, norm and discriminant	27
1. The characteristic polynomial	27
2. The discriminant	30
Chapter 4. Étale algebras	33
1. Separable field extensions	33
2. Étale algebras over a field	37
3. Extension of scalars	38
4. The trace form	42
Chapter 5. The ring of integers	45
1. Integral closure in a separable extension	45
2. Irreducibility of polynomials	48
3. Cyclotomic fields	49
Bibliography	53

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

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

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 $\mathbb{C} \rightarrow \mathbb{N}, \alpha \mapsto |\alpha|^2$, namely:

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

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

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

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 $N(\alpha) = 1$.*

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

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

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

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

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

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

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

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

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

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

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

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

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 $\beta \in I$ such that $N(\beta) \in \mathbb{N} \setminus \{0\}$ is minimal. Then for any $\alpha \in I$, by Lemma 0.6 we may write $\alpha = \gamma\beta + \rho$ with $\gamma, \rho \in \mathbb{Z}[i]$ and $N(\rho) < N(\beta)$. By minimality of $N(\beta)$, 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

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

Since by Lemma 0.2 we have $N(\alpha) \neq 1$ and $N(\beta) \neq 1$, and as p is prime, we must have $p = N(\alpha)$. 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

$$(0.a) \quad x^2 = \begin{cases} 0 & \text{mod } 4 \quad \text{if } x \equiv 0 \pmod{2}, \\ 1 & \text{mod } 4 \quad \text{if } x \equiv 1 \pmod{2}. \end{cases}$$

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

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

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

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 $\iota_R: A \rightarrow R$. When R, S are A -algebra, a ring morphism $f: R \rightarrow S$ 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

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

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 $A/(\mathfrak{q} \cap A) \rightarrow B/\mathfrak{q}$ 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 . \square

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. \square

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 $I \subset \mathfrak{p}_1 \cup \dots \cup \mathfrak{p}_n$, 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 . \square

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*

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

(ii) *The natural ring morphism*

$$A/(I_1 \cdots I_n) \rightarrow (A/I_1) \times \dots \times (A/I_n)$$

is bijective.

PROOF. (i): Clearly $I_1 \cdots I_n \subset I_1 \cap \dots \cap I_n$. 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

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

proving (i) for $n = 2$. Assume now that $n \geq 3$. Let $I = I_1 \cdots I_{n-1}$. By induction, we know that $I = I_1 \cap \dots \cap I_{n-1}$. 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

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

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

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

(ii): Consider the natural ring morphism

$$(1.1.a) \quad A \rightarrow (A/I_1) \times \dots \times (A/I_n) \quad a \mapsto (a \pmod{I_1}, \dots, a \pmod{I_n}).$$

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

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

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

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

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

2. Noetherian rings

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

- (i) *every nonempty family of A -submodules of M admits a maximal element (for the relation of inclusion),*
- (ii) *if P_n for $n \in \mathbb{N}$ are A -submodules of M satisfying $P_n \subset P_{n+1}$ for all n , there exists $s \in \mathbb{N}$ such that $P_n = P_s$ for all $n \geq s$,*
- (iii) *every A -submodule of M is finitely generated.*

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

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

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

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 $f: M \rightarrow P$ 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 $\pi: M \oplus N \rightarrow N$. 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

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

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. \square

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, \dots, x_n be a set of generators for the A -module M . We define a morphism of A -modules $A^{\oplus n} \rightarrow M$ 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 1.2.4 (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. \square

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. \square

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 . \square

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 $\Phi \neq \emptyset$ 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 $x, y \in A \setminus I$ 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. \square

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 $\Phi \neq \emptyset$ 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 $\mathcal{M}(A) = \emptyset$ is finite. Thus we may find $x, y \in A \setminus J$ 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. \square

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

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

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 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 $f: A^{\oplus n} \rightarrow M$, 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 $\varphi: M \xrightarrow{\sim} (A/a_1 A) \oplus \cdots \oplus (A/a_n A)$. 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 $\varphi: G \xrightarrow{\sim} (\mathbb{Z}/a_1 \mathbb{Z}) \times \cdots \times (\mathbb{Z}/a_n \mathbb{Z})$, 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 $\text{card } G \leq m$. 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. \square

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 \tilde{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 $x \in \tilde{N}$, 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 $a = b_1 \cdots b_s$. \square

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

$$(1.3.a) \quad r(N) = \dim_K \tilde{N}.$$

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 \tilde{N} . Assume that $\lambda_1, \dots, \lambda_m \in K$ are such that

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

Letting $b \in A \setminus \{0\}$ 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 $b\lambda_1 = \dots = b\lambda_m = 0$ in A , and thus in K . As $b \neq 0$, we obtain

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

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 $\widetilde{N_1 \oplus N_2} = \widetilde{N_1} + \widetilde{N_2}$. 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 $x = a^{-1}ax = 0 \in V$. \square

We will denote by $\text{Hom}_A(F, A)$ the set of morphisms of A -modules $F \rightarrow A$. Let us choose $\varphi \in \text{Hom}_A(F, A)$ 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, \dots, x_n) of F . Let $\pi_1, \dots, \pi_n \in \text{Hom}_A(F, A)$ 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*:

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

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

$$(1.3.c) \quad \alpha \neq 0.$$

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 $\psi \in \text{Hom}_A(F, A)$, 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 $\rho = u\psi + v\varphi \in \text{Hom}_A(F, A)$, 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. \square

Lemma 1.3.10 implies in particular that for each $i \in \{1, \dots, n\}$, 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 $Ae' \cap (M \cap \ker \varphi) = 0$. \square

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 . \square

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 $(a_2 e_2, \dots, a_q e_q)$ 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 $(a_1 e_1, \dots, a_q e_q)$ 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 $\xi \in \text{Hom}_A(F, A)$ 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 $\xi(a_2 e_2) = a_2 \in \xi(M)$, we have $a_1 = \alpha \mid a_2$. This concludes the proof of Theorem 1.3.2. \square

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 the 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, \dots, a_qe_q) is an A -basis of M , then M is free of rank q . \square

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 $a_0, \dots, a_{n-1} \in A$ such that

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

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, \dots, b_n) be a finite system of generators for the A -module B , and (m_1, \dots, 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 $a_n x^n + \dots + a_0$, where $a_0, \dots, a_n \in A$. We warn the reader that, despite the notation, the ring $A[x]$ depends on the extension $A \subset R$, and will not necessarily be 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 $A[x_1, \dots, x_n]$ the A -subalgebra of R generated by the elements $x_1, \dots, x_n \in R$.

We will need the following observation:

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

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

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

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

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

$$x^{n+j} = -a_{n-1}x^{n+j-1} - \dots - a_0x^j, \quad \text{where } a_0, \dots, a_{n-1} \in A.$$

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 $i \in \{1, \dots, n\}$

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

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

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

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

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

(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 . \square

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. \square

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. \square

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

$$(2.1.c) \quad x^n + a_{n-1}x^{n-1} + \dots + a_0 = 0,$$

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 $A \subset K$

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

and therefore

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

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

$$a^n u^n = (au)^n = (1 - bv)^n = 1 \pmod{bA},$$

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

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 that 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 $\varphi: k \rightarrow A$ (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

$$(2.1.d) \quad 0 = x^n + b_{n-1}x^{n-1} + \dots + b_0.$$

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) \Rightarrow (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) \Rightarrow (i) in Proposition 2.1.6 that x is integral over A . \square

LEMMA 2.1.16. *Let $A \subset R$ be a subring, and $\sigma: R \rightarrow S$ 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 $Q(\sigma(x)) = 0$. \square

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 $\sigma: R \rightarrow R/J$. 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 $\sigma(A) = A/(J \cap A) \subset R/J$. \square

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

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

We may arrange that the integer $n \in \mathbb{N} \setminus \{0\}$ 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

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

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

$$x^{-1} = -a_{n-1} - \cdots - a_0x^{n-1} \in R,$$

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 $I = J \cap A$ 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 $k \rightarrow A/\mathfrak{p}$ 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 $d < 0$.

¹By \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 $d \in \mathbb{Z} \setminus \{1\}$, where d is square-free.*

PROOF. Let K be a quadratic field. Pick an element $x \in K \setminus \mathbb{Q}$. 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 $x \notin \mathbb{Q}$), hence we have an equation of the form

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

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 $f = v^2e$ belongs to \mathbb{Z} . Then f may be written as $f = dg^2$, where $g \in \mathbb{Z}$ and d is square-free. Then $d = (v/g)^2e$, 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. \square

THEOREM 2.2.3. *Let K be a quadratic field, and write $K = \mathbb{Q}(\sqrt{d})$ where $d \in \mathbb{Z} \setminus \{1\}$ is square-free (see Proposition 2.2.2), and in particular $d \not\equiv 0 \pmod{4}$. Then a \mathbb{Z} -basis of the ring of integers \mathcal{O}_K (see Definition 2.1.10) is given by*

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

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 $\mathbb{Q}[X]/(X^2 - d) \rightarrow \mathbb{Q}[X]/(X^2 - d)$ given by $X \mapsto -X$ yields a morphism of \mathbb{Q} -algebras

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

It follows that $\mathbb{Q} \subset K$ is the subset of elements fixed by the endomorphism $\sigma: K \rightarrow K$. 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

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

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 $a, b \in \mathbb{Q}$

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

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

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

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 $u^2 \equiv 1 \pmod{4}$ and thus (2.2.c) implies that

$$(2.2.d) \quad dv^2 \equiv 1 \pmod{4}.$$

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

Conversely, assume that $d \equiv 1 \pmod{4}$. 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

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

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. \square

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

$$l_b: B \rightarrow B, \quad x \mapsto bx.$$

The *characteristic polynomial* of b is the polynomial¹

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

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

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

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

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

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. \square

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

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

where $p_0, \dots, p_r, q_0, \dots, q_s \in A$, 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

¹We 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 $p_0q_0 = 0$ (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. \square

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 $b_1 \in B_1$ 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

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

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. \square

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

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

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

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

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. \square

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):

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

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

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

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 $\text{sgn}: \mathfrak{S}_n \rightarrow \{1, -1\}$ is the signature morphism)

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

This polynomial has constant coefficient

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

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

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

PROPOSITION 3.1.9. The following hold:

(i) We have

$$\text{Tr}_{B/A}(0) = 0 \quad \text{and} \quad N_{B/A}(1) = 1.$$

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

$$\text{Tr}_{B/A}(x + y) = \text{Tr}_{B/A}(x) + \text{Tr}_{B/A}(y) \quad \text{and} \quad N_{B/A}(xy) = N_{B/A}(x) N_{B/A}(y).$$

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

$$\text{Tr}_{B/A}(a) = na \quad \text{and} \quad N_{B/A}(a) = a^n.$$

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 $l_a: B \rightarrow B$ is diagonal with coefficients (a, \dots, a) . \square

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

$$b \in B^\times \iff N_{B/A}(b) \in A^\times.$$

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

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

$$N_{B/A}: B^\times \rightarrow A^\times.$$

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

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

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 $\varphi: B \rightarrow B$ be a morphism of A -modules. Then*

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

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

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

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

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

where tM denotes the transpose of the matrix M . Taking determinants yields the statement (as transposing a matrix does not change its determinant). \square

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

LEMMA 3.2.4. *If $\alpha: B \xrightarrow{\sim} B'$ is an isomorphism of A -algebras, then $\mathfrak{D}_{B'/A} = \mathfrak{D}_{B/A}$.*

PROOF. Consider a system $(x_1, \dots, x_n) \in B^n$. It follows from Lemma 3.1.2 that, for any $i, j \in \{1, \dots, n\}$

$$\text{Tr}_{B/A}(x_i x_j) = \text{Tr}_{B'/A}(\alpha(x_i x_j)) = \text{Tr}_{B'/A}(\alpha(x_i)\alpha(x_j)).$$

Taking the determinants of the matrices whose coefficients are displayed in the above equation shows that

$$D_{B/A}(x_1, \dots, x_n) = D_{B'/A}(\alpha(x_1), \dots, \alpha(x_n)).$$

This implies that $\mathfrak{D}_{B/A} \subset \mathfrak{D}_{B'/A}$. Applying this reasoning to the inverse morphism $\alpha^{-1}: B' \rightarrow B$ shows that $\mathfrak{D}_{B'/A} \subset \mathfrak{D}_{B/A}$. \square

PROPOSITION 3.2.5. *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 $D_{B/A}(x_1, \dots, x_n)$ 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 $\varphi: B \rightarrow B$ such that $\varphi(e_i) = x_i$ for all $i \in \{1, \dots, n\}$, and by Lemma 3.2.2 we have

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

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

Now let $d = D_{B/A}(x_1, \dots, x_n)$, and assume that d generates the ideal $\mathfrak{D}_{B/A}$ in A . Then $D_{B/A}(e_1, \dots, e_n) = ad$ 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 . \square

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

LEMMA 3.2.6. *Assume that $A = \mathbb{Z}$, and let $(x_1, \dots, x_n) \in B^n$ be a system such that the integer $D_{B/\mathbb{Z}}(x_1, \dots, x_n) \in \mathbb{Z}$ 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 $\varphi: B \rightarrow B$ such that $\varphi(e_i) = x_i$ for each $i \in \{1, \dots, n\}$. By Lemma 3.2.2 we have

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

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 . \square

REMARK 3.2.7. Lemma 3.2.6 merely provides a sufficient condition for a given system to be a \mathbb{Z} -basis, which is not always necessary, as shown by Example 3.2.8 below.

EXAMPLE 3.2.8. Let $K = \mathbb{Q}(\sqrt{d})$, with $d \in \mathbb{Z} \setminus \{1\}$ 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 $d \equiv 1 \pmod{4}$, 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 $\iota_A: k \rightarrow A$. A morphism of k -algebras $\varphi: A \rightarrow B$ 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 $k \rightarrow F$ 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 $1, x, \dots, x^{d-1}$, 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. \square

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 $d = (\deg P_1) + \dots + (\deg P_n)$ (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 $i \in \{1, \dots, n\} \setminus \{j\}$, we have

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

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. \square

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 $L \rightarrow F$.*

PROOF. We proceed by induction on the degree $[L : k]$, the case $[L : k]$ being clear. Assume that $L \neq k$, and pick $x \in L \setminus k$. 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 $K \rightarrow E'$ (corresponding to $X \mapsto Y$). By induction, we find a field extension F/E' of finite degree and a morphism of K -algebras $L \rightarrow F$, concluding the proof. \square

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.*

¹There 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

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

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. \square

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

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

and $a_n \neq 0$. Then

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

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. \square

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

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

(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 ma_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 write $P = B(X^p)$, for some $B \in k[Y]$. Let us write

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

In view of (4.1.b) (applied to $A = k$), the Frobenius map $\phi: k \rightarrow k$ 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 $c_0, \dots, c_r \in k$ such that $c_i^p = b_i$ for all $i = 0, \dots, r$. 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. \square

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 $\sigma_1, \dots, \sigma_n : F \rightarrow \ell$.*

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 $x \in F \setminus E$ 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 $\sigma'_1, \dots, \sigma'_m : E \rightarrow \ell'$.

For each $i \in \{1, \dots, m\}$ 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 monic 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 $F \rightarrow \ell$ 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 ℓ . We have thus found $m[F : k] = n$ morphisms of k -algebras $F \rightarrow \ell$, as required. \square

We will need the following consequence later:

COROLLARY 4.1.17 (Primitive Element Theorem). *If F/k is a separable field extension of finite degree, there exists an element $x \in F$ such that $F = k[x]$.*

PROOF. When k is finite, the group k^\times is cyclic by Proposition 1.3.5, and we may simply take x a generator of that group.

We now assume that k is infinite. Let $n = [F : k]$. By Proposition 4.1.16 we find a field extension ℓ/k of finite degree, and n distinct morphisms $\sigma_1, \dots, \sigma_n : F \rightarrow \ell$. For each pair $(i, j) \in \{1, \dots, n\}^2$, consider the k -subspace $V_{i,j} \subset F$ consisting of those elements $y \in F$ such that $\sigma_i(y) = \sigma_j(y)$. Since the morphisms $\sigma_1, \dots, \sigma_n$ are pairwise distinct, we have $V_{i,j} \neq F$ whenever $i \neq j$. By Lemma 4.1.18 below, we may find an element $x \in F$ which belongs to no $V_{i,j}$ with $i \neq j$. The elements $\sigma_i(x)$ for $i \in \{1, \dots, n\}$ are then pairwise distinct. Those are roots (in ℓ) of the minimal polynomial P of x over k . Letting $d = \deg P$, we thus have $d \geq n$. The elements $1, x, \dots, x^{d-1} \in F$ are linearly independent over k , hence $[k[x] : k] \geq d$. But $k[x] \subset F$, hence $[k[x] : k] \leq [F : k] = n$. We conclude that $d = n$, and $[k[x] : k] = [F : k]$, which implies that $k[x] = F$. \square

LEMMA 4.1.18. *Let k be an infinite field, and V a k -vector space. If V_1, \dots, V_n are k -subspaces of V such that $V = V_1 \cup \dots \cup V_n$, then there exists $i \in \{1, \dots, n\}$ such that $V_i = V$.*

PROOF. We proceed by induction on n , the statement being clear if $n = 1$. Assume that $n > 1$. Assume $V_1 \neq V$ (otherwise the conclusion of the lemma holds), and pick $y \in V \setminus V_1$. Let $x \in V_1$. Then the set

$$E = \{x + \lambda y \mid \lambda \in k \setminus \{0\}\}$$

is in bijection with $k \setminus \{0\}$ (as $y \neq 0$), and in particular is infinite. Since $y \notin V_1$, it follows that $E \cap V_1 = \emptyset$, and thus $E \subset V_2 \cup \dots \cup V_n$, or equivalently

$$E = (E \cap V_2) \cup \dots \cup (E \cap V_n).$$

As the set E is infinite, we may find an index $j \in \{2, \dots, n\}$ such that the set $E \cap V_j$ is infinite, and in particular contains two distinct elements. So there are $\lambda_1 \neq \lambda_2 \in k$ such that $x + \lambda_1 y \in V_j$ and $x + \lambda_2 y \in V_j$. This implies that

$$y = (\lambda_1 - \lambda_2)^{-1}((x + \lambda_1 y) - (x + \lambda_2 y))$$

belongs to V_j , and thus $x = (x + \lambda_1 y) - \lambda_1 y \in V_j$. We have proved that $V_1 \subset V_2 \cup \dots \cup V_n$. Therefore $V = V_2 \cup \dots \cup V_n$, and by induction we find $i \in \{2, \dots, n\}$ such that $V_i = V$. \square

2. Étale algebras over a field

In this section k is a field. When X is any set, and F a field, then the set of maps $X \rightarrow F$ is naturally F -vector space; namely for any $f, g: X \rightarrow F$ and $\lambda \in F$, we define

$$f + \lambda g: X \rightarrow F, \quad x \mapsto f(x) + \lambda g(x).$$

LEMMA 4.2.1 (Dedekind). *Let A be a k -algebra, and ℓ/k a field extension. Let $\sigma_1, \dots, \sigma_n$ be pairwise distinct morphisms of k -algebras $A \rightarrow \ell$. Then the elements $\sigma_1, \dots, \sigma_n$ are ℓ -linearly independent, in the ℓ -vector space of maps $A \rightarrow \ell$.*

In particular $n \leq \dim_k A$ when A is finite-dimensional.

PROOF. Assume that

$$(4.2.a) \quad a_1 \sigma_1 + \dots + a_m \sigma_m = 0.$$

where $a_1, \dots, a_m \in \ell$ are not all zero. Pick such a relation, where $m \in \{1, \dots, n\}$ is minimal. In particular $a_m \neq 0$. As $\sigma_m \neq 0$ (because $\sigma_m(1) = 1 \in \ell$, which is nonzero since ℓ is a field), there exists $j \in \{1, \dots, m-1\}$ such that $a_j \neq 0$ (in particular $m > 1$). Since $\sigma_j \neq \sigma_m$, we may find $z \in A$ such that $\sigma_j(z) \neq \sigma_m(z)$. Since the morphisms $\sigma_1, \dots, \sigma_n$ are multiplicative, it follows from (4.2.a) (applied to zx for all $x \in A$) that

$$(4.2.b) \quad a_1 \sigma_1(z) \sigma_1 + \dots + a_m \sigma_m(z) \sigma_m = 0.$$

Subtracting $\sigma_m(z)$ times Equation (4.2.a) to (4.2.b) yields

$$a_1 (\sigma_1(z) - \sigma_m(z)) \sigma_1 + \dots + a_{m-1} (\sigma_{m-1}(z) - \sigma_m(z)) \sigma_{m-1} = 0.$$

Since $a_j (\sigma_j(z) - \sigma_m(z)) \neq 0$, we have found a contradiction with the minimality of m . \square

DEFINITION 4.2.2. A k -algebra A of finite dimension n is called *étale* if there exist a field extension ℓ/k and n distinct morphisms of k -algebras $\sigma_1, \dots, \sigma_n: A \rightarrow \ell$.

It is clear from the definition that any k -algebra isomorphic to an étale k -algebra is itself étale.

LEMMA 4.2.3. *Let A be an étale k -algebra. Then there exist a field extension ℓ/k of finite degree, and n distinct morphisms of k -algebras $\sigma_1, \dots, \sigma_n: A \rightarrow \ell$.*

PROOF. Let $\sigma_1, \dots, \sigma_n: A \rightarrow \ell$ be as in Definition 4.2.2, and let e_1, \dots, e_n be a k -basis of A . Recall that the ring A is integral over k (see Example 2.1.14), hence the elements $\sigma_i(e_j) \in \ell$ are integral over k by Lemma 2.1.16. Therefore, by Corollary 2.1.7, the k -subalgebra ℓ' of ℓ generated by the elements $\sigma_i(e_j)$ for $i, j \in \{1, \dots, n\}$ is of finite dimension as a k -vector space. Since the ring ℓ' is contained in the field ℓ , it is a domain, and thus ℓ' is a field by Proposition 2.1.19. Since $\ell' \subset \ell$ contains the image of each morphism σ_i for $i \in \{1, \dots, n\}$, we may thus replace ℓ with ℓ' . \square

Recall that a field F is called *algebraically closed* if the only algebraic field extension of F is F itself.

LEMMA 4.2.4. *Let \bar{k}/k be a field extension, with \bar{k} algebraically closed. Then a k -algebra A of finite dimension n is étale if and only if there are exactly n morphisms of k -algebras $A \rightarrow \bar{k}$.*

PROOF. Assume that A is étale, and pick a finite field extension ℓ/k and morphisms $\sigma_1, \dots, \sigma_n: A \rightarrow \ell$ (see Lemma 4.2.3). Then it follows from Proposition 4.1.9 that we may find a morphism of k -algebras $\ell \rightarrow \bar{k}'$, where \bar{k}'/\bar{k} is a field extension of finite degree, and in particular an algebraic field extension. Since the field \bar{k} is algebraically closed, we must have $\bar{k}' = \bar{k}$. We have thus n distinct morphisms $A \rightarrow \bar{k}$. By Dedekind's Lemma 4.2.1, there are no other such morphisms.

The converse follows from Definition 4.2.2, with $\ell = \bar{k}$. \square

PROPOSITION 4.2.5. *A finite separable field extension of k is an étale k -algebra.*

PROOF. This is Proposition 4.1.16. \square

PROPOSITION 4.2.6. *Let $P \in k[X]$ be a nonzero polynomial, and consider the k -algebra $A = k[X]/P$. Then A is étale if and only if P is separable.*

PROOF. Let $n = \deg P = \dim_k A$, and denote by $x \in A$ the class of X .

Assume that P is separable. Then by Proposition 4.1.8 we may find a field extension ℓ/k such that P splits into linear factors in $\ell[X]$, and so has n distinct roots $\alpha_1, \dots, \alpha_n \in \ell$. This yields n distinct morphisms of k -algebras, given by $x \mapsto \alpha_i$ for $i = 1, \dots, n$. We have proved that A is étale.

Conversely, assume that A is étale. According to Lemma 4.2.3, we may find a finite field extension ℓ/k and n distinct morphisms of k -algebras $\sigma_1, \dots, \sigma_n: A \rightarrow \ell$. The elements $\sigma_1(x), \dots, \sigma_n(x) \in \ell$ are then n distinct roots of P . Let us consider now a field extension F/k . By Proposition 4.1.9 we may find an extension E/k containing both F and ℓ . The polynomial P splits into a product of pairwise distinct monic linear factors in $E[X]$ (because it does so in $\ell[X]$), hence its roots in E are pairwise distinct in E , and thus so are its roots in F . We have proved that the polynomial P is separable. \square

3. Extension of scalars

Let k be a field. When A is a k -algebra and ℓ/k a field extension, we recall that we may define an ℓ -algebra $A \otimes_k \ell$ (see exercises). Its elements are of the form

$$\sum_{i=1}^m a_i \otimes \lambda_i, \quad \text{where } a_i \in A, \lambda_i \in \ell.$$

The map $A \rightarrow A \otimes_k \ell$ given by $a \mapsto a \otimes 1$ is an injective morphism of k -algebra, and we will thus view A as a k -subalgebra of $A \otimes_k \ell$.

When A is finite-dimensional as a k -vector space, so is the ℓ -vector space $A \otimes_k \ell$, and

$$(4.3.a) \quad \dim_k A = \dim_\ell(A \otimes_k \ell).$$

This construction satisfies the following universal property: if C is an ℓ -algebra, every morphism of k -algebras $A \rightarrow C$ extends uniquely to a morphism of ℓ -algebras $A \otimes_k \ell \rightarrow C$.

If A, B are k -algebras, then we have a canonical isomorphism of ℓ -algebras

$$(4.3.b) \quad (A \times B) \otimes_k \ell \simeq (A \otimes_k \ell) \times (B \otimes_k \ell).$$

PROPOSITION 4.3.1. *Let A be an étale k -algebra, and consider the distinct morphisms of k -algebras $\sigma_1, \dots, \sigma_n: A \rightarrow \ell$, where ℓ/k is a field extension and $n = \dim_k A$ (see Definition 4.2.2). Then there exists an isomorphism of ℓ -algebras*

$$\sigma: A \otimes_k \ell \xrightarrow{\sim} \ell^n$$

mapping $x \otimes y$ to $(\sigma_1(x)y, \dots, \sigma_n(x)y)$.

PROOF. Let us write $A' = A \otimes_k \ell$. By the universal property mentioned above, the n distinct morphisms of k -algebras $\sigma_1, \dots, \sigma_n: A \rightarrow \ell$ extend uniquely to n distinct morphisms of ℓ -algebras $\sigma'_1, \dots, \sigma'_n: A' \rightarrow \ell$, and we set

$$\sigma = (\sigma'_1, \dots, \sigma'_n): A' \rightarrow \ell^n.$$

For $i \in \{1, \dots, n\}$ and $x \in A, y \in \ell$, we have, by ℓ -linearity of σ'_i and the fact that σ'_i extends σ_i ,

$$\sigma'_i(x \otimes y) = \sigma'_i(x)y = \sigma_i(x)y.$$

By Dedekind's Lemma 4.2.1, the elements $\sigma'_1, \dots, \sigma'_n$ are linearly independent in the ℓ -vector space $\text{Hom}_\ell(A', \ell)$ of ℓ -linear forms $A' \rightarrow \ell$. This vector space has dimension $\dim_\ell A' = \dim_k A = n$ (see (4.3.a)), hence the family $\sigma'_1, \dots, \sigma'_n$ generates it.

Let now $a \in A'$ be such that $\sigma_i(a) = 0 \in \ell$ for all $i \in \{1, \dots, n\}$. If $a \neq 0$, then we may find an ℓ -linear form $\varphi: A' \rightarrow \ell$ such that $\varphi(a) \neq 0$ (take an ℓ -basis (e_1, \dots, e_n) of A' , pick $i \in \{1, \dots, n\}$ such that i -th coordinate of a is nonzero in that basis, and take for φ the linear form given by $\varphi(e_j) = \delta_{ij}$). We may then write φ as an ℓ -linear combination of $\sigma'_1, \dots, \sigma'_n$ (recall that those generate the ℓ -vector space $\text{Hom}_\ell(A', \ell)$). This implies that $\varphi(a) = 0$, a contradiction. We have proved that σ is injective, hence bijective by dimensional reasons (see (4.3.a)). \square

LEMMA 4.3.2. *Let A be a finite dimensional k -algebra, and ℓ/k a field extension.*

(i) *For any $a \in A$, the characteristic polynomials (see Definition 3.1.1) satisfy*

$$\chi_{A/k}(a) = \chi_{(A \otimes_k \ell)/\ell}(a \otimes 1) \in k \subset \ell.$$

(ii) *If $(x_1, \dots, x_n) \in A^n$, the discriminant satisfy*

$$\mathfrak{D}_{A/k}(x_1, \dots, x_n) = \mathfrak{D}_{(A \otimes_k \ell)/\ell}(x_1 \otimes 1, \dots, x_n \otimes 1) \in k \subset \ell.$$

(iii) *We have*

$$\mathfrak{D}_{A/k} = 0 \iff \mathfrak{D}_{(A \otimes_k \ell)/\ell} = 0.$$

PROOF. We let (e_1, \dots, e_n) be a k -basis of A . Then $(e_1 \otimes 1, \dots, e_n \otimes 1)$ is an ℓ -basis of $A \otimes_k \ell$ (exercise).

(i): The coefficients of the matrix of $l_{a \otimes 1}: A \otimes_k \ell \rightarrow A \otimes_k \ell$ in the basis $(e_1 \otimes 1, \dots, e_n \otimes 1)$ are the images of those of the matrix of $l_a: A \rightarrow A$ in the basis (e_1, \dots, e_n) under the inclusion $k \subset \ell$. It follows that the characteristic polynomial $\chi_{(A \otimes_k \ell)/\ell}(a \otimes 1)$ is the image of the characteristic polynomial $\chi_{A/k}(a)$ under the inclusion $k \subset \ell$.

(ii): Let us write $A' = A \otimes_k \ell$ and $x'_i = x_i \otimes 1$ for $i \in \{1, \dots, n\}$. From (i), we deduce that $\text{Tr}_{A/k}(x_i x_j) = \text{Tr}_{A'/\ell}(x'_i x'_j)$ for any $i, j \in \{1, \dots, n\}$. Therefore the matrix $(\text{Tr}_{A'/\ell}(x'_i x'_j)) \in M_n(\ell)$ is the image of the matrix $(\text{Tr}_{A/k}(x_i x_j)) \in M_n(k)$ under the inclusion $k \subset \ell$, hence its determinant $D_{A'/\ell}(x'_1, \dots, x'_n) \in \ell$ is the image of the determinant $D_{A/k}(x_1, \dots, x_n) \in k$ under the inclusion $k \subset \ell$.

(iii): It follows from Proposition 3.2.5 that

$$D_{A/k}(e_1, \dots, e_n) \neq 0 \iff \mathfrak{D}_{A/k} \neq 0,$$

and that

$$D_{(A \otimes \ell)/\ell}(e_1 \otimes 1, \dots, e_n \otimes 1) \neq 0 \iff \mathfrak{D}_{(A \otimes \ell)/\ell} \neq 0.$$

Therefore (iii) follows from (ii). \square

We are now in position to prove certain formulas that will be very useful in order to perform computations in étale algebras (and in particular in separable field extensions).

PROPOSITION 4.3.3. *Let A be an étale k -algebra. In the notation of Definition 4.2.2, the characteristic polynomial of any $a \in A$ satisfies*

$$\chi_{A/k}(a) = \prod_{i=1}^n (X - \sigma_i(a)) \in k[X] \subset \ell[X].$$

In particular, in $k \subset \ell$

$$\text{Tr}_{A/k}(a) = \sum_{i=1}^n \sigma_i(a) \quad \text{and} \quad N_{A/k}(a) = \prod_{i=1}^n \sigma_i(a).$$

PROOF. Consider the isomorphism of ℓ -algebras $\sigma: A \otimes_k \ell \xrightarrow{\sim} \ell^n$ of Proposition 4.3.1. We have in $k \subset \ell$, by Lemma 4.3.2 (i) and Lemma 3.1.2

$$\chi_{A/k}(a) = \chi_{(A \otimes_k \ell)/\ell}(a \otimes 1) = \chi_{\ell^n/\ell}(\sigma(a \otimes 1)) = \chi_{\ell^n/\ell}(\sigma_1(a), \dots, \sigma_n(a)).$$

Now in the canonical basis of ℓ^n , multiplication by the element $(\sigma_1(a), \dots, \sigma_n(a))$ is given by the diagonal matrix having coefficients $\sigma_1(a), \dots, \sigma_n(a)$, whose characteristic polynomial is

$$\prod_{i=1}^n (X - \sigma_i(a)) \in \ell[X]. \quad \square$$

PROPOSITION 4.3.4. *Let A be an étale k -algebra. In the notation of Definition 4.2.2, for any system $(x_1, \dots, x_n) \in A^n$, we have*

$$D_{A/k}(x_1, \dots, x_n) = \det(\sigma_i(x_j))^2 \in k \subset \ell.$$

PROOF. For any $i, j \in \{1, \dots, n\}$, we have by Proposition 4.3.3

$$\text{Tr}_{A/k}(x_i x_j) = \sum_{p=1}^n \sigma_p(x_i x_j) = \sum_{p=1}^n \sigma_p(x_i) \sigma_p(x_j) \in \ell,$$

which coincides with the (i, j) -th coefficient of the matrix product $M \cdot {}^tM$ in $M_n(\ell)$, where M is the matrix whose (r, s) -th coefficient is $\sigma_r(x_s) \in \ell$, and tM its transpose. Thus

$$\begin{aligned} D_{A/k}(x_1, \dots, x_n) &= \det(\mathrm{Tr}_{A/k}(x_i x_j)) \\ &= \det(M \cdot {}^tM) \\ &= (\det M) \cdot (\det {}^tM) \\ &= (\det M)^2 \\ &= \det(\sigma_i(x_j))^2. \end{aligned} \quad \square$$

PROPOSITION 4.3.5. *Let $A = k[X]/P$, where $P \in k[X]$ is a monic separable polynomial. Let n be the degree of P , and $x \in A$ be the class of X . Then*

$$D_{A/k}(1, x, \dots, x^{n-1}) = (-1)^{\frac{n(n-1)}{2}} N_{A/k}(P'(x)) \in k,$$

where $P' \in k[X]$ is the derivative of P .

PROOF. Recall from Proposition 4.2.6 that the k -algebra A is étale. So we have n morphisms of k -algebras $\sigma_1, \dots, \sigma_n: A \rightarrow \ell$, where ℓ/k is a field extension. Let $\alpha_i = \sigma_i(x)$ for $i = 1, \dots, n$. Then $\alpha_1, \dots, \alpha_n$ are n distinct roots of P in ℓ , hence

$$P = \prod_{i=1}^n (X - \alpha_i) \in \ell[X],$$

so that

$$P' = \sum_{i=1}^n \prod_{j \neq i} (X - \alpha_j) \in \ell[X],$$

and in particular, for any $i \in \{1, \dots, n\}$

$$(4.3.c) \quad P'(\alpha_i) = \prod_{j \neq i} (\alpha_i - \alpha_j) \in \ell[X].$$

We now compute:

$$\begin{aligned} D_{A/k}(1, x, \dots, x^{n-1}) &= \det((\alpha_i)^{j-1})^2 && \text{by Proposition 4.3.4} \\ &= \left(\prod_{j < i} (\alpha_i - \alpha_j) \right)^2 && \text{(Vandermonde determinant)} \\ &= (-1)^{\frac{n(n-1)}{2}} \prod_{i \neq j} (\alpha_i - \alpha_j) && \text{as } \mathrm{card}\{(i, j) | 1 \leq i < j \leq n\} = \frac{n(n-1)}{2} \\ &= (-1)^{\frac{n(n-1)}{2}} \prod_{i=1}^n \prod_{j \neq i} (\alpha_i - \alpha_j) \\ &= (-1)^{\frac{n(n-1)}{2}} \prod_{i=1}^n P'(\alpha_i) && \text{by (4.3.c)} \\ &= (-1)^{\frac{n(n-1)}{2}} \prod_{i=1}^n \sigma_i(P'(x)) && \text{as } \sigma_i \text{ is a morphism of } k\text{-algebras} \\ &= (-1)^{\frac{n(n-1)}{2}} N_{A/k}(P'(x)) && \text{by Proposition 4.3.3.} \end{aligned} \quad \square$$

4. The trace form

LEMMA 4.4.1. *Let A, B be k -algebras. Then A and B are étale if and only if $A \times B$ is étale.*

PROOF. Clearly A and B are finite-dimensional over k if and only if $A \times B$ is so. Let us assume that this is the case, and write $n = \dim_k A, m = \dim_k B$.

Assume that the k -algebras A, B are étale. Then by Lemma 4.2.3 there exist field extensions ℓ/k and ℓ'/k of finite degrees, as well as n morphisms of k -algebras $A \rightarrow \ell$ and m morphisms of k -algebras $B \rightarrow \ell'$. By Proposition 4.1.9, we may assume that $\ell = \ell'$ (upon enlarging ℓ). Composing with the projections $A \times B \rightarrow A$ and $A \times B \rightarrow B$, we obtain $n + m$ distinct morphisms of k -algebras $A \times B \rightarrow \ell$. This proves that the k -algebra $A \times B$ is étale.

Let now ℓ/k be a field extension, and $f: A \times B \rightarrow \ell$ a morphism of k -algebras. Then the image of f is a domain (being contained in the field ℓ). Thus $\ker f$ is a prime ideal of $A \times B$, hence a maximal ideal by Corollary 2.1.20. This implies that $\ker f = \mathfrak{m} \times B$ or $\ker f = A \times \mathfrak{m}'$, where $\mathfrak{m} \subset A$ or $\mathfrak{m}' \subset B$ is a maximal ideal (this follows from the fact that the ideals of $A \times B$ are precisely the subsets $I \times J$, where $I \subset A$ and $J \subset B$ are ideals). In particular the morphism f factors through exactly one of the projections $A \times B \rightarrow A$ or $A \times B \rightarrow B$.

Assume now that the k -algebra $A \times B$ is étale. Then we find a field extension ℓ/k and $m + n$ morphisms of k -algebras $A \times B \rightarrow \ell$. Let a , resp. b , the number of those morphisms which factor through the quotient $A \times B \rightarrow A$, resp. $A \times B \rightarrow B$. Then $a \leq n$ and $b \leq m$ by Dedekind's Lemma 4.2.1. We have just seen that $a + b = n + m$. We conclude that $a = n$ and $b = m$, showing that both A and B are étale k -algebras. \square

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

LEMMA 4.4.2. *Let A, B be rings. Then $A \times B$ is reduced if and only if both A and B are reduced.*

PROOF. Certainly an element $(a, b) \in A \times B$ is nilpotent if and only if both $a \in A$ and $b \in B$ are nilpotent. \square

LEMMA 4.4.3. *In a reduced noetherian ring, the zero ideal is the intersection of a finite family of pairwise distinct prime ideals.*

PROOF. Let A be a ring. We know that the ideal 0 contains a product of prime ideals of A (Lemma 1.2.9), hence $0 = \mathfrak{p}_1 \cdots \mathfrak{p}_n$, for some prime ideals $\mathfrak{p}_1, \dots, \mathfrak{p}_n$ of A (possibly not pairwise distinct). If $x \in \mathfrak{p}_1 \cap \cdots \cap \mathfrak{p}_n$, then $x^n \in \mathfrak{p}_1 \cdots \mathfrak{p}_n$, hence $x^n = 0$, and thus $x = 0$ as A is reduced. Thus $\mathfrak{p}_1 \cap \cdots \cap \mathfrak{p}_n = 0$, where, upon removing duplicates, we may now assume that $\mathfrak{p}_i \neq \mathfrak{p}_j$ when $i \neq j$. \square

PROPOSITION 4.4.4. *Every reduced finite-dimensional k -algebra is a product of finite field extensions of k .*

PROOF. Let A be a reduced finite-dimensional k -algebra. Then A is noetherian by Example 1.2.3, hence by Lemma 4.4.3 we may write $0 = \mathfrak{p}_1 \cap \cdots \cap \mathfrak{p}_n$, where $\mathfrak{p}_1, \dots, \mathfrak{p}_n$ are pairwise distinct prime ideals of A . Then $\mathfrak{p}_i + \mathfrak{p}_j = A$ for $i \neq j$ because \mathfrak{p}_i is maximal by Corollary 2.1.20. We conclude using Lemma 1.1.5 that $A \simeq (A/\mathfrak{p}_1) \times \cdots \times (A/\mathfrak{p}_n)$, where each A/\mathfrak{p}_i is a field extension of k (this is an isomorphism of A -algebras, hence in

particular of k -algebras). These field extensions have finite degrees, being quotients of the finite-dimensional k -vector space A . \square

When V is a k -vector space, we recall that a symmetric bilinear form $\varphi: V \times V \rightarrow k$ is called *nondegenerate* if the k -linear map

$$(4.4.a) \quad V \rightarrow \text{Hom}_k(V, k), \quad x \mapsto (y \mapsto \varphi(x, y))$$

is bijective.

LEMMA 4.4.5. *Let V be a finite-dimensional k -vector space, and $\varphi: V \times V \rightarrow k$ a nondegenerate symmetric bilinear form. Then for each k -basis (y_1, \dots, y_n) of V we may find a k -basis (x_1, \dots, x_n) of V such that $\varphi(x_i, y_j) = \delta_{ij}$ for all $i, j \in \{1, \dots, n\}$ (we use the notation of (1.3.b)).*

PROOF. For each $i \in \{1, \dots, n\}$, consider the linear form $y_i^* \in \text{Hom}_k(V, k)$ given by $y_i^*(y_j) = \delta_{ij}$ for all $j \in \{1, \dots, n\}$. Since the map (4.4.a) is surjective, we may find an element x_i mapping to y_i^* under (4.4.a), which means that $\varphi(x_i, y_j) = \delta_{ij}$ for all $j \in \{1, \dots, n\}$. It remains to prove that the system (x_1, \dots, x_n) is a k -basis of V . Assume that

$$\sum_{i=1}^n \lambda_i x_i = 0 \in V, \quad \text{with } \lambda_1, \dots, \lambda_n \in k.$$

Applying (4.4.a) yields

$$\sum_{i=1}^n \lambda_i y_i^* = 0 \in \text{Hom}_k(V, k).$$

Evaluating at $y_j \in V$, for $j \in \{1, \dots, n\}$, shows that $\lambda_j = 0$. We have proved that the system (x_1, \dots, x_n) is k -linearly independent, hence a k -basis by dimensional reasons. \square

THEOREM 4.4.6. *Let A be a finite-dimensional k -algebra. Then the following conditions are equivalent:*

- (i) *the k -algebra A is étale,*
- (ii) *there exists a field extension ℓ/k of finite degree such that $A \otimes_k \ell \simeq \ell^n$ as ℓ -algebras,*
- (iii) *$\mathfrak{D}_{A/k} \neq 0$ (see Definition 3.2.3),*
- (iv) *the symmetric bilinear form $A \times A \rightarrow k$ given by $(x, y) \mapsto \text{Tr}_{A/k}(xy)$ is nondegenerate,*
- (v) *for every field extension ℓ/k , then ring $A \otimes_k \ell$ is reduced,*
- (vi) *A is isomorphic to a product of separable field extensions of k .*

PROOF. (i) \Rightarrow (ii) : This is Proposition 4.3.1.

(ii) \Rightarrow (iii) : The discriminant of the canonical ℓ -basis of ℓ^n is 1, hence $\mathfrak{D}_{\ell^n/\ell} \neq 0$. In view of Lemma 3.2.4, the assumption (ii) thus implies that $\mathfrak{D}_{(A \otimes_k \ell)/\ell} \neq 0$. Using Lemma 4.3.2 (iii) we deduce that $\mathfrak{D}_{A/k} \neq 0$.

(iii) \Leftrightarrow (iv) : Let (e_1, \dots, e_n) be a k -basis of A . Let $(e_1^*, \dots, e_n^*) \in \text{Hom}_k(A, k)$ be the dual basis, characterised by the equations $e_i^*(e_j) = \delta_{ij}$ for $i, j \in \{1, \dots, n\}$ (we use the notation of (1.3.b)). Then in these basis, the matrix of the k -linear map $A \rightarrow \text{Hom}_k(A, k)$ sending $x \in A$ to the linear form $y \mapsto \text{Tr}_{A/k}(xy)$ is given by $(\text{Tr}_{A/k}(e_i e_j))$, so that its determinant is the discriminant $\text{D}_{A/k}(e_1, \dots, e_n) \in k$. We thus see that $\text{D}_{A/k}(e_1, \dots, e_n)$ is nonzero if and only if the trace form given in (iv) is nondegenerate. But it follows from Proposition 3.2.5 that $\text{D}_{A/k}(e_1, \dots, e_n) \neq 0$ if and only if $\mathfrak{D}_{A/k} \neq 0$.

(iii) \Rightarrow (v) : Let ℓ/k be a field extension, and consider the ℓ -algebra $A' = A \otimes_k \ell$. We have $\mathfrak{D}_{A/k} \neq 0$ by (iii), hence $\mathfrak{D}_{A'/\ell} \neq 0$ by Lemma 4.3.2 (iii). In view of the implication (iii) \Rightarrow (iv) established above (applied to the ℓ -algebra A'), we deduce that the trace form $A' \times A' \rightarrow \ell$ is nondegenerate. Thus for every nonzero element $a \in A'$, we may find an element $b \in A'$ such that $\text{Tr}_{A'/\ell}(ab) \neq 0 \in \ell$. As the trace of a nilpotent element is zero (see Proposition 3.1.3), the element $ab \in A'$ is not nilpotent, hence the element $a \in A'$ is not nilpotent. We have proved that the ring A' is reduced, as required.

(v) \Rightarrow (vi) : By Proposition 4.4.4, the k -algebra A is isomorphic to a product of field extensions of k of finite degrees. It remains to prove that these are separable. Let K/k be one of these field extensions, and $x \in K$. Let $B = k[x] \subset K$. Then the k -algebra B is isomorphic to $k[X]/P$, where P is the minimal polynomial of x over k . For every field extension ℓ/k , the ring $\ell[X]/P \simeq B \otimes_k \ell$ is reduced, being contained² in $K \otimes_k \ell$, which is reduced because $A \otimes_k \ell$ is so (Lemma 4.4.2, in view of (4.3.b)). This implies that the polynomial $P \in k[X]$ is separable: indeed if $P = (X - a)Q \in \ell[X]$ where $Q \in \ell[X]$ and $a \in \ell$ are such that $Q(a) = 0$, then $P \mid Q^2$, hence the image of Q is a nonzero nilpotent element of $\ell[X]/P$.

(vi) \Rightarrow (i) : This follows from Proposition 4.2.5 and Lemma 4.4.1. \square

COROLLARY 4.4.7. *Let F/k be a field extension of finite degree. Then the k -algebra F is étale if and only if the field extension F/k is separable.*

PROOF. One implication has been proved in Proposition 4.2.5. So assume that the k -algebra F is étale. Then by Theorem 4.4.6 we have an isomorphism of k -algebras $F \simeq A = F_1 \times \cdots \times F_r$, where each F_i/k is a separable field extension. If $r \geq 2$, then A is not a domain, because

$$(1, 0, 0, \dots, 0) \cdot (0, 1, 0, \dots, 0) = 0 \in A.$$

As F is a domain, we must have $r = 1$. Thus $F \simeq F_1$ as a k -algebra, hence F is a separable extension of k . \square

PROPOSITION 4.4.8. *Assume that the field k is perfect, for instance of characteristic zero (Proposition 4.1.14) or finite (Proposition 4.1.15). Then a finite-dimensional k -algebra is étale if and only if it is reduced.*

PROOF. An étale k -algebra is in particular reduced by the criterion (v) in Theorem 4.4.6. Conversely, let A be a reduced finite-dimensional k -algebra. By Proposition 4.4.4, the k -algebra A is isomorphic to $F_1 \times \cdots \times F_r$, where F_1, \dots, F_r are finite field extensions of k . As k is perfect, each extension F_i/k is separable, hence each F_i is an étale k -algebra by Proposition 4.2.5. We conclude using Lemma 4.4.1 that the k -algebra $F_1 \times \cdots \times F_r$ is étale, and thus so is A . \square

²here we use the following easy fact: if $R \rightarrow S$ is an injective morphism of k -algebras, then the induced morphism of ℓ -algebras $R \otimes_k \ell \rightarrow S \otimes_k \ell$ is injective.

CHAPTER 5

The ring of integers

1. Integral closure in a separable extension

A fundamental property of the norm and trace functions is that they produce integers out of integers:

PROPOSITION 5.1.1. *Let A be a domain, with fraction field K . Let L/K be a finite separable extension, and $x \in L$ an element which is integral over A . Then the coefficients of the characteristic polynomial $\chi_{L/K}(x) \in K[X]$ are integral over A .*

PROOF. We apply Proposition 4.1.16 with $F/k = L/K$, and so find a field extension E/K ($= \ell/k$) and n morphisms of K -algebras $\sigma_1, \dots, \sigma_n: L \rightarrow E$. By Proposition 4.3.3 we have

$$(5.1.a) \quad \chi_{L/K}(x) = \prod_{i=1}^n (X - \sigma_i(x)) \in E[X].$$

Let C be the integral closure of A in E . Then the elements $\sigma_1(x), \dots, \sigma_n(x) \in E$ are integral over A by Lemma 2.1.16, hence belong to C . Therefore the formula (5.1.a) implies that $\chi_{L/K}(x) \in C[X]$, as required. \square

COROLLARY 5.1.2. *Let A be an integrally closed domain, with fraction field K . Let L/K be a finite separable extension, and B the integral closure of A in L . Then*

$$\mathrm{Tr}_{L/K}(B) \subset A \quad \text{and} \quad \mathrm{N}_{L/K}(B) \subset A.$$

PROOF. This follows from Proposition 5.1.1, since the maps $\mathrm{Tr}_{L/K}$ and $\mathrm{N}_{L/K}$ are given by certain coefficients of the characteristic polynomial (Lemma 3.1.8). \square

COROLLARY 5.1.3. *Let A be an integrally closed domain, with fraction field K . Let L/K be a finite separable extension, and B the integral closure of A in L . Let $b \in B$. Then*

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

PROOF. Assume that $b \in B^\times$. Then by Corollary 5.1.2 we have $\mathrm{N}_{L/K}(b) \in A$ and $\mathrm{N}_{L/K}(b^{-1}) \in A$, and by Proposition 3.1.9

$$1 = \mathrm{N}_{L/K}(1) = \mathrm{N}_{L/K}(bb^{-1}) = \mathrm{N}_{L/K}(b) \mathrm{N}_{L/K}(b^{-1}).$$

In particular $\mathrm{N}_{L/K}(b) \in A^\times$.

Conversely, assume that $\mathrm{N}_{L/K}(b) \in A^\times$. Then by Proposition 5.1.1, we may write

$$\chi_{L/K}(b) = X^n + a_{n-1}X^{n-1} + \dots + a_0, \quad \text{with } a_0, \dots, a_{n-1} \in A.$$

Recall that by Lemma 3.1.8 we have $a_0 = (-1)^n N_{L/K}(b)$, and so $a_0 \in A^\times$. By the Cayley–Hamilton theorem (Proposition 3.1.6) we have

$$b^n + a_{n-1}b^{n-1} + \cdots + a_0 = 0 \in L.$$

Therefore

$$b(b^{n-1} + a_{n-1}b^{n-2} + \cdots + a_1) = -a_0 \in A^\times \subset B^\times,$$

so that $b \in B^\times$. \square

LEMMA 5.1.4. *Let A be an integrally closed domain, with fraction field K . Let L/K be a finite field extension, and B the integral closure of A in L . Then every element of L is of the form ba^{-1} with $b \in B$ and $a \in A \setminus \{0\}$. In particular L is the fraction field of B .*

PROOF. Let $x \in L$. Then x is algebraic over K , hence satisfies an equation of the form

$$a_mx^m + \cdots + a_0 = 0,$$

where $a_0, \dots, a_m \in K$ are not all zero. Observe that $m > 0$. We may assume that $a_m \neq 0$. Multiplying with a (nonzero) common denominator of a_0, \dots, a_m , we may assume that $a_0, \dots, a_m \in A$. Multiplying with the nonzero element $a_m^{m-1} \in A$ and setting $y = a_mx \in K$, we obtain an equation

$$y^m + a_{m-1}y^{m-1} + a_ma_{m-2}y^{m-2} + \cdots + a_m^{m-1}a_0 = 0,$$

showing that the element $y \in L$ is integral over A , hence belongs to B . So $x = y(a_m)^{-1}$ is of the required form. \square

THEOREM 5.1.5. *Let A be an integrally closed domain, with fraction field K . Let L/K be a finite separable field extension, and B the integral closure of A in L . Then B contains a K -basis of L . Moreover there exists an A -submodule F of L , which is free of rank $[L : K]$ and which contains B .*

PROOF. Let $n = [L : K]$, and (e_1, \dots, e_n) a K -basis of L . By Lemma 5.1.4, for each $i \in \{1, \dots, n\}$ we may find a nonzero element $a_i \in A$ such that $x_i = a_ie_i \in B$. Then (x_1, \dots, x_n) is a K -basis (x_1, \dots, x_n) of L contained in B .

Recall that by Theorem 4.4.6 (and Proposition 4.2.5), the trace form $L \times L \rightarrow K$ is nondegenerate, hence by Lemma 4.4.5 we may find a K -basis (y_1, \dots, y_n) such that $\text{Tr}_{L/K}(x_i y_j) = \delta_{ij}$ for all $i, j \in \{1, \dots, n\}$ (we use the notation of (1.3.b)). Let $b \in B$, and write

$$b = b_1 y_1 + \cdots + b_n y_n, \quad \text{with } b_1, \dots, b_n \in K.$$

Then for any $i \in \{1, \dots, n\}$ we have $bx_i \in B$ (because $b \in B$ and $x_i \in B$), hence by Proposition 5.1.1 we have $\text{Tr}_{L/K}(bx_i) \in A$. But by K -linearity of $\text{Tr}_{L/K}: L \rightarrow K$ (see Proposition 3.1.9), we have

$$\text{Tr}_{L/K}(bx_i) = \text{Tr}_{L/K}\left(\sum_{j=1}^n b_j x_i y_j\right) = \sum_{j=1}^n b_j \text{Tr}_{L/K}(x_i y_j) = b_i,$$

so that $b_i \in A$. It follows that the element b lies in the A -submodule F of L generated by the elements y_1, \dots, y_n . We have proved that $B \subset F$. The system (y_1, \dots, y_n) is A -linearly independent in F , because its image in L is so (being K -linearly independent). Therefore the system (y_1, \dots, y_n) is an A -basis of F , and so the A -module F is free of rank n . \square

COROLLARY 5.1.6. *Let A be a principal ideal domain, with fraction field K . Let L/K be a finite separable field extension, and B the integral closure of A in L . Then B is a free A -module of rank $[L : K]$.*

PROOF. Let $n = [L : K]$. By Theorem 5.1.5, the A -module B is contained in a submodule F of L , which is free of rank n , and in addition the subset $B \subset L$ spans L as a K -vector space. By the implication (ii) \Rightarrow (i) in Proposition 1.3.13 (applied with $V = L$) the A -module B is free of rank n . \square

EXAMPLE 5.1.7. Let K be a number field of degree $n = [K : \mathbb{Q}]$. Then the field extension K/\mathbb{Q} is separable (Proposition 4.1.14), and the ring \mathbb{Z} is a principal ideal domain. Thus by Corollary 5.1.6 the \mathbb{Z} -module \mathcal{O}_K is free of rank n .

LEMMA 5.1.8. *In the situation of Corollary 5.1.6, the following hold:*

- (i) *Let (e_1, \dots, e_n) be an A -basis of B . Then (e_1, \dots, e_n) is a K -basis of L .*
- (ii) *For any $b \in B$, we have*

$$\chi_{B/A}(b) = \chi_{L/K}(b) \in A[X] \subset K[X].$$

- (iii) *For any system $(x_1, \dots, x_n) \in B^n$, we have*

$$D_{B/A}(x_1, \dots, x_n) = D_{L/K}(x_1, \dots, x_n) \in A \subset K.$$

PROOF. (i): Assume that

$$\sum_{i=1}^n \lambda_i e_i = 0, \quad \text{with } \lambda_1, \dots, \lambda_n \in K.$$

Then we may find a nonzero element $a \in A$ such that $a\lambda_i \in A$ for each $i \in \{1, \dots, n\}$. The A -linear independence of (e_1, \dots, e_n) implies that $a\lambda_i = 0$, and therefore $\lambda_i = 0$, for all $i \in \{1, \dots, n\}$. Thus the system (e_1, \dots, e_n) is K -linearly independent in L , hence a K -basis of L since $\dim_K L = n$.

(ii): We pick an A -basis (e_1, \dots, e_n) of B . The coefficients of the matrix of the K -linear map $l_b: L \rightarrow L$ in the K -basis (e_1, \dots, e_n) are the images of those of the matrix of the A -linear map $l_b: B \rightarrow B$ in the A -basis (e_1, \dots, e_n) under the inclusion $A \subset K$. Hence the characteristic polynomial of the former is the image of the characteristic polynomial of the latter under the inclusion $A[X] \subset K[X]$.

(iii): By (ii), the coefficients of the matrix $(\text{Tr}_{L/K}(x_i x_j))$ in $M_n(K)$ are the images of those of the matrix $(\text{Tr}_{B/A}(x_i x_j))$ in $M_n(A)$. Taking determinants yields the statement. \square

DEFINITION 5.1.9. The *absolute discriminant* of a number field K is the integer

$$D_{K/\mathbb{Q}}(x_1, \dots, x_n) = D_{\mathcal{O}_K/\mathbb{Z}}(x_1, \dots, x_n) \in \mathbb{Z},$$

where (x_1, \dots, x_n) is any \mathbb{Z} -basis of \mathcal{O}_K (see Lemma 5.1.8). This integer does not depend on the choice of the basis by Lemma 3.2.2, because $\mathbb{Z}^\times = \{-1, 1\}$ and so the square of any invertible element of \mathbb{Z} is 1.

EXAMPLE 5.1.10. Consider the case of a quadratic field $K = \mathbb{Q}(\sqrt{d})$, with $d \in \mathbb{Z}$ square-free. Then Example 3.2.8 provides a computation of the absolute discriminant d_K of K :

$$d_K = \begin{cases} d & \text{if } d \equiv 1 \pmod{4} \\ 4d & \text{if } d \equiv 2, 3 \pmod{4}. \end{cases}$$

2. Irreducibility of polynomials

The next proposition is a variant of the classical Gauss Lemma, which is sometimes referred to as “Dedekind’s Prague Theorem”:

PROPOSITION 5.2.1. *Let A be an integrally closed domain with fraction field K . If $Q, R \in K[X]$ are monic polynomials such that $QR \in A[X]$, then $Q, R \in A[X]$.*

PROOF. Let L/K be a field extension where $Q, R \in L[X]$ split into a product of linear factors (Proposition 4.1.8). Then we may write in $L[X]$

$$(5.2.a) \quad Q = \prod_{i=1}^n (X - \alpha_i) \quad \text{and} \quad R = \prod_{i=1}^m (X - \beta_i),$$

where $\alpha_1, \dots, \alpha_n, \beta_1, \dots, \beta_m \in L$ are the roots of Q, R (with repetitions allowed). These roots are then integral over A (being roots of the monic polynomial $P \in A[X]$), hence belong to the integral closure B of A in L . The formulas (5.2.a) then show that $Q, R \in B[X]$. Since A is integrally closed (in K), we have $B \cap K = A$. As $Q, R \in K[X]$, we conclude that $Q, R \in A[X] = B[X] \cap K[X] \subset L[X]$. \square

COROLLARY 5.2.2. *Let A be an integrally closed domain with fraction field K . Let $P \in A[X]$ be a monic polynomial. Then the polynomial P is irreducible in $A[X]$ if and only if it is irreducible in $K[X]$.*

PROOF. Certainly if P is irreducible in $K[X]$, it is so in $A[X]$. Conversely, assume that P is irreducible in $A[X]$. We assume that $P = QR$ with $Q, R \in K[X]$, and show that one of Q, R is a unit in $K[X]$. Let $q, r \in K$ be the leading coefficients of Q, R . Since the polynomial P is monic, we have $qr = 1$. Replacing Q with rQ , and R with qR , we may assume that the polynomials Q and R are monic. By Proposition 5.2.1 we have $Q, R \in A[X]$. Since P is irreducible in $A[X]$, one of the elements Q, R must be a unit in $A[X]$, and a fortiori also in $K[X]$. \square

COROLLARY 5.2.3 (Eisenstein’s criterion). *Let A be an integrally closed domain, and \mathfrak{p} a prime ideal of A . Consider a monic polynomial*

$$P = X^n + a_{n-1}X^{n-1} + \dots + a_0 \in A[X]$$

where $a_0, \dots, a_{n-1} \in A$. Assume that $a_i \in \mathfrak{p}$ for all $i = 0, \dots, n-1$, but that $a_0 \notin \mathfrak{p}^2$. Then P is irreducible in $K[X]$, where K is the fraction field of A .

PROOF. By Corollary 5.2.2, it will suffice to prove that P is irreducible in $A[X]$. Let us write $P = FG$ in $A[X]$, with F, G monic. Consider the quotient ring $C = A/\mathfrak{p}$, and denote by $\overline{Q} \in C[X]$ the image of a polynomial in $Q \in A[X]$. In $C[X]$ we have $\overline{P} = X^n$ (by the assumption) and $\overline{P} = \overline{F} \cdot \overline{G}$. As the ring C is a domain, it follows from Lemma 3.1.4 that \overline{F} and \overline{G} are powers of X in $C[X]$. Thus $F - X^r \in \mathfrak{p}A[X]$ and $G - X^s \in \mathfrak{p}A[X]$, where $r = \deg F$ and $s = \deg G$. If F and G are both nonconstant, then $r > 0$ and $s > 0$, and so $F(0) \in \mathfrak{p}$ and $G(0) \in \mathfrak{p}$. Thus

$$a_0 = P(0) = F(0)G(0) \in \mathfrak{p}^2,$$

which contradicts the assumption. \square

3. Cyclotomic fields

In this section p will be a prime number, and $\xi \in \mathbb{C}$ a primitive p -th root of unity. This means that $\xi^p = 1$ and $\xi \neq 1$. We investigate the *cyclotomic field* $K = \mathbb{Q}(\xi) \subset \mathbb{C}$, and its ring of integers \mathcal{O}_K .

Consider the *cyclotomic polynomial*

$$(5.3.a) \quad \Phi_p = X^{p-1} + \cdots + 1 \in \mathbb{Z}[X],$$

which satisfies the relation

$$(5.3.b) \quad X^p - 1 = (X - 1)\Phi_p \in \mathbb{Z}[X].$$

The image of Φ_p in $K[X]$ admits $\xi, \dots, \xi^{p-1} \in K$ as roots and thus

$$(5.3.c) \quad \Phi_p = (X - \xi) \cdots (X - \xi^{p-1}) \in K[X].$$

LEMMA 5.3.1. *The polynomial Φ_p is irreducible in $\mathbb{Q}[X]$.*

PROOF. Set $Y = X - 1 \in \mathbb{Z}[X]$. Then, in $\mathbb{Z}[X]$ we have

$$Y\Phi_p = X^p - 1 = (Y + 1)^p - 1 = Y^p + \sum_{i=1}^{p-1} \binom{p}{i} Y^i.$$

Since Y is nonzero and $\mathbb{Z}[X]$ is a domain, we deduce that

$$(5.3.d) \quad \Phi_p = F(Y) \quad \text{where } F(T) = T^{p-1} + \sum_{i=1}^{p-1} \binom{p}{i} T^{i-1} \in \mathbb{Z}[T].$$

Now that binomial coefficient $\binom{p}{i}$ is divisible by p for $i = 1, \dots, p-1$ (classical exercise), and $\binom{p}{1} = p$ is not divisible by p^2 . Therefore by Eisenstein's criterion (Corollary 5.2.3), the polynomial F is irreducible in $\mathbb{Q}[T]$. Since $\Phi_p \in \mathbb{Q}[X]$ is the image of $F \in \mathbb{Q}[T]$ under the ring isomorphism $\mathbb{Q}[T] \mapsto \mathbb{Q}[X]$ given by $T \mapsto X - 1$, this implies that Φ_p is irreducible in $\mathbb{Q}[X]$. \square

Lemma 5.3.1 implies that the mapping $X \mapsto \xi$ induces an isomorphism of \mathbb{Q} -algebras

$$(5.3.e) \quad \mathbb{Q}[X]/\Phi_p \simeq K.$$

In particular K is a number field of degree $p-1$, and a \mathbb{Q} -basis of K is given by $1, \xi, \dots, \xi^{p-2}$. It follows from (5.3.c) that we have morphisms of \mathbb{Q} -algebras

$$\sigma_i: K \rightarrow K, \quad \xi \mapsto \xi^i$$

for $i \in \{1, \dots, p-1\}$. Those are pairwise distinct, and there are $p-1 = [K : \mathbb{Q}]$ of them. (So in the notation of Definition 4.2.2, we have $n = p-1$, and $k = \mathbb{Q}$, $A = K$, $\ell = K$.)

LEMMA 5.3.2. *We have*

- (i) $\text{Tr}_{K/\mathbb{Q}}(1) = p-1$,
- (ii) $\text{Tr}_{K/\mathbb{Q}}(\xi^j) = -1$ for $j \in \{1, \dots, p-1\}$,

PROOF. Observe that for $j \in \{0, \dots, p-1\}$ we have $\sigma_i(\xi^j) = \xi^{ij}$ for all $i \in \{1, \dots, p-1\}$. Using the formula of Proposition 4.3.3, we have

$$\text{Tr}_{K/\mathbb{Q}}(\xi^j) = \sum_{i=1}^{p-1} \sigma_i(\xi^j) = \sum_{i=1}^{p-1} \xi^{ij} = \Phi_p(\xi^j) - 1.$$

Now $\Phi_p(\xi^j) = 0$ when $j \in \{1, \dots, p-1\}$ (see (5.3.c)), while $\Phi_p(\xi^0) = \Phi_p(1) = p$. This yields (i) and (ii). (Alternatively (i) follows directly from Proposition 3.1.9 (iii).) \square

LEMMA 5.3.3. *We have*

$$N_{K/\mathbb{Q}}(\xi) = (-1)^{p-1}.$$

PROOF. By Proposition 4.3.3, we have

$$N_{K/\mathbb{Q}}(\xi) = \prod_{i=1}^{p-1} \xi^i = \xi^{1+\dots+(p-1)} = \xi^{\frac{p(p-1)}{2}}.$$

If p is odd, this equals $(\xi^p)^{(p-1)/2} = 1 = (-1)^{p-1}$. If $p = 2$, this equals $\xi = -1 = (-1)^{p-1}$. \square

LEMMA 5.3.4. *We have*

$$N_{K/\mathbb{Q}}(1 - \xi) = (1 - \xi) \dots (1 - \xi^{p-1}) = p.$$

PROOF. We have

$$\begin{aligned} N_{K/\mathbb{Q}}(1 - \xi) &= (1 - \xi) \dots (1 - \xi^{p-1}) && \text{by Proposition 4.3.3} \\ &= \Phi_p(1) && \text{by (5.3.c)} \\ &= p && \text{by (5.3.a).} \end{aligned} \quad \square$$

LEMMA 5.3.5. *We have*

$$\mathbb{Z} \cap (1 - \xi)\mathcal{O}_K = p\mathbb{Z}.$$

PROOF. By Lemma 5.3.4 we have $p\mathbb{Z} \subset \mathbb{Z} \cap (1 - \xi)\mathcal{O}_K$. If this inclusion were not an equality, we would have $\mathbb{Z} = \mathbb{Z} \cap (1 - \xi)\mathcal{O}_K$ (as $p\mathbb{Z}$ is a maximal ideal of \mathbb{Z}). In particular $1 = (1 - \xi)\alpha$ for some $\alpha \in \mathcal{O}_K$. Taking the norms yields, in view of Lemma 5.3.4

$$1 = N_{K/\mathbb{Q}}(1) = N_{K/\mathbb{Q}}(1 - \xi) \cdot N_{K/\mathbb{Q}}(\alpha) = p N_{K/\mathbb{Q}}(\alpha).$$

This is a contradiction, as $N_{K/\mathbb{Q}}(\alpha) \in \mathbb{Z}$ by Corollary 5.1.2 (in view of Remark 2.1.12). \square

LEMMA 5.3.6. *We have*

$$\text{Tr}_{K/\mathbb{Q}}((1 - \xi)\mathcal{O}_K) \subset p\mathbb{Z}.$$

PROOF. Let $y \in \mathcal{O}_K$. Then the elements $\sigma_i(y) \in \mathbb{C}$, for $i \in \{1, \dots, p-1\}$, are also integral over \mathbb{Z} by Lemma 2.1.16, hence belong to \mathcal{O}_K . Thus

$$\begin{aligned} \text{Tr}_{K/\mathbb{Q}}((1 - \xi)y) &= \sum_{i=1}^{p-1} \sigma_i((1 - \xi)y) \\ &= \sum_{i=1}^{p-1} (1 - \xi^i) \sigma_i(y) \\ &= (1 - \xi) \sum_{i=1}^{p-1} (\xi^{i-1} + \dots + 1) \sigma_i(y) \end{aligned}$$

belongs to $(1 - \xi)\mathcal{O}_K$. On the other hand $\text{Tr}_{K/\mathbb{Q}}((1 - \xi)y) \in \mathbb{Z}$ by Corollary 5.1.2, and we conclude using Lemma 5.3.5. \square

PROPOSITION 5.3.7. *For the number field $K = \mathbb{Q}(\xi)$, we have $\mathbb{Z}[\xi] = \mathcal{O}_K$, and $(1, \dots, \xi^{p-2})$ is a \mathbb{Z} -basis of $\mathbb{Z}[\xi]$.*

PROOF. Since $\xi^{p-1} = -1 - \dots - \xi^{p-2}$ (because $\Phi_p(\xi) = 0$), it follows that the family $1, \dots, \xi^{p-2}$ generates the \mathbb{Z} -module $\mathbb{Z}[\xi]$. This family is \mathbb{Z} -linearly independent, because it is \mathbb{Q} -linearly independent in K . It remains to prove that $\mathbb{Z}[\xi] = \mathcal{O}_K$. It will suffice to show that $\mathcal{O}_K \subset \mathbb{Z}[\xi]$, since the other inclusion is clear.

For $j \in \mathbb{N}$, let $Q_j \subset K$ be the \mathbb{Q} -subspace generated by $1, \dots, \xi^{j-1}$, and $Z_j \subset K$ the \mathbb{Z} -submodule generated by $1, \dots, \xi^{j-1}$. We show by induction on $j \leq p-1$ that

$$Q_j \cap \mathcal{O}_K \subset Z_j.$$

The proposition then follows from the case $j = p-1$, since $Q_{p-1} = K$ and $Z_{p-1} = \mathbb{Z}[\xi]$.

The case $j = 0$ is trivial, since $Z_0 = 0 = Q_0$. Assume that $j \in \{1, \dots, p-1\}$. Let $y \in Q_j \cap \mathcal{O}_K$, and write

$$y = a_0 + a_1\xi + \dots + a_{j-1}\xi^{j-1},$$

with $a_0, \dots, a_{j-1} \in \mathbb{Q}$. Then we have

$$(1 - \xi)y = a_0(1 - \xi) + \dots + a_{j-1}(\xi^{j-1} - \xi^j).$$

Let us take the trace, having Lemma 5.3.2 in mind. This yields

$$\mathrm{Tr}_{K/\mathbb{Q}}((1 - \xi)y) = a_0p.$$

Since by assumption $y \in \mathcal{O}_K$, we have $a_0p \in p\mathbb{Z}$ by Lemma 5.3.6, which implies that $a_0 \in \mathbb{Z}$. Now $\xi^{-1} = \xi^{p-1} \in \mathcal{O}_K$, and thus

$$\xi^{-1}(y - a_0) = a_1 + \dots + a_{j-1}\xi^{j-2} \in Q_{j-1} \cap \mathcal{O}_K.$$

By induction, this element belongs to Z_{j-1} , hence

$$y \in a_0\mathbb{Z} + \xi Z_{j-1} \subset Z_j.$$

This concludes the inductive proof. □

Bibliography

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