M1 Algebra 2020–2021: Commutative rings

David Harari

Table des matières

1. An introduction to rings **1**
1.1. Definitions, first properties 1
1.2. Ideals, quotient rings 3
1.3. Integral domains, fields, field of fractions 5
1.4. Principal ideal domains 7

2. Divisibility in integral domains **8**
2.1. Irreducible elements, associates 8
2.2. Unique factorization domains 10

3. Polynomial rings **13**
3.1. Reminders on polynomials in several variables 13
3.2. A-algebras 14
3.3. Noetherian rings 17
3.4. Polynomial rings are UFD 20
3.5. Symmetric polynomials 23

1. An introduction to rings

1.1. Definitions, first properties

Definition 1.1 A *ring* $(A, +, .)$ is a set A equipped with two laws '+' and '.' satisfying :

1. $(A, +)$ is an abelian group.
2. The multiplication operator '.' is associative and has an identity element (denoted 1).
3. The multiplication operator '.' is distributive with respect to + : for any x, y, z in A, we have $x(y + z) = xy + xz$ and $(y + z)x = yx + zx$.

If the multiplication operator is commutative, we say that A is a *commutative* ring.

Example 1.2 a) The zero ring $\{0\}$.

b) $(\mathbf{Z}, +, .)$, $(\mathbf{Z}/n\mathbf{Z}, +, .)$ are commutative rings.

c) A field K is by definition a commutative ring, distinct from $\{0\}$, for which any non-zero element has an inverse under multiplication (in other words, we ask that $K \setminus \{0\}$ be a commutative group).

d) The direct product $\prod_{i \in I} A_i$ of a family of rings $(A_i)_{i \in I}$ is a ring (with the obvious operations).

e) If A is a commutative [1] ring, there is also a *polynomial ring in n variables* denoted $A[X_1, \ldots, X_n]$ which is commutative. We will study this in more detail in section 3.

f) For any field K, $(M_n(K), +, .)$ is a ring, noncommutative if $n \geq 2$.

Definition 1.3 The set of *invertible* elements of a ring A are the $x \in A$ for which there exists $y \in A$ such that $xy = yx = 1$. This set is a group with respect to multiplication, generally denoted A^*.

We should be careful not to use the same "star" notation for the set of non-zero elements of A, and use instead $A \setminus \{0\}$.

Example 1.4 a) $(\mathbf{Z}/n\mathbf{Z})^*$ is the set of classes $\bar{m}$, where m is prime to n.

b) In a field K, we have by definition $K^* = K \setminus \{0\}$.

c) If K is a field, then $K[X_1, \ldots, X_n]^*$ consists of all non-zero constant polynomials (which is isomorphic to the multiplicative group K^*).

d) If K is a field, we have $M_n(K)^* = \mathrm{GL}_n(K)$.

Definition 1.5 A ring *homomorphism* (or *morphism*) $f : A \to B$ is a map from one ring to another satisfying :

1. $f(x + y) = f(x) + f(y)$.
2. $f(xy) = f(x)f(y)$.
3. $f(1) = 1$.

Note that the zero map is not a ring homomorphism since (3) is not satisfied.

1. It is possible to define a polynomial ring when A is noncommutative, but none of the usual "good" properties still hold, so in this course we stick to commutative rings.

Definition 1.6 A subset A of B is a *subring* if $(B, +, .)$ is a ring *with the same identity element as* A. This is equivalent to saying that $1 \in B$ and $(B, +)$ is a subgroup of $(A, +)$ that is stable under internal multiplication.

Be especially careful with the condition $1 \in B$; for example, the set of $(x, 0)$ with $x \in \mathbf{Z}$ is not a subring of $\mathbf{Z} \times \mathbf{Z}$, and the zero ring is not a subring of a non-zero ring. As we will see, subrings are not always of great interest ; rather, subsets known as *ideals* tend to be more useful.

1.2. Ideals, quotient rings

From this point on, we suppose that all of the rings we talk about are commutative unless otherwise stated (the theory of noncommutative rings is interesting but quite different, and has different applications).

Definition 1.7 A subset I of a commutative ring A is an *ideal* of A if it satisfies :

1. I is a subgroup of A for $+$.
2. For any x in I and a in A, we have $ax \in I$.

Be careful not to mix this notion up with subrings. In particular, an ideal of A contains 1 (resp. an invertible element of A) if and only if it is equal to A.

Example 1.8 a) $\{0\}$ and A are ideals of A. They are the only ones if A is a field.

b) The ideals of $\mathbf{Z}$ are the $n\mathbf{Z}$ with $n \in \mathbf{N}$.

c) If $f : A \to B$ is a homomorphism between commutative rings, the inverse image of an ideal of B by f is an ideal of A. In particular, the *kernel* $\ker f = f^{-1}(0)$ is an ideal of A. This implies that a field homomorphism (= homomorphism between the underlying rings) is always one-to-one. Note that if f is not onto, the direct image of an ideal of A by f is not necessarily an ideal of B (e.g., take for f the inclusion map from $\mathbf{Z}$ to $\mathbf{Q}$). However, the image $\operatorname{Im} f$ of f is a subring of B.

d) If E is a subset of a commutative ring A, then the set of elements of A of the form $a_1x_1 + \ldots + a_nx_n$ with $x_i \in E$ and $a_i \in A$ is an ideal, called the *ideal generated by* E ; this is the smallest ideal of A containing E. We will write (a) or aA for the ideal generated by an element a of A.

Remark 1.9 Unlike what happens for vector spaces, an ideal J inside an ideal I generated by n elements cannot necessarily be generated by n elements itself. For example, the ideal A can always be generated by 1 while certain others cannot be *principal* ideals (i.e., generated by a single element). In fact, it may even be that J cannot be generated by a finite number of elements. However, we will see that for certain specific types of rings (PID, Noetherian rings), these problems go away, at least partially.

Proposition 1.10 *Let A be a commutative ring and I an ideal of A. Then the quotient group A/I endowed with multiplication $\bar{a}\bar{b} := \overline{ab}$ is a ring known as a quotient ring of A by I. The canonical projection $p : A \to A/I$ is a ring homomorphism, and the identity element of A/I is $\bar{1}$.*

Proof: The only non-trivial thing to check is that the element $\overline{ab}$ of A/I does not depend on the choice of a and b. To this end, $\bar{a} = \bar{a}'$ and $\bar{b} = \bar{b}'$, so there exists i and j in I such that $a' = a + i$, $b' = b + j$, from which $a'b' = ab + (aj + ib + ij)$ with $(aj + ib + ij) \in I$.

□

We therefore immediately obtain the usual factorization theorem :

Theorem 1.11 *Let $f : A \to B$ be a ring homomorphism. Then there exists a unique ring homomorphism $\tilde{f} : A/\ker f \to B$ such that $f = \tilde{f} \circ p$, where $p : A \to A/\ker f$ is the canonical projection. Furthermore, $\tilde{f}$ is one-to-one with image $\operatorname{Im} f$, i.e., we have a ring isomorphism $A/\ker f \simeq \operatorname{Im} f$.*

Example 1.12 a) $\mathbf{Z}/n\mathbf{Z}$ is the quotient of $\mathbf{Z}$ by the ideal $n\mathbf{Z}$.

b) The function $P \mapsto P(i)$ is an onto ring homomorphism from $\mathbf{R}[X]$ to $\mathbf{C}$ whose kernel is the ideal $(X^2 + 1)$ generated by the polynomial $X^2 + 1$ (to see this, perform Euclidean division by $X^2 + 1$). We have therefore a ring isomorphism $\mathbf{R}[X]/(X^2+1) \simeq \mathbf{C}$ and $\mathbf{R}[X]/(X^2+1)$ is a field (this can even be taken as the definition of $\mathbf{C}$!).

c) If K is a field, the ring $K[X]/(X^2)$ contains a non-zero element ε (the class of X) such that $\varepsilon^2 = 0$.

Remark 1.13 It is easy to show, as in the study of subgroups of a quotient group, the following : the ideals of A/I are the J/I (these are in theory abelian groups, but we see immediately that they are ideals) where J is an ideal of A containing I. Furthermore, the quotient ring of A/I by the ideal J/I is isomorphic to A/J. More generally, if B is an ideal of A, then its image by the canonical projection $A \to A/I$ is the ideal $(B+I)/I$ of A/I. A simple

example is the ideals of $\mathbf{Z}/n\mathbf{Z}$, which are the $d\mathbf{Z}/\mathbf{Z}$ for which d divides n. We also have that $(B+I)/I$ is isomorphic to $B/(B\cap I)$ as A-modules (see the lecture notes on modules), but be careful that the notion of isomorphic ideals is not meaningful since "ideal" is a relative concept.

1.3. Integral domains, fields, field of fractions

Definition 1.14 Let A be a commutative ring and a a non-zero element of A. We say that a is a *zero divisor* in A if there exists a non-zero $b \in A$ for which $ab = 0$.

Definition 1.15 A commutative ring A is called an *integral domain* if it is non-zero and if for all a, b in A, $ab = 0$ implies $a = 0$ or $b = 0$.

In other words, an integral domain is a non-zero commutative ring with no zero divisors.

Example 1.16 a) For $n \in \mathbf{N}^*$, $\mathbf{Z}/n\mathbf{Z}$ is an integral domain if and only if n is prime.

b) Any field is an integral domain.

c) Any subring of an integral domain is an integral domain.

d) If A is an integral domain, the rings $A[X]$ and $A[X_1, \ldots, X_n]$ are integral domains. It is easy to show that for these two examples, the group of invertible elements is simply the constants of A^*.

Let us now recall the following classical result :

Proposition 1.17 *Let A be an integral domain. Then there exists a field K and a one-to-one homomorphism $i : A \to K$ such that for any one-to-one ring homomorphism from A to a field K', there exists a unique field homomorphism $j : K \to K'$ such that $f = j \circ i$. K is unique up to isomorphism, and known as the field of fractions of A. It is written* $\operatorname{Frac} A$.

This means that K is the "smallest field" containing A. Therefore, a ring is an integral domain if and only if it is a subring of a field. For example, $\operatorname{Frac} \mathbf{Z} = \mathbf{Q}$, and $\operatorname{Frac}(K[X]) = K(X)$ (the field of rational fractions in one variable). Note that the zero ring does not have a field of fractions (which justifies that by convention it is not an integral domain).

Proof (sketch): To construct $K = \operatorname{Frac} A$, consider couples (a, b) where $a \in A$ and $b \in A \setminus \{0\}$, and define (as a set) K as the quotient of the set of such couples via the equivalence relation : $(a, b) \sim (c, d)$ if and only if $ad = bc$. We then check that K, endowed with the laws

$$(a, b)(c, d) := (ac, bd); \quad (a, b) + (c, d) = (ad + bc, bd),$$

is a field (in which (a, b) corresponds to a/b) which satisfies the properties required, taking for $i(a)$ the class of $(a, 1)$.

□

Definition 1.18 An ideal I of A is said to be *prime* if A/I is an integral domain. Equivalently, this means that $A \neq I$ and $ab \in I$ implies that $a \in I$ or $b \in I$.

Examples :

1. The prime ideals of $\mathbf{Z}$ are $\{0\}$ and the $n\mathbf{Z}$ with n prime.
2. A ring A is an integral domain if and only if $\{0\}$ is prime.
3. The inverse image of a prime ideal by a ring homomorphism is a prime ideal.
4. The ideals (X_1) and (X_1, X_2) are both prime in $K[X_1, X_2]$.

Definition 1.19 An ideal I of A is said to be *maximal* if $I \neq A$ and any ideal J containing I is equal to A or I.

Proposition 1.20 *An ideal I is maximal if and only if A/I is a field.*

Proof: If I is maximal and $\bar{x}$ is non-zero in A/I, then $x \notin I$ so the ideal $I + xA$ strictly contains I ; by maximality of I, we have $A = I + xA$ and 1 is written $1 = i + xa$ with $i \in I$ and $a \in A$, which means that $\bar{1} = \bar{x}\bar{a}$, and thus $\bar{x}$ is invertible in A/I. Since $I \neq A$, the ring A/I is non-zero and its non-zero elements are invertible, i.e., A/I is a field.

In the other direction, A/I is a field, so $I \neq A$, and any ideal J of A strictly containing I has an element $x \notin I$. Thus $\bar{x}$ is invertible in A/I, so $\bar{1} = \bar{x}\bar{a}$ with $a \in A$, and thus $1 = xa + i$ with $i \in I \subset J$ and $x \in J$. Hence, $1 \in J$ and $J = A$.

□

Remark 1.21 In general, the inverse image of a maximal ideal by a ring homomorphism is not a maximal ideal. For example, the inverse image of $\{0\}$ by the inclusion map $\mathbf{Z} \to \mathbf{Q}$ is $\{0\}$, which is not a maximal ideal of $\mathbf{Z}$ (though it is one of $\mathbf{Q}$ since $\mathbf{Q}$ is a field). This is what leads to the need in algebraic geometry to consider the set of prime ideals of a commutative ring rather than the set of its maximal ideals, though the latter is in theory easier to understand [2].

The following theorem is useful for general theoretical questions. [3]

Theorem 1.22 (Krull) *In a commutative ring*[4] *A, any ideal $I \neq A$ is contained in a maximal ideal.*

Proof: The set of ideals of A containing I and different from A is non-empty and it is an inductive ordered set, since if $(I_i)_{i \in I}$ is a totally ordered family of proper ideals of A, its union is still an ideal (since the family is totally ordered) different to A (since it does not contain 1). The result follows by applying Zorn's lemma.

□

1.4. Principal ideal domains

Definition 1.23 A commutative ring A is said to be a principal ideal domain (PID) if it is an integral domain and if all of its ideals are principal, i.e., of the form $(a) = aA$ with $a \in A$.

In practice, we often determine whether a ring is a PID using the following concept.

Definition 1.24 An integral domain A is said to be *Euclidean* if there exists a function $v : A - \{0\} \to \mathbf{N}$ ("Euclidean function") such that if a, b are in A with $b \neq 0$, then there exists q, r in A where $a = bq + r$, with r satisfying : $r = 0$ or $v(r) < v(b)$.

Note that we are not requiring uniqueness in this "Euclidean division".

2. Hilbert's Nullstellensatz (theorem of zeros) for instance shows that the maximal ideals of $\mathbf{C}[X_1, \ldots, X_n]$ are in bijection with $a \in \mathbf{C}^n$ via the map that sends a given a to the set of polynomials whose a is a zero–see tutorials.

3. In particular when we work with non-Noetherian rings, often the case in analysis.

4. Note that the existence of an identity element in A is crucial for this theorem. An analogous result holds for noncommutative rings by replacing "ideal" with "left ideal", "right ideal", or "two-sided ideal".

Example 1.25 a) The ring $\mathbf{Z}$ is Euclidean with $v(x) = |x|$.

b) If K is a field, the ring $K[X]$ is Euclidean with $v(P) = \deg P$.

c) We can show that $\mathbf{Z}[i]$ is Euclidean with $v(x) = |x|^2$; in this case there is not uniqueness in the Euclidean division.

Theorem 1.26 *If A is Euclidean, it is a PID.*

Proof: Let I be a non-zero ideal of A, and choose a non-zero b in I with $v(b)$ minimal. Then any a from I can be written $a = bq + r$ with $r = 0$ or $v(r) < v(b)$. The latter is however impossible since $r \in I$, so $a \in (b)$. Hence, $I = (b)$.

□

The result is not true in the other direction ; there are well-known counter examples that are not entirely obvious ($\mathbf{Z}[\frac{1+i\sqrt{19}}{2}]$, $\mathbf{R}[X, Y]/(X^2 + Y^2 + 1)$; see the tutorials and [1], chapter II, §5).

Example 1.27 a) The rings $\mathbf{Z}$ and $K[X]$ (where K is a field) are Euclidean and therefore are PID.

b) The ring $\mathbf{Z}/4\mathbf{Z}$ is not a PID (even though all of its ideals are) since it is not an integral domain !

c) Be careful to remember that A being a PID does not at all imply that $A[X]$ is (in fact, this is only true if A is a field). For instance, we can show that in $K[X_1, X_2]$ (where K is a field), the ideal I generated by X_1 and X_2 is not principal (if it were, a generator of I should divide X_1 and X_2, and therefore be a constant polynomial, so we would have $I = A$; however, $1 \notin I$).

2. Divisibility in integral domains

2.1. Irreducible elements, associates

In this section, A denotes a commutative integral domain.

Definition 2.1 Suppose a and b are in A. We say that a *divides* b and write $a|b$ if there exists $c \in A$ such that $b = ac$. In terms of ideals, this is equivalent to $(a) \supset (b)$.

In particular, 0 only divides itself, while an element of A^* divides all of the elements of A.

Proposition 2.2 *Suppose that a and b are in A. Then ($a|b$ and $b|a$) if and only if there exists $u \in A^*$ such that $a = ub$. We then say that a and b are* associates.

Proof: If $a = ub$ with $u \in A^*$, then $b|a$ and $b = u^{-1}a$, so $a|b$. In the other direction, if $a = bc$ and $b = ad$ with c, d in A, then $a = adc$, so $dc = 1$ since A is an integral domain, and thus $c \in A^*$.

□

Being associates in A is equivalent to being associates in $A \setminus \{0\}$.

Definition 2.3 We say that an element p in A is *irreducible* if it satisfies :

1. p is *not* invertible in A,
2. If $p = ab$ with a and b in A, then a or b is invertible.

The second condition means that the only divisors of p are its associates and the invertible elements of A. Make sure to remember that by convention, the elements of A^* are not irreducible.

Example 2.4 a) The irreducible elements in $\mathbf{Z}$ are the $\pm p$ where p is prime.

b) If K is a field, the polynomials of degree 1 as well as those of degree 2 or 3 that have no roots, are irreducible in $K[X]$ (though the reverse is false in $\mathbf{Q}[X]$ for example).

c) The irreducible elements of $\mathbf{C}[X]$ are the polynomials of degree 1, those of $\mathbf{R}[X]$ are the polynomials of degree 1 and the polynomials of degree 2 without real-valued roots. We will see in the course on fields that in $\mathbf{Q}[X]$ or $F[X]$ with F a finite field, there are irreducible polynomials of any degree.

Definition 2.5 We say that two elements a and b in A are *coprime* if their only common divisors are the elements of A^*.

There is an analogue to Bézout's theorem when A is a PID :

Proposition 2.6 *Let A be a PID. Then, a and b in A are coprime if and only if there exist elements u and v in A such that $ua + vb = 1$ (i.e., if $A = (a, b)$, the ideal generated by a and b).*

Proof: If $1 = ua + bv$, then any common divisor of a and b divides 1 and is thus invertible (this implication is true in any commutative ring). In the other direction, if a and b are coprime, then the ideal (a, b) is written (d) with $d \in A$ since A is a PID. In particular, d divides a and b and is thus invertible, so $(d) = A$.

□

Note that in the ring $A = K[X, Y]$, the polynomials X and Y are coprime but do not satisfy $A = (X, Y)$ (e.g., since any polynomial in (X, Y) equals zero at $(0, 0)$). Thus, $K[X, Y]$ is not a PID.

2.2. Unique factorization domains

It would be nice to have a reasonable divisibility theorem for more general rings than PID. This desire motivates the introduction of the notion of unit factorization domain.

Definition 2.7 A commutative ring A is said to be a *unique factorization domain* (UFD) if it satisfies :

1. A is an integral domain.
2. Any non-zero a in A can be written as a product

$$a = up_1...p_r$$

with $u \in A^*$ and irreducible p_i. [5]

3. The decomposition is unique in the following sense : if $a = vq_1...q_s$ is another decomposition, then $r = s$ and there exists a permutation σ of $\{1, \ldots, r\}$ such that for any i in $\{1, \ldots, r\}$, the elements p_i and $q_{\sigma(i)}$ are associates.

Remarks: a) Like for PID, do not forget that A must be an integral domain.

b) Another, often more convenient formulation of the uniqueness condition is the following : fix an *irreducible representation* $\mathcal{P}$ of A, i.e., a set of irreducible elements for which each irreducible element of A is associate with one and only one element of $\mathcal{P}$. Then any non-zero a in A can be written uniquely as $a = u \prod_{p \in \mathcal{P}} p^{n_p}$ with $u \in A^*$, and $(n_p)_{p \in \mathcal{P}}$ is almost-zero set of natural numbers. We then write $n_p = v_p(a)$.

5. If a is not invertible, the product of the p_i's that appears is not an empty one ; we can then replace up_1 by p_1 and thus do without the invertible element u in the decomposition.

c) Most integral domains (notably Noetherian ones, see below) that we come into contact with in algebra have an irreducible decomposition[6]. The strong property is that of uniqueness.

Example 2.8 a) $\mathbf{Z}$ is a UFD (take for $\mathcal{P}$ the set of prime numbers).

b) $K[X]$ is a UFD (we can take for $\mathcal{P}$ the set of monic irreducible polynomials).

c) We will see that more generally, any PID is a UFD, but the converse is false, e.g., take $K[X_1, \ldots, X_n]$.

d) The ring $A = \mathbf{Z}[i\sqrt{5}] \simeq \mathbf{Z}[T]/(T^2+5)$, which is the subring of $\mathbf{C}$ made up of the $a + bi\sqrt{5}$ with $a, b \in \mathbf{Z}$, is an integral domain but not a UFD. To see this, for any $z = a + ib$ in, set :

$$N(z) = z\bar{z} = a^2 + 5b^2,$$

which we call the *norm* of z. Then, we have $N(z) \in \mathbf{N}$, which implies that all $z \in A^*$ satisfy $N(z) = 1$ and thus $z \in \{\pm 1\}$ (in the other direction, 1 and -1 are indeed in A^*). Then, the elements 3, $2 - i\sqrt{5}$, and $2 + i\sqrt{5}$ are irreducible since their norms are equal to 9, and A does not contain an element of norm 3, which means that if an element z of norm 9 is written $z = z_1 z_2$, then $9 = N(z_1)N(z_2)$ and thus $N(z_1) = 1$ or $N(z_2) = 1$, which implies that z_1 or z_2 is invertible.

Nevertheless, $9 = 3 \times 3 = (2 - i\sqrt{5})(2 + i\sqrt{5})$ in A, which indeed gives two different decompositions since 3 is not an associate of either $2 - i\sqrt{5}$ or $2 + i\sqrt{5}$.

We see in passing that a quotient of a UFD by a prime ideal does not always remain a UFD (we will see in the next chapter that $\mathbf{Z}[X]$ is a UFD) ; this also does not work for subrings, since every integral domain is a subring of a field, which is obviously a UFD.

The following proposition gives conditions equivalent with being a UFD when we know that an irreducible decomposition exists.

Proposition 2.9 *Let A be an integral domain in which any non-zero element has an irreducible decomposition. Then the following conditions are equivalent :*

1. *A is a UFD.*
2. *If $p \in A$ is irreducible, then the ideal (p) is prime.*
3. *Let a, b, c be in $A \setminus \{0\}$. If a divides bc and is prime to b, then a divides c ("Gauss's lemma").*

6. It is common to use the expression "irreducible decomposition" to mean "decomposition as a product of an invertible element with irreducible ones".

Proof: (3) implies (2) : First, $(p) \neq A$ because p is not invertible as it is not irreducible. If now p divides ab and not a, then p is prime to a since p is irreducible (thus a non-invertible common divisor of a and p would be associate with p, and p would divide a), so p divides b according to (3). Thus (p) is a prime ideal.

(2) implies (1) : Let $\mathcal{P}$ be an irreducible representation. If $u\prod_{p\in\mathcal{P}} p^{m_p} = v\prod_{p\in\mathcal{P}} p^{n_p}$ are two decompositions, then the condition $m_q > n_q$ for a certain q in $\mathcal{P}$ would imply that q divides $\prod_{p\in\mathcal{P},p\neq q} p^{n_p}$ and thus one of its factors, according to (2). However, q cannot divide p if $p \in \mathcal{P}$ and distinct from q since $\mathcal{P}$ is an irreducible representation. Thus, $m_p = n_p$ for all $p \in \mathcal{P}$, so $u = v$ since A is integral.

(1) implies (3) : we decompose a uniquely as

$$a = u\prod_{p\in\mathcal{P}} p^{v_p(a)}, \quad u \in A^*,$$

and do the same for b and c. Then for any p in $\mathcal{P}$, $v_p(a) \leq v_p(b) + v_p(c)$ (since a divides bc) and $v_p(b) > 0$ implies that $v_p(a) = 0$ (since a is prime to b), so $v_p(a) \leq v_p(c)$ always. Thus, a divides c.

□

Proposition 2.10 *If A is a UFD, then non-zero elements a and b in A have a greatest common divisor that is well defined up to multiplication by an element of a^*.*

Remember that a greatest common divisor of a and b is a common divisor d of a and b for which any other common divisor divides d; here, "greatest" refers to the partial order "divides" on the quotient set of $A \setminus \{0\}$ by the equivalence relation "being associated".

The proof of the proposition is immediate : decompose a and b using a system $\mathcal{P}$ of irreducible elements. A greatest common divisor is $\prod_{p\in\mathcal{P}} p^{\min(v_p(a),v_p(b))}$ (proceed similarly for any family of elements of $A \setminus \{0\}$). This can then be extended to a family of elements of A, for which the greatest common divisor is the same as that of the previous family, possibly with 0 removed (the greatest common divisor of the empty family or the family that is nothing but 0, is 0). Note that two elements of A are coprime if and only if their greatest common divisor is 1. On the other hand, if A is a PID, we can take as greatest common divisor of a and b any generator of the ideal $(a, b) = aA + bA$ (this can be immediately extended to any family of elements of A).

We also have a smallest common multiple of a and b by taking

$$\prod_{p\in\mathcal{P}} p^{\max(v_p(a),v_p(b))},$$

a notion that can be extended to a *finite*[7] family of elements of $A \setminus \{0\}$. If A is a PID, the smallest common multiple of (a, b) can be obtained by taking a generator of the ideal $aA \cap bA$ (and similarly for a finite family of elements of A).

For the existence of the decomposition, we need a finiteness property which is at the origin of the notion of Noetherian rings. Historically, this notion was introduced to generalize a property of polynomial rings, which we are now going to study in detail.

3. Polynomial rings

Let A continue to denote a commutative ring. Recall that a family of elements of A is said to be *almost-zero* if all of its elements are zero except for a finite number. If I is a set, we denote by $A^{(I)}$ the set of almost-zero families of elements of A indexed by I.

3.1. Reminders on polynomials in several variables

For any integer $n \geq 2$, we define the ring $A[X_1, \ldots, X_n]$ by induction using the formula

$$A[X_1, \ldots, X_n] := (A[X_1, \ldots, X_{n-1}])[X_n].$$

In other words, $A[X_1, \ldots, X_n]$ is the polynomial ring in one variable (denoted X_n) over the commutative ring $A[X_1, \ldots, X_{n-1}]$. The elements of $A[X_1, \ldots, X_n]$ are called *polynomials in n variables* (with coefficients in A).

It can easily shown using induction on n that an element P in the commutative ring $A[X_1, \ldots, X_n]$ can be written uniquely as :

$$P = \sum_{(i_1,\ldots,i_n)\in\mathbf{N}^n} a_{i_1,\ldots,i_n} X_1^{i_1} \ldots X_n^{i_n}, \tag{1}$$

where $(a_{i_1,\ldots,i_n})_{(i_1,\ldots,i_n)\in\mathbf{N}^n}$ is an almost-zero family of elements of A indexed by $\mathbf{N}^n$ (with the convention $X_i^0 = 1$). This means that for each $r \in \{1, \ldots, n\}$ we can also see the elements of $A[X_1, \ldots, X_n]$ as elements of $(A[X_1, \ldots, \widehat{X_r}, \ldots, X_n])[X_r]$ (the notation $A[X_1, \ldots, \widehat{X_r}, \ldots, X_n]$ signifies that we omit the term X_r).

7. Or to any family if we accept that 0 is the smallest common multiple of a family that has no non-zero common multiple.

Definition 3.1 We call the elements of $\mathbf{N}^n$ *exponents*. An exponent $(i_1, \ldots, i_n)$ is said to *appear in* P if, written in the form (1), the coefficient $a_{i_1,\ldots,i_n}$ is non-zero. If $\alpha = (\alpha_1, \ldots, \alpha_n)$ is an exponent, set $|\alpha| = \sum_{i=1}^n \alpha_i$. We say that P is *homogeneous of degree* d if all of the exponents α that appear in P satisfy $|\alpha| = d$.

In particular, any polynomial F in n variables can be written uniquely as $P = \sum_{d \geq 0} F_d$, with F_d homogeneous of degree d and the family of F_d being non-zero.

The following proposition is easily proved starting from the $n = 1$ case :

Proposition 3.2 *a) Let $P \in A[X_1, \ldots, X_n]$ be non-zero. Suppose that there exists $i \in \{1, \ldots, n\}$ such that the term with the largest degree in P seen as a polynomial in $(A[X_1, \ldots, \widehat{X_i}, \ldots, X_n])[X_i]$ is of the form $aX_1^{i_1} \ldots X_r^{i_r}$, where a does not divide zero in A. Then P does not divide zero in $A[X_1, \ldots, X_n]$.*

b) The ring $A[X_1, \ldots, X_n]$ is an integral domain if and only if A is an integral domain.

c) If A is an integral domain, the group of invertible elements of $A[X_1, \ldots, X_n]$ is the group A^* of invertible constant polynomials in A.

3.2. A-algebras

Definition 3.3 An *A-algebra* is a commutative ring [8] B that comes equipped with a (not necessarily one-to-one) ring homomorphism $\varphi : A \to B$.

Note that B is therefore endowed with an external law (which makes it an A-module) defined by $a.b = \varphi(a)b$ for all $a \in A, b \in B$. This leads to another definition :

Definition 3.4 A *homomorphism of A-algebras* $f : B \to C$ is a ring homomorphism that also satisfies $f(a.b) = a.f(b)$ for any $a \in A, b \in B$. A sub-A-algebra of B is a subring C of B that also satisfies $a.c \in C$ for any $a \in A, c \in C$.

Note that the image of a homomorphism $f : B \to C$ of A-algebras is a sub-A-algebra of B, and the kernel $\ker f$ is an ideal of the ring B. Factorization theorem 1.11 can be immediately extended to homomorphisms of A-algebras.

8. The same notion can be defined without supposing that B is commutative, but in this course we only deal with commutative A-algebras.

Example 3.5 a) Any commutative ring B is automatically a $\mathbf{Z}$-algebra via the homomorphism $n \mapsto n.1$ from $\mathbf{Z}$ to B.

b) The ring $A[X_1, \ldots, X_n]$ is an A-algebra via the inclusion map $A \to A[X_1, \ldots, X_n]$.

c) If $r \in \mathbf{N}^*$, the product ring A^r is an A-algebra via the homomorphism $a \mapsto (a, a, \ldots, a)$ from A to A^r.

Proposition 3.6 (The universal property of polynomial algebras) *Let B be a commutative ring and $\varphi : A \to B$ a ring homomorphism. Suppose that $b_1, \ldots, b_n$ are elements of B. Then there exists a unique ring homomorphism $f : A[X_1, \ldots, X_n] \to B$ satisfying :*

1. *For any constant polynomial a of $A[X_1, \ldots, X_n]$, we have $f(a) = \varphi(a)$.*
2. *We have $f(X_i) = b_i$ for all $i \in \{1, \ldots, n\}$.*

If we consider B as an A-algebra via φ, an equivalent formulation consists of saying that there exists a unique homomorphism of A-algebras $f : A[X_1, \ldots, X_n] \to B$ that maps X_i onto b_i. Once the homomorphism φ has been fixed, we can denote (for any polynomial P of $A[X_1, \ldots, X_n]$) $P(b_1, \ldots, b_n)$ the element of B obtained by taking the image of P by the homomorphism f in the theorem. We get this by "substituting in" $b_1, \ldots, b_n$ for the variables $X_1, \ldots, X_n$, then using the A-algebra structure of B.

Proof: We prove the result by induction on $n \geq 1$. Suppose that $n = 1$. Then, the homomorphism $f : A[X_1] \to B$ mus necessarily be defined by the formula

$$f(\sum_{n \in \mathbf{N}} \alpha_n X_1^n) = \sum_{n \in \mathbf{N}} \varphi(\alpha_n) b_1^n.$$

Inversely, we see immediately that f satisfies $f(1) = 1$ and $f(P+Q) = f(P) + f(Q)$ for any polynomials P, Q in $A[X_1]$. If $P = \sum_n \alpha_n X_1^n$ and $Q = \sum_n \beta_n X_1^n$ are polynomials, then $PQ = \sum_n \gamma_n X_1^n$ with $\gamma_n = \sum_{p+q=n} \alpha_p \beta_q$, from which

$$f(PQ) = \sum_n \varphi(\gamma_n) b_1^n = \sum_n \sum_{p+q=n} \varphi(\alpha_p)\varphi(\beta_q) b_1^p b_1^q =$$

$$\sum_n \sum_{p+q=n} (\varphi(\alpha_p) b_1^p)(\varphi(\beta_q) b_1^q) = \sum_{p,q} (\varphi(\alpha_p) b_1^p)(\varphi(\beta_q) b_1^q) =$$

$$(\sum_n \varphi(\alpha_n) b_1^n))(\sum_n \varphi(\beta_n) b_1^n)) = f(P) f(Q),$$

which shows that f is indeed a ring homomorphism.This completes the proof for $n = 1$.

We now suppose that the result is true for $n-1$ and show that it is also true for n. By the induction hypothesis, we have a unique ring homomorphism $\psi : A[X_1, \ldots, X_{n-1}] \to B$ such that $\psi(X_i) = b_i$ for $1 \leq i \leq n-1$ and ψ coincides with φ on the constant polynomials. From the $n = 1$ case (applied to polynomials in one variable with coefficients in the ring $A[X_1, \ldots, X_{n-1}]$), we have therefore a unique ring homomorphism $f : A[X_1, \ldots, X_n] \to B$ which coincides with ψ on the polynomials of $A[X_1, \ldots, X_{n-1}]$ and satisfies $f(X_n) = b_n$. It is thus clear that f works and is the unique solution to the problem.

□

Example 3.7 Let $P, Q_1, \ldots, Q_n \in A[X_1, \ldots, X_n]$. We have the polynomial $R = P(Q_1, \ldots, Q_n)$ obtained by substituting the Q_i into the X_i. More precisely, the polynomial R is the image of P by the unique homomorphism of A-algebras which maps X_i onto Q_i. In particular, we have $P = P(X_1, \ldots, X_n)$ by definition (which justifies the use of the two different notations!). When $n = 1$, we often write $P \circ Q$ for the polynomial of $A[X]$ defined by $(P \circ Q)(X) = P(Q(X))$.

Definition 3.8 Let B be an A-algebra and suppose S is a subset of B. The sub-A-algebra of B *generated by* S is the set C of $P(x_1, \ldots, x_n)$ with $n \in \mathbf{N}^*$, $x_1, \ldots, x_n \in S$ and $P \in A[X_1, \ldots, X_n]$.

It is easy to see immediately that C is the smallest sub-A-algebra of B containing S.

Proposition 3.9 *Suppose B is an A-algebra. Then there exists a finite subset $S = \{b_1, \ldots, b_n\}$ of B that generates B if and only if B is isomorphic to the quotient of $A[X_1, \ldots, X_n]$ by an ideal I. In this case we say that the A-algebra B is generated by a finite subset.* [9]

Proof: It is easy to see that the A-algebra $A[X_1, \ldots, X_n]/I$ is generated by the images of $X_1, \ldots, X_n$ via the canonical projection, which therefore make up a finite generating subset. Conversely, if B is an A-algebra generated by $S = \{b_1, \ldots, b_n\}$, then according to proposition 3.6, there exists a (unique) homomorphism of A-algebras $f : A[X_1, \ldots, X_n] \to B$ that maps X_i onto b_i. The image of f contains the b_i and is thus equal to B (which is generated by the b_i). The result is proved by invoking the factorization theorem.

□

9. We can also say that it is "of finite type" but this brings in ambiguity between being of finite type as an A-algebra or an A-module (a notion we will see in the chapter on modules). Typically, if for example K is a field, $K[X]$ is of finite type as a K-algebra but not as a K-vector space.

Remark 3.10 If I is some (not necessarily finite) subset, we can still define the ring $A[(X_i)_{i\in I}]$ by considering the polynomials P given in the form (1) for some multi-indices $(i_1,\dots,i_n)$ in I^n, but where n is any positive integer (which depends on the polynomial P), with addition and multiplication of polynomials being defined using the fact that there exists a finite subset J of I for which the two polynomials in question are in $A[(X_j)_{j\in J}]$. The ring $A[(X_i)_{i\in I}]$ is in some sense the union [10] of the $A[(X_j)_{j\in J}]$ where J is finite. We can also define $A[(X_i)_{i\in I}]$ as the set of almost-zero families of elements of $A^{(I)}$ with the usual addition and multiplication induced by those of the polynomials of $A[(X_j)_{j\in J}]$ for J a finite subset of I, the latter being seen as almost-zero families of elements of A^J. The universal property of proposition 3.6 remains true for $A[(X_i)_{i\in I}]$ when I is infinite by defining f on each $A[(X_j)_{j\in J}]$ with finite J.

3.3. Noetherian rings

Proposition 3.11 *Let A be a commutative ring. Then the following properties are equivalent :*

1. *Every ideal of A is generated by a finite number of elements.*
2. *Any increasing sequence (for the inclusion relation) $(I_n)_{n\in\mathbf{N}^*}$ of ideals is stationary.*
3. *Any non-empty family of ideals of A has a maximal element for the inclusion relation.*

We say that A is Noetherian *if these properties hold.*

Proof: (1) implies (2) : let (I_n) be such a sequence ; then the union I of the I_n is still an ideal since the familly (I_n) is totally ordered for the inclusion relation. Let $x_1,\dots,x_r$ be elements of I that generate it ; then each x_i is in one of the I_n, so there exists an n_0 (the largest of the corresponding indices) such that I_{n_0} contains all of them. Thus, $I = I_{n_0}$ and the sequence (I_n) is stationary at I_{n_0}.

(2) implies (3) : if a non-empty family of ideals of A does not have a maximal element, we can construct by induction a strictly increasing infinite sequence of ideals of A, which contradicts (2).

(3) implies (1) : let I be an ideal of A ; then the family E of ideals $J \subset I$ that are generated by a finite number of elements is non-empty (it contains $\{0\}$). Let J_0 be a maximal element of E. Then for any x in I, the ideal $J_0 + xA$

10. More precisely, it is the *inductive limit* or *colimit*.

is also in E, so $J_0 + xA = J_0$ due to maximality. This signifies that $x \in J_0$. Thus, $I = J_0$ and I is generated by a finite number of elements. □

Example 3.12 a) All PID are Noetherian via (1).

b) If A is Noetherian, any quotient of A is too due to (1) seeing as the ideals of A/I are the J/I, where J is an ideal of A containing I (if J is an ideal generated by $a_1, \ldots, a_r$, then J/I is generated by the images of $a_1, \ldots, a_r$ via the canonical projection).

c) The ring $K[(X_n)_{n\in\mathbf{N}^*}]$ is not Noetherian since $(X_1) \subset (X_1, X_2) \subset \ldots (X_1, \ldots, X_n) \subset \ldots$ forms a strictly increasing infinite sequence of ideals. [11]

d) A subring of a Noetherian ring is not necessarily Noetherian (take a non-Noetherian integral domain such as $K[(X_n)_{n\in\mathbf{N}^*}]$, which is a subring of its field of fractions ; and a field is obviously a Noetherian ring).

Most of the rings we work with in algebra are Noetherian given the following theorem :

Theorem 3.13 (Hilbert) *Let A be a Noetherian ring. Then $A[X]$ is a Noetherian ring.*

Proof: Let I be an ideal of $A[X]$ and $n \in \mathbf{N}$; we note $d_n(I)$ the subset of A made up of 0 and the main coefficient of the elements of degree n in I. It is clear that I is an ideal of A, and that $I \subset J$ implies $d_n(I) \subset d_n(J)$. We also have the two following properties :

i) If $n \in \mathbf{N}$, then $d_n(I) \subset d_{n+1}(I)$: in effect, it suffices to see that if $P \in I$, then $XP \in I$.

ii) If $I \subset J$, then the fact that $d_n(I) = d_n(J)$ for all $n \in \mathbf{N}$ implies that $I = J$: in effect, if J strictly contains I, we select a polynomial P in $J \setminus I$ which has minimal degree r ; since $d_r(I) = d_r(J)$, I contains a polynomial Q of degree r which has the same main coefficient as P, but then $P - Q$ is in $J \setminus I$ and of degree $< r$, which is a contradiction.

Given these, let $(I_n)_{n\in\mathbf{N}^*}$ be an increasing sequence of ideals of $A[X]$. Since A is Noetherian, the family of $d_k(I_n)$ for $k \in \mathbf{N}$ and $n \in \mathbf{N}^*$ has a maximal element, which we denote $d_l(I_m)$. Also, for each $k \leq l$, the sequence of ideals $(d_k(I_n))_{n\in\mathbf{N}^*}$ is increasing, and thus stationary, i.e., there exists an n_k such that for $n \geq n_k$, we have $d_k(I_n) = d_k(I_{n_k})$. Now define N as the largest of the integers $m, n_0, n_1, \ldots, n_l$, and we show that for any $n \geq N$, we

11. This ring is a UFD ; this can be easily deduced from the fact, proven later, that $K[X_1, \ldots, X_n]$ is a UFD, since a fixed element of $K[(X_n)_{n\in\mathbf{N}^*}]$ is in $K[X_1, \ldots, X_n]$ for a certain n.

have $d_k(I_n) = d_k(I_N)$, which will complete the proof with the help of (i) and (ii) above. We deal with two cases separately :

a) If $k \leq l$, then $d_k(I_N) = d_k(I_{n_k}) = d_k(I_n)$ by the definition of n_k since n and N are both $\geq n_k$.

b) If $k \geq l$, then $d_k(I_N)$ and $d_k(I_n)$ both contain $d_l(I_m)$ according to (i) above, so by the maximality of $d_l(I_m)$ they are equal to it, and in particular, $d_k(I_N) = d_k(I_n)$.

□

Corollary 3.14 *1. If A is a Noetherian ring, then the ring $A[X_1, \ldots, X_n]$ is also Noetherian.*

2. If A is a Noetherian ring, any ring B that is an A-algebra generated by a finite subset is Noetherian.

Proof: (1) is a consequence of the previous theorem ; use induction on n.

(2) follows from (1) and proposition 3.9, using the fact that the quotient of a Noetherian ring is a Noetherian ring.

□

We now look at the existence of decompositions into products of irreducible elements in Noetherian integral domains.

Proposition 3.15 *Let A be a Noetherian integral domain. Then any non-zero element x of A can be written : $x = up_1...p_r$ with $u \in A^*$ and irreducible p_i's.*

Proof: Let $\mathcal{F}$ be the set of ideals of A of the form xA with x non-invertible and not able to be written as a product of irreducible elements. If $\mathcal{F}$ were non-empty, it would have a maximal element $(a) = aA$. In particular a would then not be irreducible, and since it is not invertible, it is of the form $a = bc$ with b and c in A not associates with a. However, the ideals (b) and (c) strictly contain (a), so by maximality, b and c can be broken down into products of irreducible elements, which contradicts the fact that a cannot be written as a product of irreducible elements.

□

Remark: Being either a Noetherian ring or a UFD does not imply that the other is true. For instance, if K is a field, $K[X_n]_{n \in \mathbf{N}^*}$ is a UFD but not a Noetherian one. Also, $\mathbf{Z}[X]/(X^2 + 5)$ is a Noetherian ring via theorem 3.13, and we have already seen that this is not a UFD.

Corollary 3.16 *If A is a PID, it is also a UFD.*

Proof: We have just seen the existence of the decomposition into irreducible elements. Also, if $p \in A$ is irreducible, then the ideal (p) is maximal because if $I = (a)$ contains (p), then a divides p, which implies that a is invertible or associate with p, i.e., $(a) = (p)$ or $(a) = A$. In particular (p) is a prime ideal and the result follows from proposition 2.9. [12]

□

3.4. Polynomial rings are UFD

We have seen that A being a PID does not in any way imply that $A[X]$ is a PID (this is only true if A is a field). We will see however that the analogous relation does hold for UFD. We begin with a definition :

Definition 3.17 Let A be a UFD. The *content* (denoted $c(P)$) of a polynomial P is the greatest common divisor of its coefficients. P is said to be *primitive* if $c(P) = 1$.

Note that the content is well-defined for multiplication up to an invertible element of A; however, the ideal it generates is well-defined.

Lemma 3.18 (Gauss) *For all P, Q in $A[X]$, we have $c(PQ) = c(P)c(Q)$ (still modulo A^*).*

Proof: First, suppose that P and Q are primitive and let us show that PQ is primitive. If it were not, there would exist some irreducible element p of A that divides all of the coefficients of PQ. Since P and Q are primitive, each has at least one coefficient not divisible by p. Let a_{i_0} (resp. b_{j_0}) be the coefficient of P (resp. Q) non-divisible by p with the smallest index. Then the coefficient with index $i_0 + j_0$ of PQ is a sum of terms divisible by p and $a_{i_0}b_{j_0}$, so it is not divisible by p since (p) is prime given that A is a UFD. This contradicts the fact that all of the coefficients of PQ are divisible by p.

We can then get back to primitive P and Q by applying the previous result to $P/c(P)$ and $Q/c(Q)$.

□

An important result follows from this lemma :

12. We say that an integral ring is *of dimension 1* if any non-zero prime ideal is maximal. We have just seen that a PID is of dimension 1. However, $\mathbf{Z}[i\sqrt{5}]$ is of dimension 1 without being a PIS (or even a UFD), and $K[X_1, X_2]$ is a UFD without being of dimension 1.

Theorem 3.19 *Let A be a UFD with field of fractions K. Then the irreducible elements of $A[X]$ fall into two categories :*

i) Constant polynomials $P = p$ with p irreducible in A.

ii) Primitive polynomials of degree ≥ 1 that are irreducible in $K[X]$.

In particular, for a primitive polynomial of $A[X]$, it turns out to be the same thing to be irreducible in $A[X]$ and in the PID $K[X]$ (which is not at all obvious seeing as there would initially appear to be more possible decompositions in $K[X]$). Be careful when it comes to non-primitive polynomials : 2 is irreducible in $\mathbf{Z}[X]$ but not in $\mathbf{Q}[X]$ (though it is invertible) while $2X$ is irreducible in $\mathbf{Q}[X]$ but not in $\mathbf{Z}[X]$.

Proof: Since $A[X]^* = A^*$, it is clear that a constant polynomial $P = p$ is irreducible if and only if p is irreducible in A. If then P is a primitive polynomial of degree ≥ 1 of $A[X]$ that is irreducible in $K[X]$, then writing $P = QR$ with Q, R in $A[X]$ implies using the previous lemma that $c(Q)$ and $c(R)$ are invertible. Furthermore, since one of the polynomials Q and R must be constant (since P is irreducible in $K[X]$), it is an invertible constant in A. Hence P is indeed irreducible in $A[X]$ (but not invertible since it is of degree at least 1).

It remains to show that a polynomial P of degree ≥ 1 that is irreducible in $A[X]$ is primitive, and irreducible in $K[X]$. P is primitive because $c(P)$ divides P in $A[X]$ and they are not associates due to differences in degree. It remains to show that P (which is not invertible in $K[X]$) is irreducible in $K[X]$. Suppose that $P = QR$ in $K[X]$; we can then write $Q = Q_1/q$ and $R = R_1/r$ with q, r in A and Q_1, R_1 in $A[X]$. Then, setting $a = qr$, we get that $aP = Q_1R_1$, and moving to contents : $a = c(Q_1)c(R_1)$ (modulo A^*). Thus, $P = u\frac{P_1}{C(P_1)}\frac{Q_1}{C(Q_1)}$ with $u \in A^*$. Since P is irreducible in $A[X]$, one of the polynomials $\frac{P_1}{C(P_1)}$, $\frac{Q_1}{C(Q_1)}$ in $A[X]$ must be invertible and thus constant, and one of the polynomials Q, R must be constant, which concludes the proof. □

We can now state the theorem.

Theorem 3.20 *If A is a UFD, then $A[X]$ is a UFD.*

Proof: We must first show existence of the decomposition (if A is also a Noetherian ring, we have this already via theorem 3.13 and proposition 3.15). Writing $P = c(P)P_1$ and breaking down $c(P)$ into a product of irreducible elements in A, we can get P primitive. We thus decompose P (which we can suppose non-constant) in the PID $K[X]$ as $P = P_1...P_r$, or rather $aP =$

$Q_1...Q_r$ with $Q_i \in A[X]$, $a \in A$, and Q_i irreducible in $K[X]$. Moving to contents, we obtain $a = c(Q_1)...c(Q_r)$ (modulo A^*) and from the previous theorem, $P = \prod_{i=1}^{r} \frac{P_i}{c(P_i)}$ is a decomposition of P into a product of irreducible elements of $A[X]$, since each $\frac{P_i}{c(P_i)}$ is a primitive polynomial of $A[X]$ that is irreducible in $K[X]$ (equal to the product of Q_i with a constant from K^*).

Given the result in proposition 2.9, it therefore suffices to show that if $P \in A[X]$ is irreducible, then (P) is a prime ideal. If $P = p$ is an irreducible constant in $A[X]$, this is immediate (by direct proof, or by noting that $A[X]/(p)$ is isomorphic to $(A/(p))[X]$, which is an integral domain since (p) is a prime ideal in A). Hence, suppose that P is primitive and of degree at least 1, and thus irreducible in $K[X]$ due to the previous theorem. Then, if P divides the product QR of two polynomials in $A[X]$, it divides either Q or R in $K[X]$ since $K[X]$ is a PID. Suppose it divides Q. There therefore exists a in A such that $aQ = SP$ with $S \in A[X]$. Thus, $ac(Q) = c(S)$ since P is primitive, and a divides $c(S)$. In particular, $Q = (S/a)P$ with S/a in $A[X]$, i.e., P divides Q in $A[X]$. The result is thus proven.

□

Corollary 3.21 *If A is a UFD, $A[X_1, \ldots, X_n]$ is a UFD.*[13]

It is convenient to have a practical criterion for irreducibility in UFD. The following result is often helpful in this regard.

Theorem 3.22 (Eisenstein's criterion) *Let A be a UFD, P a non-constant polynomial in $A[X]$, and p irreducible in A. Set $P = \sum_{k=0}^{n} a_k X^k$ and suppose that :*

1. *p does not divide a_n.*
2. *p divides a_k for $0 \leq k \leq n-1$.*
3. *p^2 does not divide a_0.*

Then P is irreducible in $K[X]$ (and thus also in $A[X]$ if it is primitive).

Proof: Note that $P/c(P)$ satisfies the same hypotheses as P since $c(P)$ is not divisible by p via (1). We can therefore suppose that P is primitive and $\deg P \geq 2$. If P were not irreducible, it could be written (according to theorem 3.19) $P = QR$ with Q and R non-constant in $A[X]$. Set $Q = b_r X^r + \ldots + b_0$, $R = c_s X^s + \ldots + c_0$. The ring $B = A/(p)$ is integral, and $A[X]/pA[X]$ is isomorphic to $B[X]$. In $A[X]/pA[X]$, we have $\overline{P} = \overline{QR}$, that is $\bar{a}_n X^n = \overline{Q}.\overline{R}$ in $B[X]$. We have $\bar{a}_n \neq 0$ in B, so $\bar{b}_r$ and $\bar{c}_s$ are also non-zero.

13. A similar result holds for the infinite case, and follows directly from the finite one.

Thus, $\overline{Q}$ and $\overline{R}$ are not constants and the fact that $\bar{a}_n X^n = \overline{Q}.\overline{R}$ in the PID (and thus UFD) ring $(\mathrm{Frac}\, B)[X]$ implies (since X is irreducible in this ring) that $\overline{Q}$ and $\overline{R}$ are divisible by X in $(\mathrm{Frac}\, B)[X]$. This means that p divides b_0 and c_0, which contradicts the fact that a_0 is not divisible by p^2.

□

For example, $X^{18} - 4X^7 - 2$ is irreducible in $\mathbf{Q}[X]$, and $X^5 - XY^3 - Y$ is irreducible in $\mathbf{C}[X, Y]$ (take $A = \mathbf{C}[Y]$ and $p = Y$). If p is a prime number, then $R := 1 + X + \ldots + X^{p-1} = \frac{X^p - 1}{X - 1}$ is irreducible in $\mathbf{Q}[X]$ (apply Eisenstein's criterion to the polynomial $R(X + 1)$).

We will see further on (in the chapter on field extensions) other examples of irreducible polynomials including notably the *cyclotomic polynomials* over $\mathbf{Q}$, and we will also show that if F is a finite field, there are irreducible polynomials of any degree > 0 over F.

3.5. Symmetric polynomials

Let A be a commutative ring and let $\sigma \in \mathcal{S}_n$. According to proposition 3.6, there exists a unique homomorphism of A-algebras $\varphi_\sigma : A[X_1, \ldots, X_n] \to A[X_1, \ldots, X_n]$ that maps each X_i onto $X_{\sigma(i)}$. It can immediately be seen that for σ, τ in $\mathcal{S}_n$, we have $\varphi_{\sigma\tau} = \varphi_\sigma \circ \varphi_\tau$. In other words :

Proposition 3.23 *The formula $\sigma.P := \varphi_\sigma(P)$ defines the action of the symmetric group $\mathcal{S}_n$ on $A[X_1, \ldots, X_n]$.*

This corresponds to an action by automorphisms of A-algebras, where the inverse of φ_σ is $\varphi_{\sigma^{-1}}$.

Definition 3.24 We say that a polynomial $P \in A[X_1, \ldots, X_n]$ is *symmetric* if $\sigma.P = P$ for all $\sigma \in \mathcal{S}_n$. We denote by $A[X_1, \ldots, X_n]^{\mathcal{S}_n}$ the sub-A-algebra of $A[X_1, \ldots, X_n]$ made up of symmetric polynomials.

There is an analogue for rational fractions, with the following connection when A is a field :

Proposition 3.25 *Le K be a field. Denote $K(X_1, \ldots, X_n)^{\mathcal{S}_n}$ the subfield of $K(X_1, \ldots, X_n) = \mathrm{Frac}\,(K[X_1, \ldots, X_n])$ made up of the symmetric rational fractions (i.e the fixed points for the action of $\mathcal{S}_n$ on $K(X_1, \ldots, X_n)$). Then*

$$K(X_1, \ldots, X_n)^{\mathcal{S}_n} = \mathrm{Frac}\,(K(X_1, \ldots, X_n)^{\mathcal{S}_n}).$$

Proof: It is clear that the quotient of symmetric polynomials is a symmetric rational fraction. In the other direction, let $R = P/Q$ be a symmetric rational fraction where P and Q are in $K[X_1, \ldots, X_n]$ and Q is non-zero. We then note that R can be written

$$R = \frac{\prod_{\sigma \in \mathcal{S}_n} \sigma.P}{(\prod_{\sigma \in (\mathcal{S}_n \setminus \mathrm{Id})} P)Q}$$

as a quotient of two symmetric polynomials. This is easy to see for the numerator, and for the denominator this results from the fact that if $\tau \in \mathcal{S}_n$, then $\tau.R = R$ gives $\tau.Q = (\tau.P)Q/P$, while the action of τ on

$$\prod_{\sigma \in (\mathcal{S}_n \setminus \mathrm{Id})} P$$

corresponds to multiplying by $P/\tau.P$.

□

Example 3.26 a) Suppose $k \in \{1, \ldots, n\}$. We define the k-th *elementary symmetric polynomial in n variables* by

$$\sigma_k := \sum_{I \subset \{1,\ldots,n\}, \#I = k} \prod_{i \in I} X_i.$$

In particular, we have $\sigma_1 = X_1 + \ldots + X_n$ and $\sigma_n = X_1 ... X_n$. Notice that in the ring $A[X_1, \ldots, X_n][X]$, we have also :

$$\prod_{i=1}^{n} (X - X_i) = \sum_{k=0}^{n} (-1)^k \sigma_k X^{n-k},$$

with the convention $\sigma_0 = 1$. The polynomial σ_k is homogeneous of degree k.

b) For any integer $k \geq 1$, the *Newton sums* (in n variables) :

$$s_k = \sum_{i=1}^{n} X_i^k$$

are homogeneous symmetric polynomials of degree k.

Before getting to the main theorem, we first require a few words on combinatorics :

Definition 3.27 Let us define a relation $<$ on $\mathbf{N}^n$ by $\alpha = (\alpha_1, \ldots, \alpha_n) < \beta = (\beta_1, \ldots, \beta_n)$ if and only if $|\alpha| < |\beta|$, or instead $|\alpha| = |\beta|$ and there exists some $r \in \{1, \ldots, n\}$ such that $\alpha_r < \beta_r$ and $\alpha_i = \beta_i$ for $1 \leq i < r$. It can then be immediately seen that the relation $\alpha \leq \beta$ if and only if $\alpha = \beta$ or $\alpha < \beta$ is a total order on $\mathbf{N}^n$, and that any finite non-empty family of elements of $\mathbf{N}^n$ has a largest element.

The main result for symmetric polynomials is the following theorem.

Theorem 3.28 *Let $\Phi : A[X_1, \ldots, X_n] \to A[X_1, \ldots, X_n]$ be the homomorphism of A-algebras that maps each X_k to the elementary symmetric polynomial σ_k. Then Φ induces an isomorphism from $A[X_1, \ldots, X_n]$ onto $A[X_1, \ldots, X_n]^{\mathcal{S}_n}$.*

In other words : for any symmetric polynomial R in n variables, there exists a unique polynomial P in n variables such that $R = P(\sigma_1, \ldots, \sigma_n)$, where the σ_i are the elementary symmetric polynomials. Note that therefore the A-algebras $A[X_1, \ldots, X_n]$ and $A[X_1, \ldots, X_n]^{\mathcal{S}_n}$ are isomorphic, even though the latter is strictly contained in the former !

Proof: a) The map Φ is onto : Let $F \in A[X_1, \ldots, X_n]$ be symmetric, and we want to show that it is in the image of Φ. We can suppose that F is non-zero, and therefore write $F = \sum_{d=0}^{r} F_d$ with $r \in \mathbf{N}$ and each F_d homogeneous of degree d. For any $\tau \in \mathcal{S}_n$, we have thus :

$$\tau.F = \sum_{d=0}^{r} \tau.F_d = F = \sum_{d=0}^{r} F_d,$$

with $\tau.F_d$ and F_d homogeneous of degree d, which implies that $\tau.F_d = F_d$ for all d ; in other words, each F_d is symmetric. We have therefore arrived at a setting in which the symmetric polynomial F is homogeneous of degree $d \geq 0$. We now proceed by induction on $n + d$.

If $n = 1$, there is nothing to prove, and if $d = 1$, the polynomial F is a multiple of σ_1. Suppose therefore that d and n are equal to at least 2. Set $F_1(X_1, \ldots, X_{n-1}) = F(X_1, \ldots, X_{n-1}, 0)$; this is a symmetric polynomial in $n - 1$ variables (the permutations of $\{1, \ldots, n-1\}$ matched to those of $\{1, \ldots, n\}$ leaving n unchanged). First, suppose that $F_1 = 0$, which means that F can be written $F = X_n G$ with $G \in A[X_1, \ldots, X_n]$ (use the formulation [14] (1)). Since F is symmetric, it also satisfies

$$F(X_1, \ldots, X_{i-1}, 0, X_{i+1}, \ldots, X_n) = 0$$

14. Warning : we do not suppose A is an integral domain, so reasoning using divisibility is not really meaningful.

for all i, and in particular, $G(X_1, \ldots, 0, X_n) = 0$ since X_n is not a divisor of zero in $A[X_1, \ldots, X_n]$ via proposition 3.2 (a). We therefore write $G = X_{n-1}H$, etc., from which comes $F = \sigma_n F_2$, with F_2 homogeneous of degree $d - n$. Furthermore, F_2 is symmetric since for any permutation $\tau \in \mathcal{S}_n$, we have $\tau.F = F = \sigma_n F_2 = \sigma_n(\tau.F_2)$, from which $\tau.F_2 = F_2$ given that σ_n is not a divisor of 0 in $A[X_1, \ldots, X_n]$ by proposition 3.2 (a). We can therefore apply the induction hypothesis to F_2, and the result follows.

Suppose now that $F_1 \neq 0$ and apply the induction hypothesis, which means we can write

$$F_1 = Q(\sigma'_1, \ldots, \sigma'_{n-1}),$$

where $Q \in A[X_1, \ldots, X_{n-1}]$ and $\sigma'_k = \sigma_k(X_1, \ldots, X_{n-1}, 0)$ is the k-th elementary symmetric polynomial in $n-1$ variables. Therefore set :

$$G = F(X_1, \ldots, X_n) - Q(\sigma_1, \ldots, \sigma_{n-1}).$$

Hence, G is symmetric in n variables and satisfies $G(X_1, \ldots, X_{n-1}, 0) = 0$, so after what we have already seen, G is in the image of Φ. Since $Q(\sigma_1, \ldots, \sigma_{n-1})$ is obviously also in this image, it follows that $F \in \operatorname{Im}\Phi$.

b) Φ one-to-one : For a monomial $P = aX_1^{i_1}...X_n^{i_n}$ with $a \neq 0$, we see that the largest exponent (in terms of definition 3.27) appearing in $P(\sigma_1, \ldots, \sigma_n)$ (homogeneous of degree $i_1 + 2i_2 + \ldots + ni_n$) is

$$(i_1 + \ldots + i_n, i_2 + \ldots + i_n, i_n).$$

Set $\varphi(i_1, \ldots, i_n) = (i_1 + \ldots + i_n, i_2 + \ldots + i_n, \ldots, i_n)$; then φ is a bijection from $\mathbf{N}^n$ onto the set of decreasing elements $(\alpha_1, \ldots, \alpha_n)$ (i.e., those for which $\alpha_1 \geq \alpha_2 \ldots \geq \alpha_n$) of $\mathbf{N}^n$. It results that if $Q \in A[X_1, \ldots, X_n]$ is non-zero, then when given in the form (1) it has one and only one monomial $aX_1^{i_1}...X_n^{i_n}$ with $a \neq 0$ and $\varphi(i_1, \ldots, i_n)$ maximal. Thus, $Q(\sigma_1, \ldots, \sigma_n)$ is written with one and only one monomial $a\sigma_1^{i_1}...\sigma_n^{i_n}$ with a maximal exponent equal to $\varphi(i_1, \ldots, i_n)$, since all of the others are strictly smaller. In particular, $Q(\sigma_1, \ldots, \sigma_n)$ is non-zero.

□

We now round up this chapter with a theorem that connects elementary symmetric polynomials and Newton sums in the ring $A[X_1, \ldots, X_n]$.

Theorem 3.29 (Newton's identities) *a) Let $k \geq n$. Then*

$$s_k - \sigma_1 s_{k-1} + \ldots + (-1)^n \sigma_n s_{k-n} = 0.$$

b) Let $1 \leq k \leq n$. Then

$$s_k - \sigma_1 s_{k-1} + \ldots + (-1)^{k-1} \sigma_{k-1} s_1 + (-1)^k k\sigma_k = 0.$$

Proof: a) Let :

$$Q = \prod_{i=1}^{n}(X - X_i) = X^n - \sigma_1 X^{n-1} + \ldots + (-1)^n \sigma_n.$$

Evaluating this at $X = X_i$, we obtain :

$$X_i^n - \sigma_1 X_i^{n-1} + \ldots + (-1)^n \sigma_n = 0.$$

For $k \geq n$, if we multiply by X_i^{k-n}, we get that :

$$X_i^k - \sigma_1 X_i^{k-1} + \ldots + (-1)^n \sigma_n X_i^{k-n},$$

and the required formula is obtained by summing from $i = 1$ to $i = n$.

b) For $k = n$, the formula is proven in (a) (note that in this case, $s_0 = k$), so suppose that $k > n$. Set :

$$S = s_k - \sigma_1 s_{k-1} + \ldots + (-1)^k k \sigma_k.$$

The polynomial S is homogeneous of degree k. We see that

$$S(X_1, \ldots, X_k, 0, \ldots, 0) = 0,$$

since this equality exactly corresponds to the $k = n$ case in the formula ; in effect, for $r = 1, \ldots, k$, the polynomial $\sigma_r(X_1, \ldots, X_k, 0, \ldots, 0)$ is the r-th symmetric polynomial in k variables and $s_r(X_1, \ldots, X_k, 0, \ldots, 0)$ is the r-th Newton sum in k variables. Let us now write S in the form (1) :

$$S = \sum_{(\alpha_1, \ldots, \alpha_n) \in \mathbf{N}^n} a_{\alpha_1, \ldots, \alpha_n} X_1^{\alpha_1} \ldots X_n^{\alpha_n}.$$

The equality $S(X_1, \ldots, X_k, 0, \ldots, 0) = 0$ therefore means that all coefficients of the type $a_{\alpha_1, \ldots, \alpha_k, 0, \ldots, 0}$ are equal to zero. Also, all of the exponents $\alpha = (\alpha_1, \ldots, \alpha_n)$ which appear in S satisfy $|\alpha| = k$, and in particular have at most k non-zero (integer) values in the α_i. Since S is also symmetric, we thus obtain that all of the $a_{\alpha_1, \ldots, \alpha_n}$ are zero, and therefore $S = 0$.

□

Remark 3.30 When A is a field of characteristic zero (or more generally a ring containing a field of characteristic zero as a subring), Newton's identities allow us to calculate the σ_k as a function of the s_k by solving an upper-triangular system of linear equations. In this case, it turns out that any symmetric polynomial in $A[X_1, \ldots, X_n]$ can be written as a unique polynomial in the s_k.

Références

[1] D. Perrin : *Cours d'algèbre*, Ellipses 1996.