Commutative Algebra

Undergraduate course

Charles De Clercq, Matteo Tamiozzo

These English notes were produced from the original French version using artificial intelligence.
Inaccuracies may have arisen during the process; refer to the original version if necessary.

Contents

1 Ideals and spectrum of a ring

1.1 Introduction

We assume familiarity with the notion of a ring and ring homomorphisms. Unless otherwise stated, all rings in this text are commutative and unital, and every ring homomorphism $f : A \to B$ sends the (multiplicative) identity of A to that of B.

Commutative algebra, i.e., the study of properties of rings, was developed starting from the 19th century. A fundamental motivation was the concrete example of rings $\mathbb{Z}[e^{2\pi i/p}] \subset \mathbb{C}$, used by Kummer to try to prove Fermat's Last Theorem. The properties of these rings were studied in more detail by Dedekind, who understood that the same ideas could be useful to develop the theory of Riemann surfaces in a purely algebraic way. Later, in the 20th century, commutative algebra became the basic tool for the study of algebraic varieties, playing a role analogous to that of analysis (in several variables) in the study of differentiable manifolds. In this course, we will explain the basics of commutative algebra while trying to highlight its relation with geometry. The guiding idea is the following.

Think of rings not as "abstract" objects, but rather as rings of functions on geometric spaces.

For example (for $k = \mathbb{R}$ or $\mathbb{C}$).

$k[X]$	(polynomial) functions $k \to k$
$k[X_1, \ldots, X_n]$	functions $k^n \to k$
$\{\frac{P(X)}{X^d}, P(X) \in k[X], d \geq 0\}$	functions $k \smallsetminus \{0\} \to k$
?	functions $S^1 = \{(x, y) \in \mathbb{R}^2 \mid x^2 + y^2 = 1\} \to \mathbb{R}$
$\mathbb{Z}$	?

We will be interested in the interaction between algebraic properties of rings and geometric properties of the corresponding spaces. Here are two examples.

- The spaces $\mathbb{C}$ and $\mathbb{C}^\times$ are not "the same" (they are not homeomorphic). On the algebraic side, show that there is no ring isomorphism between the rings in the first and third lines above that is the identity on $k = \mathbb{C}$. On the

other hand, what is the relation between the ring of polynomial functions on $\mathbb{C} \smallsetminus \{0\}$ and that of polynomial functions on the complex circle $\{(x, y) \in \mathbb{C}^2 \mid x^2 + y^2 = 1\} \subset \mathbb{C}^2$?

- What is the "algebraic incarnation" of the Möbius strip?

1.2 Rings and ideals

Let $(A, +, \cdot, 0, 1)$ be a ring. We recall the following terminology.

- An element $a \in A \smallsetminus \{0\}$ is a zero divisor if there exists $b \in A \smallsetminus \{0\}$ such that $ab = 0$.
- An element $a \in A$ is nilpotent if there exists an integer $n \geq 0$ such that $a^n = 0$. We say that A is a reduced ring if the only nilpotent element of A is 0.
- A is an integral domain if $1 \neq 0$ and A has no zero divisors, i.e.,

$$\forall a, b \in A \smallsetminus \{0\}, ab \neq 0.$$

- An element $a \in A$ is a unit if there exists $b \in A$ such that $ab = 1$. The set of units of A endowed with multiplication $\cdot$ is an abelian group, denoted $A^\times$.
- A is a field if $1 \neq 0$ and $A \smallsetminus \{0\} = A^\times$, i.e.,

$$\forall a \in A \smallsetminus \{0\}, \exists b \in A : ab = 1.$$

Example 1.1. *(Some proofs in TD)*

(i) The ring $\mathbb{Z}$ is an integral domain, and $\mathbb{Z}^\times = \{\pm 1\}$. The ring

$$\mathbb{Q} = \left\{ \frac{a}{b}, a \in \mathbb{Z}, b \in \mathbb{Z} \smallsetminus \{0\} \right\}$$

is a field; note that any field containing $\mathbb{Z}$ necessarily contains $\mathbb{Q}$.

(ii) If k is a field, then the ring $A = k[X]$ of polynomials in X with coefficients in k is an integral domain, and $A^\times = k^\times$.

(iii) More generally, for any integral domain A, the ring $A[X]$ is an integral domain. In particular, $k[X_1, \ldots, X_n]$ is an integral domain for any field k and any integer $n \geq 1$.

(iv) Let k be a field, and $A = \{a + b\varepsilon, a, b \in k, \varepsilon^2 = 0\}$. The element $\varepsilon \in A$ is nilpotent; moreover, $A^\times = \{a + b\varepsilon, a, b \in k, a \neq 0\}$.

Fraction field. To every integral domain A we can associate a field $K(A)$, called the fraction field of A; it is the smallest field containing A. Its construction generalizes the construction of $\mathbb{Q}$ from $\mathbb{Z}$. Precisely, we define

$$K(A) = \{(a, b), a \in A, b \in A \smallsetminus \{0\}\}/\sim$$

where $(a, b) \sim (a', b')$ if $ab' = a'b$. We define the sum by $(a, b) + (a', b') = (ab' + a'b, bb')$ and the product by $(a, b) \cdot (a', b') = (aa', bb')$. One checks that these formulas endow $K(A)$ with a field structure, and that the map $A \to K(A)$ sending a to $(a, 1)$ is an injective ring homomorphism.

For example, for $A = \mathbb{Z}$ we obtain $K(A) = \mathbb{Q}$, and for $A = k[X]$, where k is a field, we obtain $K(A) = k(X) = \{P(X)/Q(X), P(X), Q(X) \in k[X], Q(X) \neq 0\}$. We will see later a generalization of this construction, the localization of a ring.

Ideals. Consider the parabola $C \subset \mathbb{R}^2$ with equation $x = y^2$. We aim to describe the ring A_C of polynomial functions $C \to \mathbb{R}$. Such a function f sends $(x, y) \in C$ to $P(x, y)$, for some $P(X, Y) \in \mathbb{R}[X, Y]$. On the other hand, for any $Q(X, Y) \in \mathbb{R}[X, Y]$, the polynomial $P(X, Y)+Q(X, Y)\cdot(X-Y^2)$ also gives rise to the function f. In the ring A_C, we must therefore identify $P(X, Y) + Q(X, Y) \cdot (X - Y^2)$ with $P(X, Y)$. To do this, we introduce the notion of an ideal and quotient ring.

Definition 1.2. *Let A be a ring. An ideal $I \subset A$ is a subgroup of $(A, +)$ such that for all $a \in A$, if $i \in I$ then $ai \in I$.*

Operations with ideals. Let A be a ring.

Principal and finitely generated ideals: If $a \in A$, the set $(a) = \{ab, b \in A\}$ of multiples of a is an ideal, called the principal ideal generated by a. An integral domain A in which every ideal is principal is called a principal ideal domain.

Sum: if $I_1, \ldots, I_k \subset A$ are ideals, then $I_1 + \cdots + I_k = \{i_1 + \cdots + i_k, i_j \in I_j \text{ for } 1 \leq j \leq k\} \subset A$ is an ideal. If $a_1, \ldots, a_k \in A$, we denote $(a_1, \ldots, a_k) = (a_1) + \cdots + (a_k)$.

Product: if $I_1, \ldots, I_k \subset A$ are ideals, the additive subgroup of A generated by the elements $i_1 i_2 \cdots i_k$, with $i_j \in I_j$ for $1 \leq j \leq k$, is an ideal denoted $I_1 I_2 \cdots I_k$.

Lemma 1.3.

1. *Let $f : A \to B$ be a ring homomorphism. The kernel* $\ker(f) = \{a \in A \mid f(a) = 0\}$ *is an ideal of A.*

2. *Let A be a ring and $I \subset A$ an ideal. There exists a unique ring structure on the additive quotient group A/I such that the projection $q : A \to A/I$ is a ring homomorphism. Moreover, for any ring B,*

$$\begin{array}{ccc} \{\bar{f} : A/I \to B\} & \longrightarrow & \{f : A \to B \text{ such that } I \subset \ker(f)\} \\ \bar{f} & \longmapsto & \bar{f} \circ q \end{array}$$

is a bijection.

3. *Let A be a ring, $I \subset A$ an ideal and $q : A \to A/I$ the projection. For any ideal $\bar{J} \subset A/I$, the inverse image $q^{-1}(\bar{J}) \subset A$ is an ideal, and*

$$\begin{array}{c} \{\text{ideals of } A/I\} \to \{\text{ideals } I \subset J \subset A\} \\ \bar{J} \mapsto q^{-1}(\bar{J}) \end{array}$$

is a bijection.

Proof. 1. If $a, b \in \ker(f)$, then $f(a+b) = f(a) + f(b) = 0$ so $a + b \in \ker(f)$. If $b \in \ker(f)$ and $a \in A$ then $f(ab) = f(a)f(b) = 0$ so $ab \in \ker(f)$.

2. For q to be a ring homomorphism, the laws $\bar{+}, \bar{\cdot}$ on A/I must be defined by $q(a)\bar{+}q(b) = q(a+b)$ and $q(a)\bar{\cdot}q(b) = q(ab)$. We verify that these laws are well-defined, and that $(A/I, \bar{+}, \bar{\cdot}, q(0), q(1))$ is a ring. For example, let's verify that $\bar{\cdot}$ is well-defined (the other checks are left to the reader). Let $a, b \in A$ and $i_1, i_2 \in I$. Then

$$q(a+i_1)\bar{\cdot}q(b+i_2) = q((a+i_1)\cdot(b+i_2)) = q(ab + ai_2 + bi_1 + i_1 i_2) = q(ab)$$

where the last equality follows from the fact that $ai_2 + bi_1 + i_1 i_2 \in I$.

Finally, the map $\bar{f} \mapsto \bar{f} \circ q$ is injective because q is surjective. If $f : A \to B$ is a homomorphism such that $I \subset \ker(f)$, we verify that the map $\bar{f} : A/I \to B$ sending $q(a)$ to $f(a)$ is well-defined, and is a ring homomorphism such that $f = \bar{f} \circ q$.

3. The ideals of A/I are the kernels $\ker \bar{f}$ of homomorphisms $\bar{f} : A/I \to B$; by the previous point, they correspond to the kernels $q^{-1}(\ker(\bar{f}))$ of the homomorphisms $f = \bar{f} \circ q : A \to B$, i.e., to the ideals $I \subset J \subset A$.

□

Example 1.4. *(Some proofs in TD)*

- *$\mathbb{Z}$ is a principal ideal domain; if k is a field, then $k[X]$ is a principal ideal domain. In both cases, the proof relies on the Euclidean algorithm.*

- *The ring $\mathbb{C}[X,Y]$ is not principal: for example, the ideal (X,Y) is not principal.*

- *Let k be a field, $A = k[X]$ and $I = (X^2)$. The quotient A/I is (isomorphic to) the ring in Example 1.1(iv).*

- *For $A = \mathbb{R}[X,Y]$ and $I_1 = (X - Y^2)$, the quotient A/I can be interpreted as the ring of (polynomial) functions $C_1 \to \mathbb{R}$, where C_1 is the parabola with equation $x = y^2$. On the other hand, let $I_2 = (XY)$; the quotient A/I_2 is the ring of real-valued functions on the curve*

$$C_2 = \{(x,y) \in \mathbb{R}^2 \mid xy = 0\}.$$

The ring A/I_1 is an integral domain, but A/I_2 is not, because $x \in A/I_1$ is a zero divisor. Geometrically, this corresponds to the fact that C_2 is the union of two lines, but C_1 cannot "break into two pieces".

Lemma 1.5. *(Chinese Remainder Theorem) Let A be a ring and let $I_1, \dots, I_k \subset A$ be ideals such that, for all $i \neq j$, we have $I_i + I_j = A$. Then $I_1 \cdots I_k = I_1 \cap \cdots \cap I_k$ and the natural map $A \to A/I_1 \times \cdots \times A/I_k$ induces an isomorphism $A/I_1 \cdots I_k \simeq A/I_1 \times \cdots \times A/I_k$.*

Proof. First show that $I_1 \cdots I_k = I_1 \cap \cdots \cap I_k$ by induction on $k \geq 1$. For $k = 1$ there is nothing to prove; assume $k \geq 2$. We have $1 \in I_1 + I_j$ for $2 \leq j \leq k$, so $1 \in (I_1 + I_2) \cdots (I_1 + I_k) = I_1 + I_2 \cdots I_k$. Let $i_1 \in I_1$ and $i' \in J = I_2 \cdots I_k$ such that $i_1 + i' = 1$. If $i \in I_1 \cap J$ then $i = i \cdot (i_1 + i') \in J \cdot I_1 + I_1 \cdot J = I_1 I_2 \cdots I_k$. So $I_1 \cap J = I_1 J$. Since $J = I_2 \cap \cdots \cap I_k$ by induction, we obtain $I_1 \cap I_2 \cap \cdots \cap I_k = I_1 I_2 \cdots I_k$.

Now, the kernel of $q : A \to A/I_1 \times \cdots \times A/I_k$ is $I_1 \cap \cdots \cap I_k$, so it remains to show that q is surjective. We have $q(i') = (1, 0, 0, \dots, 0)$; more generally, for $2 \leq i \leq k$ the above argument with I_i in place of I_1 shows that $(0, \dots, 0, 1, 0, \dots, 0)$ (1 is in the i-th position) is in the image of q, so q is surjective. □

Example 1.6.

- *Let $n \in \mathbb{Z}_{>0}$; write $n = \prod_{i=1}^r p_i^{e_i}$ where the p_i are distinct prime numbers. If $i \neq j$ then $(p_i^{e_i}) + (p_j^{e_j}) = \mathbb{Z}$, so*

$$\mathbb{Z}/n\mathbb{Z} \simeq \prod_{i=1}^{r} \mathbb{Z}/(p_i^{e_i}).$$

- *Let $A = \mathbb{R}[X,Y]$ and $I = (X^2 - X)$. Then $I = I_1 I_2$ with $I_1 = (X)$ and $I_2 = (1 - X)$. Since $I_1 + I_2 = A$, we obtain $A/I \simeq \mathbb{R}[X,Y]/(X) \times \mathbb{R}[X,Y]/(X - 1) \simeq \mathbb{R}[Y] \times \mathbb{R}[Y]$. Geometrically, this decomposition of A/I corresponds to the fact that the set $\{(x,y) \in \mathbb{R}^2 : x^2 = x\}$ is the union of the two lines $x = 0$ and $x = 1$.*

Lemma 1.7. *Let A be a ring. The set $\sqrt{A}$ of nilpotent elements of A is an ideal; the quotient ring $A/\sqrt{A}$ is reduced.*

Proof. If $a \in \sqrt{A}$ then, for all $b \in A$, we have $ab \in \sqrt{A}$, because $a^n = 0$ implies $(ab)^n = 0$. Now verify that the sum of two nilpotent elements is nilpotent. Let $a, b \in A$ and n, m positive integers such that $a^n = b^m = 0$. We have

$$(a+b)^{n+m} = \sum_{k=0}^{n+m} \binom{n+m}{k} a^k b^{n+m-k};$$

if $k \geq n$ then $a^k = 0$; on the other hand, if $k < n$ then $n + m - k > m$ so $b^{n+m-k} = 0$. So every term in the sum is zero, and $(a+b)^{n+m} = 0$. We have verified that $\sqrt{A}$ is an ideal of A.

Now show that $A/\sqrt{A}$ is reduced. Let $q : A \to A/\sqrt{A}$ be the projection. Let $a \in A$ such that $q(a)$ is nilpotent: then $q(a)^n = 0 \in A/\sqrt{A}$ for some positive integer n, i.e., $a^n \in \sqrt{A}$. So a^n is nilpotent, which implies that a is also nilpotent, so $q(a) = 0$. □

Example 1.8.

- *If k is a field and $A = k[X]/(X^n)$ with $n \geq 1$ then $\sqrt{A} = (X)$, and $A/\sqrt{A} \simeq k$.*
- *Let $n = \prod_{i=1}^r p_i^{e_i}$ as in Example 1.6, and $A = \mathbb{Z}/n\mathbb{Z}$. Then $\sqrt{A} = (p_1 p_2 \cdots p_r)$, and $A/\sqrt{A} \simeq \mathbb{Z}/p_1\mathbb{Z} \times \cdots \times \mathbb{Z}/p_r\mathbb{Z}$.*

1.3 Prime and maximal ideals

Remark 1.9. *A ring A with $0 \neq 1$ is a field if and only if the ideals of A are $\{0\}$ and A. Indeed, if A is a field then $A \setminus \{0\} = A^\times$, so every ideal $I \neq \{0\}$ contains a unit, hence is equal to A. Conversely, let $a \in A \setminus \{0\}$. Then $(a) \supsetneq \{0\}$, so $(a) = A$, i.e., there exists $b \in A$ such that $ab = 1$.*

Definition 1.10. *Let A be a ring.*

- *An ideal $I \subset A$ is prime if $I \neq A$ and for all $a, b \in A$, if $ab \in I$ then $a \in I$ or $b \in I$.*
- *An ideal $I \subset A$ is maximal if $I \neq A$ and for every ideal $I \subset J \subset A$ we have $J = I$ or $J = A$.*

We denote by $\mathrm{Spec}(A)$ *the spectrum of A, i.e., the set of prime ideals of A, and by* $\mathrm{MaxSpec}(A)$ *the set of maximal ideals of A.*

Lemma 1.11. *Let A be a ring and $I \subset A$ an ideal.*

1. *I is prime if and only if A/I is an integral domain.*

2. *I is maximal if and only if A/I is a field.*

In particular, every maximal ideal is prime.

Proof. 1. Let $q : A \to A/I$ be the projection. The ring A/I is an integral domain if $A/I \neq \{0\}$ (i.e., $I \neq A$) and, for all $a, b \in A$, if $q(a)q(b) = 0$ then $q(a) = 0$ or $q(b) = 0$. In other words, if $ab \in I$ then $a \in I$ or $b \in I$, i.e., I is prime.

2. By Lemma 1.3(3) we have that I is maximal if and only if $I \neq A$ and the ideals of A/I are $\{0\}$ and A/I, which is equivalent to A/I being a field (Remark 1.9).

□

Example 1.12.

- *For an integer $n \geq 0$, the ideal $(n) \subset \mathbb{Z}$ is prime if and only if for all $a, b \in \mathbb{Z}$, if $n \mid ab$ then $n \mid a$ or $n \mid b$. This is the case if and only if $n = 0$ or n is prime. For every prime number p the ring $\mathbb{Z}/p\mathbb{Z}$ is a field, so*

$$\mathrm{Spec}(\mathbb{Z}) = \{(0)\} \coprod \{(p), p \text{ prime}\} \supset \mathrm{MaxSpec}(\mathbb{Z}) = \{(p), p \text{ prime}\}.$$

- *Let k be a field and $A = k[X]$. The prime ideals of A are of the form $P(X)$ with $P(X) = 0$ or $P(X) \in k[X] \smallsetminus k^\times$ irreducible. For example, $\mathrm{Spec}(\mathbb{C}[X]) = \{(0)\} \coprod \{(X - a), a \in \mathbb{C}\}$. So we see that*

$$\begin{aligned} \mathbb{C} &\to \mathrm{MaxSpec}(\mathbb{C}[X]) \\ a &\mapsto (X - a) \end{aligned}$$

is a bijection. For any $P \in \mathbb{C}[X]$, we have $P - P(a) \in (X - a)$, so the image of P in $\mathbb{C}[X]/(X - a)$ is $P(a)$.

Lemma 1.13.

1. *Let $f : A \to B$ be a ring homomorphism. For every $\mathfrak{p} \in \mathrm{Spec}(B)$ we have $f^{-1}(\mathfrak{p}) \in \mathrm{Spec}(A)$. So f induces a map*

$$\begin{aligned} f^\sharp : \mathrm{Spec}(B) &\to \mathrm{Spec}(A) \\ \mathfrak{p} &\mapsto f^{-1}(\mathfrak{p}). \end{aligned}$$

2. *Let A be a ring, $I \subset A$ an ideal and $q : A \to A/I$ the projection. The map $q^\sharp$ induces a bijection*

$$\mathrm{Spec}(A/I) \to \{\mathfrak{p} \in \mathrm{Spec}(A) : \mathfrak{p} \supset I\}.$$

3. *Let A be a ring. The map $\mathrm{Spec}(A/\sqrt{A}) \to \mathrm{Spec}(A)$ induced by the homomorphism $A \to A/\sqrt{A}$ is a bijection.*

Proof. 1. For $\mathfrak{p} \in \mathrm{Spec}(B)$, the inverse image $\mathfrak{q} = f^{-1}(\mathfrak{p})$ is the kernel of the composition $A \to B \to B/\mathfrak{p}$. In particular, $\mathfrak{q}$ is an ideal different from A. Moreover, $A/\mathfrak{q}$ injects into the integral domain $B/\mathfrak{p}$, so $A/\mathfrak{q}$ is an integral domain and $\mathfrak{q} \in \mathrm{Spec}(B)$ by Lemma 1.11.

2. Follows from Lemma 1.3(3) and the fact that, in the bijection of the lemma, $\bar{J}$ is prime if and only if $q^{-1}(\bar{J})$ is.

3. Follows from (2) and the fact that every $\mathfrak{p} \in \mathrm{Spec}(A)$ contains $\sqrt{A}$. Indeed, if $a \in A$ is nilpotent there exists $n \geq 0$ such that $a^n = 0 \in \mathfrak{p}$, so $a \in \mathfrak{p}$ since $\mathfrak{p}$ is prime.

□

Remark 1.14. *Caution: if $f : A \to B$ is a ring homomorphism and $\mathfrak{m} \in \mathrm{MaxSpec}(B)$, it is not true in general that $f^{-1}(\mathfrak{m}) \in \mathrm{MaxSpec}(A)$. A counterexample is given by the inclusion of $\mathbb{Z}$ into $\mathbb{Q}$, with $\mathfrak{m} = (0)$.*

Example 1.15. *(Important) We will show in TD that*

$$\mathrm{Spec}(\mathbb{C}[X,Y]) = \{(0)\} \coprod \{(P), P \in \mathbb{C}[X,Y] \text{ monic irreducible}\} \coprod \{(X-a, Y-b), (a,b) \in \mathbb{C}^2\},$$

and $\mathrm{SpecMax}(\mathbb{C}[X,Y]) \simeq \mathbb{C}^2$ via the map sending $(a,b) \in \mathbb{C}^2$ to $(X-a, Y-b)$.

Let $A = \mathbb{C}[X,Y]/(X - Y^2)$. This is the ring of polynomial functions with complex values on the parabola $C = \{(a,b) \in \mathbb{C}^2 \mid a = b^2\}$. The ring A is an integral domain, so (0) is a prime ideal. The other prime ideals of A, by Lemma 1.13, correspond to the ideals $(X-a, Y-b) \supset (X - Y^2)$. So we have $\mathrm{Spec}(A) = \{(0)\} \coprod \{(X-a, Y-b), a = b^2\}$, and the map sending (a,b) to $(X-a, Y-b) \subset A$ induces a bijection between C and $\mathrm{MaxSpec}(A)$.

Let $B = \mathbb{C}[X]$; the homomorphism $p : B \to A$ sending X to X induces $p^\sharp : \mathrm{Spec}(A) \to \mathrm{Spec}(B)$. We have $p^\sharp((0)) = (0)$ and, for every $(a,b) \in C$, $p^\sharp(X - a, Y - b) = (X - a)$. So $p^\sharp$ corresponds geometrically to the projection $\pi : C \to \mathbb{C}$ sending (a,b) to a.

For every point $a \in \mathbb{C} \smallsetminus \{0\}$ the fiber $\pi^{-1}(a)$ has two elements, but $\pi^{-1}(0) = 0$ (π is a degree 2 covering ramified at 0). Let us reformulate this observation in algebraic language. For every $a \in \mathbb{C}$, Lemma 1.13 gives a bijection between the spectrum of the quotient $A/(X-a)$ and the set of prime ideals $\mathfrak{p}$ of A such that $p^\sharp(\mathfrak{p}) = (X-a)$. In other words, $\mathrm{Spec}(A/(X-a))$ is in bijection with the inverse image by $p^\sharp$ of $(X-a) \in \mathrm{Spec}(B)$. Note that $A/(X-a) \simeq \mathbb{C}[Y]/(Y^2 - a)$ is isomorphic to $\mathbb{C} \times \mathbb{C}$ if $a \neq 0$, and to $\mathbb{C}[Y]/(Y^2)$ if $a = 0$. In both cases, $A/(X-a)$

is a $\mathbb{C}$-vector space of dimension 2; for $a = 0$ the spectrum of this ring has only one element, and the ring is not reduced.

Existence of prime and maximal ideals To conclude, we will treat two existence results for prime and maximal ideals. The proof relies on Zorn's lemma (hence on the axiom of choice), although we will see later that we can do without it for many rings of interest, for example quotients of polynomial rings $k[X_1, \dots, X_n]$ with coefficients in a field k.

Proposition 1.16. *For every ring $A \neq \{0\}$ we have* $\mathrm{MaxSpec}(A) \neq \emptyset$ *(so* $\mathrm{Spec}(A) \neq \emptyset$*).*

Proof. The naive idea is to choose an ideal $I_0 \subsetneq A$ (e.g. $I_0 = 0$); then, if I_0 is not maximal, there exists an ideal $I_0 \subsetneq I_1 \subsetneq A$; if I_1 is not maximal, we continue...

To turn this idea into a proof, let $\mathcal{I}$ be the set of ideals $I \subsetneq A$; note that $\mathcal{I}$ is non-empty, since $(0) \in \mathcal{I}$. Inclusion is a partial order on $\mathcal{I}$, and if $\{I_\lambda, \lambda \in \Lambda\}$ is totally ordered, then $I = \cup_{\lambda\in\Lambda} I_\lambda$ belongs to $\mathcal{I}$. Indeed, it is clear that if $a \in A$ then $aI \subset I$. Moreover, let $i_1, i_2 \in I$; there exist $\lambda_1, \lambda_2 \in \Lambda$ such that $i_1 \in I_{\lambda_1}$ and $i_2 \in I_{\lambda_2}$. Since $\mathcal{I}$ is totally ordered, we have $I_{\lambda_1} \subset I_{\lambda_2}$ or $I_{\lambda_2} \subset I_{\lambda_1}$. Without loss of generality, assume $I_{\lambda_1} \subset I_{\lambda_2}$. Then $i_1 + i_2 \in I_{\lambda_2} \subset I$. Finally, $I \neq A$, because for every $\lambda \in \Lambda$, 1 does not belong to I_λ.

Since $I \in \mathcal{I}$ is an upper bound for $\{I_\lambda, \lambda \in \Lambda\}$, we can apply Zorn's lemma, which tells us that $\mathcal{I}$ has a maximal element, which is therefore a maximal ideal of A. □

Proposition 1.17. *Let A be a ring and $S \subset A$ a non-empty multiplicative subset, i.e., such that, if $s_1, s_2 \in S$, then $s_1 s_2 \in S$. Let $I \subset A$ be an ideal such that $I \cap S = \emptyset$. There exists $\mathfrak{p} \in \mathrm{Spec}(A)$ such that $\mathfrak{p} \supset I$ and $\mathfrak{p} \cap S = \emptyset$.*

Proof. Let $\mathcal{I}(S) = \{J \text{ ideal}, J \supset I, J \cap S = \emptyset\}$; we have $I \in \mathcal{I}(S)$, so $\mathcal{I}(S)$ is non-empty. The argument in the proof of the previous proposition shows that $I(S)$ contains an element $\mathfrak{p}$ maximal with respect to inclusion; let us show that $\mathfrak{p} \in \mathrm{Spec}(A)$. First, since $S \neq \emptyset$ and $\mathfrak{p} \cap S = \emptyset$, we have $\mathfrak{p} \neq A$. Next, let $a_1, a_2 \in A \smallsetminus \mathfrak{p}$. We have $\mathfrak{p} + (a_1) \supsetneq \mathfrak{p}$ and $\mathfrak{p} + (a_2) \supsetneq \mathfrak{p}$, so $(\mathfrak{p} + (a_i)) \cap S \neq \emptyset$ for $i = 1, 2$. Let $p_1, p_2 \in \mathfrak{p}$ and $r_1, r_2 \in A$ such that $p_1 + a_1 r_1 \in S$ and $p_2 + a_2 r_2 \in S$. Since S is multiplicative, it contains $(p_1 + a_1 r_1)(p_2 + a_2 r_2) = p_1 p_2 + p_1 a_2 r_2 + p_2 a_1 r_1 + a_1 a_2 r_1 r_2$. Since $\mathfrak{p} \cap S = \emptyset$ we have $a_1 a_2 r_1 r_2 \notin \mathfrak{p}$, so $a_1 a_2 \notin \mathfrak{p}$. □

Corollary 1.18. *For every ring A, we have $\sqrt{A} = \cap_{\mathfrak{p}\in\mathrm{Spec}(A)} \mathfrak{p}$.*

Proof. We showed that $\sqrt{A} \subset \cap_{\mathfrak{p}\in\mathrm{Spec}(A)} \mathfrak{p}$ in the proof of Lemma 1.13(3). Conversely, let $a \in A \smallsetminus \sqrt{A}$; let $I = (0)$, and $S = \{a^n, n \geq 0\}$. This is a multiplicative subset such that $I \cap S = \emptyset$. Thanks to Proposition 1.17, there exists $\mathfrak{p} \in \mathrm{Spec}(A)$ such that $\mathfrak{p} \cap S = \emptyset$. In particular, $a \notin \mathfrak{p}$. □

2 Finite and integral algebras

2.1 Modules

This is about doing linear algebra over an arbitrary ring A, not necessarily a field.

Definition 2.1. *Let A be a ring. An A-module is an abelian group $(M, +)$ endowed with a map*

$$\begin{aligned} A \times M &\to M \\ (a, m) &\mapsto am \end{aligned}$$

such that

- $\forall m \in M, 1m = m.$
- $\forall a \in A, \forall m, n \in M, a(m + n) = am + an.$
- $\forall a, b \in A, \forall m \in M, (a + b)m = am + bm.$
- $\forall a, b \in A, \forall m \in M, (ab)m = a(bm).$

A submodule of an A-module M is a subgroup $N \subset M$ such that for all $a \in A$ and all $n \in N$ we have $an \in N$.

A map $f : M \to M'$ between $A-$modules is a homomorphism of $A-$modules if it is a group homomorphism and, for all $a \in A$ and $m \in M$, we have $f(am) = af(m)$.

Example 2.2.

- *The multiplication $A \times A \to A$ endows any ring A with an A-module structure. The submodules of A are the ideals of A. More generally, if $f : A \to B$ is a ring homomorphism, then the map $A \times B \to B$ sending (a, b) to $f(a)b$ endows $(B, +)$ with an A-module structure.*
- *If A is a field, then an A-module is the same as an A-vector space.*
- *For $A = \mathbb{Z}$, an A-module is the same as an abelian group.*
- *If $M_1, \ldots, M_n$ are $A-$modules, then the map*

$$\begin{aligned} A \times (M_1 \oplus \cdots \oplus M_n) &\to M_1 \oplus \cdots \oplus M_n \\ (a, (m_1, \ldots, m_n)) &\mapsto (am_1, \ldots, am_n) \end{aligned}$$

  endows $M_1 \oplus \cdots \oplus M_n$ with an A-module structure, called the direct sum of the M_i.

Definition 2.3. *Let A be a ring.*

- *An A-module M is said to be finitely generated if there exists an integer $n \geq 0$ and a surjective homomorphism of A-modules $A^n \to M$. Concretely, this means there exist $m_1, \ldots, m_n \in M$ that generate M, i.e., such that every $m \in M$ can be written as $m = \sum_{i=1}^n a_i m_i$ with $a_1, \ldots, a_n \in A$ (not necessarily uniquely).*
- *An A-module M is said to be free of rank $n \geq 0$ if it is isomorphic to $A^n = A \oplus A \oplus \cdots \oplus A$ (n times).*

Remark 2.4. *1. Caution: if A is a field, then every finitely generated A-module is free (every finite-dimensional vector space has a basis). This is not true if A is not a field. For example, $\mathbb{Z}/2\mathbb{Z}$ is a finitely generated $\mathbb{Z}$-module, but it is not free.*

2. If M is free of rank $n \geq 0$, then n is unique. In other words, if $n' \neq n$ then A^n is not isomorphic to $A^{n'}$. Indeed, suppose by contradiction that $A^n \simeq A^{n'}$. By Proposition 1.16 there exists $\mathfrak{m} \in \mathrm{MaxSpec}(A)$; let $k = A/\mathfrak{m}$. We obtain $A^n/\mathfrak{m}A^n \simeq A^{n'}/\mathfrak{m}A^{n'}$, i.e., $k^n \simeq k^{n'}$, contradiction.

Cofactor matrix. Recall that if A is a square matrix of size n with coefficients in a field k, the cofactor matrix of A, denoted $\mathrm{com}\mathsf{A}$, is the square matrix of size n whose (i,j) entry is $(-1)^{i+j}\det(\mathsf{A}_{i,j})$, where $\mathsf{A}_{i,j}$ is the matrix obtained by deleting the i-th row and j-th column of A. The matrix $\mathrm{com}\mathsf{A}$ satisfies

$$\mathsf{A}\ {}^t\mathrm{com}\mathsf{A} = {}^t\mathrm{com}\mathsf{A}\ \mathsf{A} = \det(\mathsf{A})\mathsf{I}_n.$$

The definition of $\mathrm{com}\mathsf{A}$ makes sense for matrices with coefficients in an arbitrary ring, and the above equality remains true in this generality.

Lemma 2.5. *(crucial!) Let A be a ring and M a finitely generated A-module, generated by $m_1, \ldots, m_n$. Let $\mathsf{m} = (m_1, \ldots, m_n) \in M^n$. Let $\mathsf{A} = (a_{ij})_{1 \leq i,j \leq n} \in M_{n\times n}(A)$ be a square matrix. If $\mathsf{A}\mathsf{m} = 0$ then, for every $m \in M$, we have $\det(\mathsf{A})m = 0$.*

Proof. Since $\mathsf{A}\mathsf{m} = 0$ we have ${}^t\mathrm{com}\mathsf{A}\ \mathsf{A}\ \mathsf{m} = 0$, so $\det(\mathsf{A})\mathsf{m} = 0$, i.e., $\det(\mathsf{A})m_i = 0$ for $1 \leq i \leq n$. Since $m_1, \ldots, m_n$ generate M, we deduce that $\det(\mathsf{A})m = 0$ for every $m \in M$. □

2.2 Integral elements, integral and finite algebras

Definition 2.6. *Let A be a ring.*

- *An A-algebra is the data of a ring B and a ring homomorphism $\iota : A \to B$ (we often omit ι from the notation).*

- *An A-algebra B is finite if B is a finitely generated A-module (with the A-module structure described in Example 2.2).*

Example 2.7. *(i) If $K \to L$ is a field homomorphism, then L is a finite K-algebra if it is a finite-dimensional K-vector space.*

(ii) Let $D \in \mathbb{Z}$ be an integer that is not a square. The ring $\mathbb{Z}[\sqrt{D}] = \{a + b\sqrt{D}, a, b \in \mathbb{Z}\} \subset \mathbb{C}$ is a finite $\mathbb{Z}$-algebra.

(iii) Let k be a field, $A = k[X]$ and $f(X) \in A$. The ring

$$B = k[X, Y]/(Y^2 - f(X)) = A[Y]/(Y^2 - f(X))$$

is a finite A-algebra.

(iv) If A is a ring and $I \subset A$ is an ideal, then A/I is a finite A-algebra.

(v) Let k be a field; the ring $k[X]$ is a k-algebra, not finite.

(vi) Let $A = k[X] \to B = k[X, Y]/(XY - 1)$. The A-algebra B is not finite; we can check this directly, and we will give a proof in the remark below.

Remark 2.8. *Let $A \to B$ be a finite A-algebra. Choose $b_1, \ldots, b_n \in B$ that generate B as an A-module. Let $b \in B$; write, for $1 \leq i \leq n$,*

$$bb_i = \sum_{j=1}^{n} a_{ij} b_j, \ a_{ij} \in A.$$

Let $\mathsf{A} = (a_{ij})_{1 \leq i,j \leq n} \in M_{n \times n}(A)$, and $\mathsf{b} = (b_1, \ldots, b_n)$. We have $(b\mathsf{I}_n - \mathsf{A})\mathsf{b} = 0$, so $\det(b\mathsf{I}_n - \mathsf{A})b' = 0$ for every $b' \in B$, thanks to Lemma 2.5. Taking $b' = 1$ we find $\det(b\mathsf{I}_n - \mathsf{A}) = 0$. Finally, note that we can write

$$\det(b\mathsf{I}_n - \mathsf{A}) = b^n + a_{n-1}b^{n-1} + \ldots + a_0, \ \text{with } a_0, \ldots, a_{n-1} \in A.$$

We have thus shown that every $b \in B$ is a root of a monic polynomial in $A[X]$. Note that in the last example above, $Y \in k[X, Y]/(XY - 1)$ does not satisfy this property.

Definition 2.9. *Let $A \to B$ be an A-algebra.*

- *An element $b \in B$ is integral over A if there exists a monic $P(X) \in A[X]$ such that $P(b) = 0$.*
- *We say that B is an integral A-algebra if every $b \in B$ is integral over A.*

If $\iota : A \to B$ is an A-algebra and $b \in B$, we denote by $A[b] \subset B$ the smallest A-algebra containing $\iota(A)$ and b, i.e., the set of polynomial expressions in b with coefficients in $\iota(A)$.

Proposition 2.10. *Let B be an A-algebra, and let $b \in B$. The following properties are equivalent.*

1. *b is integral over A.*
2. *$A[b] \subset B$ is a finite A-algebra.*
3. *There exists a finite A-algebra $B' \subset B$ such that $b \in B'$.*

In particular, if B is a finite A-algebra then it is integral.

Proof. (1) $\Rightarrow$ (2): suppose that $b^n + a_{n-1}b^{n-1} + \ldots + a_0 = 0$. Then $b^n = -a_{n-1}b^{n-1} - \ldots - a_0$, so $b^n \in A + bA = \ldots + b^{n-1}A$, and more generally $b^m \in A + bA = \ldots + b^{n-1}A$ for every $m \geq n$. So $A[b]$ is generated by $1, b, \ldots, b^{n-1}$ as an A-module.

(2) $\Rightarrow$ (3): take $B' = A[b]$.

(3) $\Rightarrow$ (1): same argument as in Remark 2.8. □

Example 2.11. *Let $K \to L$ be a field homomorphism. An element $x \in L$ integral over K is called an algebraic element over K, and we say that L/K is algebraic if L is an integral K-algebra. The fact that x is algebraic is equivalent to the existence of $P(X) \in K[X] \smallsetminus \{0\}$ such that $P(x) = 0$. Indeed, if such a P exists, we can always make it monic by multiplying by the inverse of the leading coefficient.*

For example, $L = \mathbb{Q}(\sqrt[3]{2}) = \{a + b\sqrt[3]{2} + c\sqrt[3]{4}, a, b, c \in \mathbb{Q}\} \subset \mathbb{R}$ is algebraic over $\mathbb{Q}$, by Proposition 2.10. Note that, given $x \in L$ (for example $5 + 3\sqrt[3]{2} + \sqrt[3]{4}$), it is not immediate to find a nonzero polynomial $P(X) \in \mathbb{Q}[X]$ such that $P(x) = 0$, whose existence is guaranteed by Proposition 2.10.

Corollary 2.12. *Let A be a ring, B an A-algebra and C a B-algebra (so we have homomorphisms $A \to B \to C$).*

1. *If B is a finite A-algebra and C is a finite B-algebra then C is a finite A-algebra.*
2. *If $y_1, \ldots, y_n \in B$ are integral over A, then $A[y_1, \ldots, y_n]$ is finite over A.*
3. *If B is an integral A-algebra and C is an integral B-algebra then C is an integral A-algebra.*
4. *The set $\tilde{A} = \{y \in B \mid y \text{ is integral over } A\}$ is a subring of B.*

Proof. 1. As in linear algebra: let $b_1, \dots, b_n \in B$ that generate B as an A-module, and $c_1, \dots, c_m \in C$ that generate C as a B-module. We will show that the $b_i c_j, 1 \leq i \leq n, 1 \leq j \leq m$, generate C as an A-module. Given $c \in C$, there exist $b_1(c), \dots, b_m(c) \in B$ such that $c = \sum_{j=1}^m b_j(c) c_j$. On the other hand, for $1 \leq j \leq m$ we can write $b_j(c) = \sum_{i=1}^n a_{ij} b_i$. So $c = \sum_{i,j} a_{ij} b_i c_j$.

2. By induction on n; if $n = 1$, the result follows from Proposition 2.10. Assume $n > 1$. By induction, $B = A[y_1, \dots, y_{n-1}]$ is finite over A; moreover, $A[y_1, \dots, y_n] = B[y_n]$ is finite over B by Proposition 2.10, so it is finite over A by 1.

3. Let $c \in C$. There exist $b_0, \dots, b_{n-1} \in B$ such that $c^n + b_{n-1} c^{n-1} + \dots + c_0 = 0$, so c is integral over $B' = A[b_0, \dots, b_{n-1}]$, so $B'[c]$ is finite over B' by Proposition 2.10. On the other hand B' is finite over A by 2., so $B'[c]$ is finite over A by 1. Proposition 2.10 implies that c is integral over A.

4. Let $y_1, y_2 \in \tilde{A}$. We know by 2. that $A[y_1, y_2]$ is finite over A, so $A[y_1, y_2] \subset \tilde{B}$ by Proposition 2.10. In particular $y_1 + y_2$ and $y_1 y_2$ belong to $\tilde{A}$.

□

Definition 2.13. *Let B be an A-algebra. The ring*

$$\tilde{A} = \{y \in B \mid y \text{ is integral over } A\}$$

is called the integral closure of A in B. If A is an integral domain and $B = \mathrm{Frac}(A)$, we call $\tilde{A}$ the integral closure of A. We say that an integral domain A is integrally closed if it coincides with its integral closure.

Remark 2.14. *The arguments in the proof of the corollary are quite indirect and do not give a way to determine $\tilde{A}$. This is not a simple task in general, as we will see in the examples below.*

Example 2.15.

- *Let $A = \mathbb{Z}$ and $B = \mathbb{Q}(\sqrt{5})$. Since $\sqrt{5}$ is integral over A (it is a root of $X^2 - 5$) we have $\mathbb{Z}[\sqrt{5}] \subset \tilde{A}$. But the inclusion is not an equality. Indeed, the golden ratio $\varphi = \frac{1+\sqrt{5}}{2}$ does not belong to $\mathbb{Z}[\sqrt{5}]$, but it satisfies $\varphi^2 - \varphi - 1$, so $\varphi \in \tilde{A}$. In fact, we have $\tilde{A} = \mathbb{Z}[\varphi]$.*

- *More generally, if $D \in \mathbb{Z} \smallsetminus \{0, 1\}$ is square-free, then the integral closure $\tilde{A}$ of $\mathbb{Z}$ in $\mathbb{Q}(\sqrt{D})$ is (proof in TD)*

$$\mathbb{Z}[\sqrt{D}] = \{a + b\sqrt{D}, a, b \in \mathbb{Z}\} \text{ if } D \equiv 2, 3 \pmod 4;$$
$$\mathbb{Z}[(1 + \sqrt{D})/2] = \{a + b(1 + \sqrt{D})/2, a, b \in \mathbb{Z}\} \text{ if } D \equiv 1 \pmod 4.$$

Note that in both cases, the $\mathbb{Z}$-algebra $\tilde{A}$ is finite. We will see later a generalization of this phenomenon.

- *The integral closure of* $\mathbb{Z}$ *in* $\mathbb{Q}(\sqrt[3]{10})$ *strictly contains* $\mathbb{Z}[\sqrt[3]{10}]$.
- *If* k *is a field then* $k[X_1, \ldots, X_n]$ *is a factorial ring, so it is integrally closed (TD).*
- *Let* $A = \mathbb{C}[X,Y]/(Y^2 - X^3)$. *This is an integral domain, which is not integrally closed. Indeed,* $T = \frac{Y}{X} \in \mathrm{Frac}(A)$ *satisfies* $T^2 - X = 0$, *but it does not belong to* A. *On the other hand, we have* $\mathbb{C}[T] = \tilde{A}$. *The map* $\mathrm{Spec}(\tilde{A}) \to \mathrm{Spec}(A)$ *induced by the inclusion* $A \to \tilde{A}$ *induces a bijection between maximal ideals, sending* $(T-t)$ *to* $(X - t^2, Y - t^3)$, *thus corresponding to the parametrization* $t \mapsto (t^2, t^3)$ *of the points of the curve* $y^2 = x^3$.

Finite algebras and coverings. Let us return to the example of the inclusion

$$p : A = \mathbb{C}[X] \to B = \mathbb{C}[X,Y]/(XY - 1).$$

It corresponds to the projection π of the hyperbola with equation $xy = 1$ onto the $y = 0$ axis. Note that π is not a "covering" of the $y = 0$ axis, because $(0,0)$ is not in the image of π. On the algebraic side, the ideal $(X) \subset \mathbb{C}[X]$ is not in the image of $p^\sharp$.

On the other hand, we saw in Example 1.15 that the inclusion $\mathbb{C}[X] \to \mathbb{C}[X,Y]/(Y^2 - X)$ induces a surjection at the level of spectra; the next proposition shows that this is a general property of integral ring extensions.

Proposition 2.16. *Let* $A \to B$ *be an injective ring homomorphism such that* B *is an integral* A*-algebra. The induced map* $\mathrm{Spec}(B) \to \mathrm{Spec}(A)$ *is surjective.*

Proof. We identify A with a subring of B. Let $\mathfrak{p} \in \mathrm{Spec}(A)$, and $S = A \smallsetminus \mathfrak{p}$; this is a multiplicative subset of B. Let $I = \{\sum_i p_i b_i, p_i \in \mathfrak{p}, b_i \in B\}$; this is an ideal of B. We will show that

$$I \cap S = \emptyset. \tag{2.1}$$

Assuming this fact for now, let us finish the proof. Proposition 1.17 implies that there exists $\mathfrak{q} \in \mathrm{Spec}(B)$ such that $\mathfrak{q} \supset I$ and $\mathfrak{q} \cap S = \emptyset$. Since $\mathfrak{q} \supset I$ we have $\mathfrak{p} \subset \mathfrak{q} \cap A$, and the inclusion is an equality because $\mathfrak{q} \cap (A \smallsetminus \mathfrak{p}) = \emptyset$.

It remains to show (2.1). Suppose by contradiction that there exists $s \in S \cap I$; write $s = b_1 p_1 + \ldots + b_n p_n$ with $p_1, \ldots, p_n \in \mathfrak{p}$ and $b_1, \ldots, b_n \in B$. Let $B' = A[b_1, \ldots, b_n]$; this is a finite A-algebra by Corollary 2.12. Choose generators $b'_1, \ldots, b'_m$ of B' as an A-module. Then $I' = b'_1\mathfrak{p} + \ldots + b'_m\mathfrak{p} \subset B'$ is an ideal, and $s \in I'$. So $b'_i s \in I'$ for $1 \leq i \leq m$, and we can write:

$$b'_i s = \sum_{j=1}^{m} p_{ij} b'_j \text{ with } p_{ij} \in \mathfrak{p}.$$

Let $\mathsf{P} = (p_{ij})_{1\leq i,j\leq m}$ and $\mathsf{b}' = (b'_1, \ldots, b'_m)$. We deduce that $(s\mathsf{I}_\mathsf{m} - \mathsf{P})\mathsf{b}' = 0$, so $\det(s\mathsf{I}_\mathsf{m} - \mathsf{P})b' = 0$ for every $b' \in B'$, by Lemma 2.5. Taking $b' = 1$ we find that

$$0 = \det(s\mathsf{I}_\mathsf{m} - \mathsf{P}) = s^m + p_{m-1}s^{m-1} + \ldots + p_0, \text{ with } p_0, \ldots, p_{m-1} \in \mathfrak{p}.$$

This implies that s^m belongs to $\mathfrak{p}$, so s also since $\mathfrak{p}$ is prime; but s belongs to S, contradiction. □

Remark 2.17. *The injectivity of the homomorphism is a necessary hypothesis: if I is an ideal of A, then A/I is a finite A-algebra, but the map* $\mathrm{Spec}(A/I) \to \mathrm{Spec}(A)$ *is injective and not surjective in general.*

Finite algebras over a field

Lemma 2.18. *Let $A \to B$ be an injective ring homomorphism such that B is integral over A.*

1. *If B is a field then A is a field.*
2. *If A is a field and B is an integral domain then B is a field.*

Proof.

1. This is a special case of Proposition 2.16, but it can also be checked by hand: let $a \in A \smallsetminus \{0\}$ and $b = a^{-1} \in B$. There exist $a_0, \ldots, a_{n-1} \in A$ such that $b^n + a_{n-1}b^{n-1} + \ldots + a_0 = 0$, so
$$b = -(a_{n-1} + aa_{n-2} + \ldots + a^{n-1}a_0) \in A.$$
2. Let $b \in B \smallsetminus \{0\}$, and let $a_0, \ldots, a_{n-1} \in A$ such that $b^n + a_{n-1}b^{n-1} + \ldots + a_0 = 0$. Since b is not a zero divisor, we may assume that $a_0 \neq 0$, so $c = -a_0^{-1}(b^{n-1} + a_{n-1}b^{n-2} + \ldots + a_1)$ satisfies $bc = 1$.

□

Proposition 2.19. *Let k be a field and A a finite k-algebra.*

1. $\mathrm{Spec}(A) = \mathrm{MaxSpec}(A)$, *and for every $\mathfrak{m} \in \mathrm{MaxSpec}(A)$ the quotient $A/\mathfrak{m}$ is a finite extension of k.*
2. $\mathrm{Spec}(A)$ *is finite.*
3. $A/\sqrt{A} \simeq \prod_{\mathfrak{m}\in\mathrm{MaxSpec}(A)} A/\mathfrak{m}$.

In particular, A is reduced if and only if A is a product of fields.

Proof. 1. Let $\mathfrak{p} \in \mathrm{Spec}(A)$. By Corollary 2.12 the composition $k \to A \to A/\mathfrak{p}$ endows $A/\mathfrak{p}$ with a finite k-algebra structure, so $A/\mathfrak{m}$ is a field (and a finite extension of k) by Lemma 2.18.

2. Let $\mathfrak{p}_1, \ldots, \mathfrak{p}_l \in \mathrm{Spec}(A)$. By 1. we have $\mathfrak{p}_i + \mathfrak{p}_j = A$ if $i \neq j$. Lemma 1.5 implies that $A/\mathfrak{p}_1 \ldots \mathfrak{p}_k \simeq A/\mathfrak{p}_1 \times \cdots \times A/\mathfrak{p}_l$. So we have

$$l \leq \dim_k(A/\mathfrak{p}_1 \ldots \mathfrak{p}_l) \leq \dim_k(A).$$

3. Same argument as the previous point, using Corollary 1.18.

□

Example 2.20.

- *Every finite reduced $\mathbb{C}$-algebra is a (finite) product of copies of $\mathbb{C}$.*
- *Let A be a ring and B an A-algebra, free of rank n as an A-module. Let $\mathfrak{m} \in \mathrm{MaxSpec}(A)$ and $k(\mathfrak{m}) = A/\mathfrak{m}$. The quotient $B/\mathfrak{m}B$ is free of rank n over $k(\mathfrak{m})$, so it contains at most n prime ideals by the proof of Proposition 2.19.*

  For example, for $A = \mathbb{Z}$ and $B = \mathbb{Z}[\sqrt[n]{2}]$, the spectrum of $B/(p)$ where p is a prime number contains at most n elements. Can you give conditions that imply that $\mathrm{Spec}(B/(p))$ has cardinality n?

3 Modules and Noetherian rings

3.1 Basic properties and Hilbert's basis theorem

Definition 3.1. *Let A be a ring. An A-module M is Noetherian if every submodule $N \subset M$ is finitely generated. We say that A is a Noetherian ring if it is Noetherian as an A-module, i.e., if every ideal $I \subset A$ is of the form $(a_1, \ldots, a_k)$, with $k \geq 0$ and $a_1 \ldots, a_k \in A$.*

Lemma 3.2. *Let A be a ring and M an A-module. The following conditions are equivalent.*

1. *M is Noetherian.*
2. *Every chain $N_1 \subset N_2 \subset \ldots \subset M$ of submodules of M is stationary (i.e., there exists $k \geq 1$ such that $N_j = N_k$ for all $j \geq k$).*
3. *Every non-empty set of submodules of M has a maximal element with respect to inclusion.*

Proof. (1) $\Rightarrow$ (2). Let $N_\infty = \cup_{i\geq 1} N_i$; this is a submodule of M, so there exist $m_1, \ldots, m_r \in N_\infty$ such that $N_\infty = Am_1 + \ldots + Am_r$. There exists $k \geq 1$ such that $m_i \in N_k$ for all $1 \leq i \leq r$. So $N_\infty \subset N_k$, and $N_j = N_k$ if $j \geq k$.

(2) $\Rightarrow$ (3). Let S be a non-empty set of submodules of M; choose $N_1 \in S$. For $i \geq 1$, if N_i is not maximal then there exists $N_{i+1} \in S$ such that $N_{i+1} \supsetneq N_i$. The chain $N_1 \subsetneq N_2 \subsetneq \ldots$ is stationary, so there exists $k \geq 1$ such that N_k is maximal.

(3) $\Rightarrow$ (1). Let $N \subset M$ be a submodule, and S the set of finitely generated submodules of N. We have $(0) \in S$, so S is non-empty and contains a maximal element N'. Let us show by contradiction that $N' = N$. If $N' \subsetneq N$, let $n \in N \smallsetminus N'$. The module $N' + An$ belongs to S and properly contains N', contradiction. □

Remark 3.3. *In particular, in a Noetherian ring every non-empty set of ideals has a maximal element, which simplifies the proofs of Propositions 1.16 and 1.17.*

Lemma 3.4. *Let A be a ring.*

1. *If $M_1, \ldots, M_r$ are Noetherian A-modules, then $M_1 \oplus \ldots \oplus M_r$ is Noetherian.*
2. *If $f : M \to M'$ is a surjective homomorphism of A-modules and M is Noetherian then M' is Noetherian.*
3. *Assume A is Noetherian. Then an A-module is Noetherian if and only if it is finitely generated.*
4. *If A is a Noetherian ring and $A \to B$ is a finite A-algebra then B is a Noetherian ring.*

Proof.

1. By induction on r; if $r = 1$ the statement is tautological. For $r \geq 2$, let $N \subset M_1 \oplus \ldots \oplus M_r$ be a submodule, $N_r = N \cap M_r$ and $N^{(r)} = N/N_r$. The projection onto $M_1 \oplus \cdots \oplus M_{r-1}$ induces an injection $N^{(r)} \to M_1 \oplus \cdots \oplus M_{r-1}$, so $N^{(r)}$ is a finitely generated A-module, by the inductive hypothesis. Let $n_1, \ldots, n_k \in N$ whose images in $N^{(r)}$ generate $N^{(r)}$. Then $N = N_r + An_1 + \ldots + An_k$ is finitely generated, because N_r is a finitely generated A-module.
2. Let $N' \subset M'$ be a submodule and $N = f^{-1}(N')$. There exist $n_1, \ldots, n_r$ that generate N, so $f(n_1), \ldots, f(n_r)$ generate $f(N) = N'$.
3. By definition every Noetherian A-module is finitely generated. Conversely, if there is a surjection $A^r \to M$ then A^r is Noetherian by 1., so M is Noetherian by 2.
4. B is a Noetherian A-module by 3., so every ideal $I \subset B$ is a finitely generated A-module, hence a finitely generated B-module.

□

Example 3.5.
- *Every principal ideal ring (e.g. $\mathbb{Z}$ or $k[X]$ for a field k) is Noetherian.*
- *Let k be a field. The ring $k[X_1, X_2, \ldots, X_n, \ldots]$ is not Noetherian, because $(X_1) \subset (X_1, X_2) \subset \cdots$ is a non-stationary chain of ideals.*
- *Let k be a field. The ring $\{a + XP(X,Y), a \in k\} = k[X, XY, XY^2, \ldots] \subset k[X,Y]$ is not Noetherian. Indeed, the ideal $(X, XY, XY^2, \ldots)$ is not finitely generated.*

Theorem 3.6. *(Hilbert's basis theorem) If A is a Noetherian ring, then $A[X]$ is Noetherian.*

Corollary 3.7. *Let k be a field.*

1. *For every $n \geq 0$, the ring $k[X_1, \ldots, X_n]$ is Noetherian.*
2. *For every $n \geq 0$ and every ideal $I \subset k[X_1, \ldots, X_n]$ the ring $k[X_1, \ldots, X_n]/I$ is Noetherian.*

Proof.
1. Theorem 3.6 + induction on n.
2. 1.+ Lemma 3.4.

□

Proof of Theorem 3.6. Let $I \subset A[X]$ be an ideal. Let

$$J = \{0\} \cup \{a \in A \mid \exists P(X) \in I : a \text{ is the leading coefficient of } P(X)\}.$$

Let us verify that J is an ideal of A. If $P(X) \in I$ has leading coefficient $a \in A$, then for every $b \in A$ either $ab = 0$ or ab is the leading coefficient of $bP(X)$, so $bJ \subset J$. Moreover, let $P(X) = a_n X^n + \ldots + a_0 \in I$ and $Q(X) = b_m X^m + \ldots + b_0 \in I$, so $a_n, b_m \in J$. Without loss of generality, assume that $n \geq m$. Then $P(X) + X^{n-m}Q(X) = (a_n + b_m)X^{n+m} + \ldots$ belongs to I, so $a_n + b_m$ belongs to J.

Since A is Noetherian, there exist $a_1, \ldots, a_r$ that generate J. For $1 \leq i \leq r$ choose $P_i(X) \in I$ with leading coefficient a_i, and denote by k_i the degree of $P(X)$. Let $k = \max\{k_i, 1 \leq i \leq r\}$. We will show that

$$I = \{P(X) \in I \mid \deg(P(X)) \leq k\} + A[X]P_1 + \ldots + A[X]P_r$$

which implies (thanks to Lemma 3.4(3)) that I is finitely generated as an $A[X]$-module. Let $P(X) = aX^d + \ldots \in I$ of degree $d > k$. Write $a = a_1 b_1 + \ldots + a_r b_r$ with $b_1, \ldots b_r \in A$. Consider

$$Q(X) = P(X) - (b_1 X^{d-k_1} P_1(X) + \ldots + b_r X^{d-k_r} P_r(X)) = (a - \sum_{i=1}^{r} a_i b_i)X^d + \ldots$$

This is a polynomial of degree at most $d-1$. If $\deg(Q(X)) \leq k$ we are done, otherwise we repeat the argument.

Remark 3.8.
- *The proof is not constructive, i.e., it does not give an "explicit" set of generators of I, which surprised Hilbert's colleagues.*
- *For $A = \mathbb{C}[X_1, \ldots, X_n]$, let $(P_k(X))_{k\geq 1}$ be a sequence of polynomials in A. Let $V = \{(x_1, \ldots, x_n) \in \mathbb{C}^n \mid P_k(x_1, \ldots, x_n) = 0 \text{ for all } k \geq 1\}$. Hilbert's basis theorem tells us that we can define V as the zero set of a finite number of polynomials.*

3.2 Finiteness of the integral closure

We are interested in the following question: let A be an integral domain with fraction field K, and let L/K be a finite field extension. Let B be the integral closure of A in L. If A is Noetherian, what can we say about B?

Example 3.9. *Let $A = \mathbb{Z}$ and L a finite extension of $\mathbb{Q}$, called a number field. The integral closure of A in L is denoted O_L, and is called the ring of integers of L. This is a central object in number theory. For example, when $L = \mathbb{Q}(e^{2\pi i/p})$, the arithmetic properties of O_L were studied by Kummer in his work on Fermat's equation $X^p + Y^p = Z^p$.*

Lemma 3.10. *Let A be an integral domain, K its fraction field, and L/K a finite field extension of degree n.*

1. *For every $x \in L$ there exists $d \in A$ such that dx is integral over A.*
2. *There exists a basis $x_1, \ldots, x_n$ of L as a K-vector space such that x_i is integral over A for $1 \leq i \leq n$.*

Proof.
1. Let $x \in L$ and let $c_0, \ldots, c_{k-1} \in K$ such that $x^k + c_{k-1}x^{k-1} + \ldots + c_0 = 0$. Write $c_i = \frac{a_i}{d}$, with $a_i, d \in A$. Then we have
$$d^k x^k + a_{k-1}d^{k-1}x^{k-1} + a_{k-2}dd^{k-2}x^{k-2} + \ldots + a_0 d^{k-1} = 0,$$
which shows that dx is integral over A.
2. Apply 1. to a basis of L as a K-vector space.

□

Theorem 3.11. *Let A be an integral domain, with fraction field K of characteristic zero. Let L/K be a finite field extension, and B the integral closure of A in L. If A is Noetherian and integrally closed, then B is a finite A-algebra, hence a Noetherian ring.*

Before proving the theorem, here is an important application in number theory and geometry.

Proposition 3.12. *Let $A = \mathbb{Z}$ or $k[T]$, where k is a field of characteristic zero. Let L be a finite extension of $K = \mathrm{Frac}(A)$. The integral closure B of A in L has the following properties:*

1. *B is a free A-module of rank $[L : K]$;*
2. *B is Noetherian;*
3. *B is integrally closed;*
4. *Every nonzero prime ideal of B is maximal.*

Proof.

1. B is a finitely generated A-module and torsion-free, hence free, because A is a principal ideal domain. Moreover, by Lemma 3.10 B contains a free A-module of rank $[L : K]$, so its rank is at least $[L : K]$. In fact, the rank of B is exactly $[L : K]$, because A-linearly independent elements in L are also K-linearly independent.
2. =1+Lemma 3.4.
3. We have $\mathrm{Frac}(B) = L$ by Lemma 3.10. If $x \in L$ is integral over B then it is integral over A thanks to Corollary 2.12, so $x \in B$.
4. Let $\mathfrak{p} \in \mathrm{Spec}(B)$ nonzero. Choose $x \in B$; there exist $a_0, \ldots, a_{k-1} \in A$ with $a_0 \neq 0$ such that $x^k + a_{k-1}x^{k-1} + \ldots + a_0 = 0$, so $a_0 \in \mathfrak{q} = \mathfrak{p} \cap A$. We deduce that $\mathfrak{q}$ is a nonzero prime ideal of A, so it is maximal. The homomorphism $A/\mathfrak{q} \to B/\mathfrak{p}$ is injective and $B/\mathfrak{p}$ is integral over $A/\mathfrak{q}$. Since $A/\mathfrak{q}$ is a field, Lemma 2.18 implies that $B/\mathfrak{p}$ is also a field.

□

Trace. From now on, fix the notations and hypotheses of Theorem 3.11, and denote $n = [L : K]$. The main tool in the proof of the Theorem is a K-bilinear form $\langle \cdot, \cdot \rangle : L \times L \to K$, which we will now define. For every $x \in L$, multiplication by x is a K-linear map $m_x : L \to L$, $m_x(y) = xy$. We call the trace of x the trace of m_x, denoted $Tr(x)$. We define

$$\begin{aligned} \langle \cdot, \cdot \rangle : L \times L &\to K \\ (x, y) &\mapsto Tr(xy). \end{aligned}$$

The properties of the trace that will be fundamental for us are given by the following lemma.

Lemma 3.13.

1. *If $b \in B$ then $Tr(b) \in A$.*
2. *The bilinear form $\langle \cdot, \cdot \rangle$ is non-degenerate.*

Proof. 1. Let $P(X) \in A[X]$ be a monic polynomial such that $P(b) = 0$. Let $M(X) \in K[X]$ be the monic polynomial of minimal degree such that $M(b) = 0$. We will show the following two facts in TD:

- $M(X) \mid P(X)$;
- the characteristic polynomial of m_b is a power of $M(X)$.

Since $Tr(b)$ is a coefficient of the characteristic polynomial of m_b, it suffices to show that $M(X) \in A[X]$. In a finite extension of the field K, we can write $M(X) = (X - \beta_1) \cdots (X - \beta_t)$ with $b = \beta_1$, which implies that $P(\beta_i) = 0$ for $1 \leq i \leq t$. So

$$M(X) = X^t - (\beta_1 + \ldots + \beta_t)X^{t-1} + (\sum_{1 \leq i < j \leq t} \beta_i \beta_j)X^{t-2} - \ldots \pm \beta_1 \cdots \beta_t$$

has coefficients integral over A. Since $M(X) \in K[X]$ and A is integrally closed, we deduce that $M(X)$ belongs to $A[X]$.

2. For every $x \in L^\times$, we have $\langle x, x^{-1} \rangle = Tr(1) = n \neq 0$.

□

Proof of Theorem 3.11. Choose, thanks to Lemma 3.10, $b_1, \ldots, b_n \in B$ that form a basis of L as a $K-$vector space. Let $b \in B$; write $b = x_1 b_1 + \ldots + x_n b_n$ with $x_1, \ldots, x_n \in K$. To prove the theorem, we need to bound the denominators of the x_i independently of b. For $1 \leq j \leq n$, we have

$$bb_j = \sum_{i=1}^{n} x_i b_i b_j, \text{ so } Tr(bb_j) = \sum_{i=1}^{n} x_i Tr(b_i b_j).$$

Moreover, $bb_j \in B$ so $Tr(bb_j) \in A$ thanks to Lemma 3.13. Let $\mathsf{T} \in M_{n \times n}(A)$ be the matrix whose (i, j) entry is $Tr(b_i b_j)$, and $\mathsf{x} = (x_1, \ldots, x_n)$. The above discussion implies that xT belongs to A^n, so

$$\mathsf{x}\mathsf{T}\, {}^t\mathrm{com}\mathsf{T} = \mathsf{x} \det(\mathsf{T}) \in A^n.$$

Lemma 3.13 implies that $d = \det(\mathsf{T}) \neq 0$, so $x_i \in \frac{1}{d}A$ for $1 \leq i \leq n$. We have thus shown that $B \subset \frac{b_1}{d}A + \ldots + \frac{b_1}{d}A$, so Lemma 3.4 implies that B is a finitely generated A-module.

Remark 3.14. *The above argument works if the characteristic of K does not divide $[L : K]$. In fact, the theorem is true if L/K is separable, which implies that Lemma 3.13(2) remains true.*

Definition 3.15. *A Dedekind domain is a Noetherian ring, integrally closed, and such that every nonzero prime ideal is maximal.*

Example 3.16.

- *The ring of integers O_L of a number field L is a Dedekind domain, by Proposition 3.12. On the other hand, $\mathbb{Z}[2i]$ is not a Dedekind domain, because it is not integrally closed.*

- *For $t \in \mathbb{C}$, the ring $\mathbb{C}[X,Y]/(Y^2 - X(X-1)(X-t))$ is Dedekind if and only if $t \neq 0, 1$. We see in this example - and will understand better later in the course - that the notion of Dedekind domain corresponds to the geometric notion of a smooth curve. So, given an integral domain $B = \mathbb{C}[X,Y]/(P(X,Y))$, replacing B by its integral closure corresponds geometrically to transforming the curve $\{(x,y) \in \mathbb{C}^2 \mid P(x,y) = 0\}$ into a smooth curve (resolution of singularities).*

4 Noether normalization and Nullstellensatz

We fix a field k; if A and B are k-algebras, a ring homomorphism $f : A \to B$ is called a k-algebra homomorphism if $f(x) = x$ for all $x \in k$. We are interested in algebras A that are finitely generated over k, i.e., such that there exists a surjective k-algebra homomorphism $k[X_1, \ldots, X_n] \to A$ for some integer $n \geq 1$. In other words, we can write $A = k[X_1, \ldots, X_n]/I$ for some ideal $I \subset k[X_1, \ldots, X_n]$. We know by Corollary 3.7 that there exist $P_1, \ldots, P_m \in k[X_1, \ldots X_n]$ that generate the ideal I. We denote

$$Z_k(I) = \{(x_1, \ldots, x_n) \in k^n \mid P_i(x_1, \ldots, x_n) = 0 \text{ for } 1 \leq i \leq m\}.$$

We will show two key properties of "algebraic varieties" $Z_k(I)$, when k is algebraically closed:

1. There exists an integer $d \geq 1$ (which depends on I) and a "finite covering" $Z_k(I) \to k^d$. Intuitively, d is the dimension of the space $Z_k(I)$.

2. $Z_k(I)$ is determined by A: the map $Z_k(I) \to \mathrm{MaxSpec}(A)$ sending $(x_1, \ldots, x_n)$ to $(X - x_1, \ldots, X - x_n)$ is a bijection.

4.1 Noether normalization theorem

Example 4.1. *Let k be a field and $A = k[X,Y]/(XY-1)$. We want to endow A with a finite $k[T]$-algebra structure. We have seen that the map sending T to X - which corresponds to the projection of the hyperbola $xy = 1$ onto the $y = 0$ axis - does not work. We will try to project the hyperbola onto another line through the origin. Algebraically, set $X' = X + aY$ with $a \in k^\times$. So we have $A = k[X',Y]/((X'-aY)Y-1)$, which gives the following equality in A:*

$$-aY^2 + X'Y - 1 = 0 \Rightarrow Y^2 - \frac{X'}{a}Y + \frac{1}{a} = 0.$$

So the homomorphism $k[T] \to A$ sending T to $X + aY$ with $a \in k^\times$ gives A the structure of a finite $k[T]$-algebra.

Definition 4.2. *Let k be a field, A a k-algebra and $x_1, \dots, x_n \in A$. We say that $x_1, \dots, x_n$ are algebraically independent over k if for every $P \in k[X_1, \dots, X_n] \setminus \{0\}$ we have $P(x_1, \dots, x_n) \neq 0$. In other words, the map*

$$\begin{aligned} ev_{x_1,\dots,x_n} : k[X_1, \dots, X_n] &\to A \\ P &\mapsto P(x_1, \dots, x_n) \end{aligned}$$

is injective.

Theorem 4.3. *(Noether normalization) Let k be a field and A a finitely generated k-algebra. There exist an integer $d \geq 0$ and $x_1, \dots, x_d \in A$ algebraically independent over k such that*

$$ev_{x_1,\dots,x_d} : k[X_1, \dots, X_d] \to A$$

is a finite $k[X_1, \dots, X_d]-$algebra.

Proof. We will give the proof for k infinite, generalizing the technique in Example 4.1. For the general case, cf. [1, Theorem 2.1, p. 357].

By hypothesis, there exists a surjective homomorphism $f : k[X_1, \dots, X_n] \to A$ for some integer $n \geq 0$. Denote $a_i = f(X_i)$ for $1 \leq i \leq n$. We will prove the statement by induction on n; for $n = 0$, f is an isomorphism and the statement is true with $d = 0$. For arbitrary n, if f is an isomorphism then $f = ev_{a_1,\dots,a_n}$ satisfies the conclusion of the theorem. Otherwise, let $P(X_1, \dots, X_n) \in k[X_1, \dots, X_n] \setminus \{0\}$ such that $P(a_1, \dots, a_n) = 0$. We will show that there exist $b_1, \dots, b_n \in A$ such that $A = k[b_1, \dots, b_n]$ and A is a finite $k[b_1, \dots, b_{n-1}]-$algebra. By induction, there exist $x_1, \dots, x_d \in k[b_1, \dots, b_{n-1}]$ algebraically independent over k such that $k[b_1, \dots, b_{n-1}]$ is a finite $k[x_1, \dots, x_d]$-algebra. Corollary 2.12 implies that A is a finite $k[x_1, \dots, x_d]$-algebra, so $ev_{x_1,\dots,x_d}$ satisfies the conclusion of the theorem.

We set $b_n = a_n$, and we look for $b_1, \ldots, b_{n-1}$ of the form $b_i = a_i - \alpha_i a_n$, with $\alpha_1, \ldots, \alpha_{n-1} \in k$ to be determined. Write

$$P(X_1, \ldots, X_n) = P_r(X_1, \ldots, X_n) + P_{r-1}(X_1, \ldots, X_n) + \ldots + P_0,$$

with $P_i(X_1, \ldots, X_n)$ homogeneous of degree i and $P_r \neq 0$. In particular,

$$P_r(X_1, \ldots, X_n) = \sum_{i_1+\ldots+i_n=r} c_{i_1,\ldots,i_r} X_1^{i_1} X_2^{i_2} \cdots X_n^{i_n},$$

so

$$P(a_1, \ldots, a_n) = \sum_{i_1+\ldots+i_n=r} c_{i_1,\ldots,i_r} (b_1+\alpha_1 b_n)^{i_1} \cdots (b_{n-1}+\alpha_{n-1} b_n)^{i_{n-1}} b_n^{i_n} + Q(b_1, \ldots, b_n)$$

where $\deg(Q) < r$. Since $P(a_1, \ldots, a_n) = 0$, we find

$$\begin{aligned} 0 &= \left(\sum_{i_1+\ldots+i_n=r} c_{i_1,\ldots,i_r} \alpha_1^{i_1} \cdots \alpha_{n-1}^{i_{n-1}} \right) b_n^r + \text{ terms where } b_n \text{ appears with degree } < r \\ &= P_r(\alpha_1, \ldots, \alpha_{n-1}, 1) b_n^r + \text{ terms where } b_n \text{ appears with degree } < r. \end{aligned}$$

It remains to show that there exist $\alpha_1, \ldots, \alpha_{n-1} \in k$ such that $P_r(\alpha_1, \ldots, \alpha_{n-1}, 1) \neq 0$. Suppose the contrary; the polynomial P_r being homogeneous and nonzero, we have $P_r(\alpha_1, \ldots, \alpha_{n-1}, \alpha_n) = 0$ for all $\alpha_1, \ldots, \alpha_{n-1} \in k$ and $\alpha_n \in k^\times$. We will show that this is not possible. Write

$$P_r(X_1, \ldots, X_n) = \sum_{i=0}^{t} Q_i(X_1, \ldots, X_{n-1}) X_n^i.$$

For every $\alpha_1, \ldots, \alpha_{n-1} \in k$ the polynomial $P_r(\alpha_1, \ldots, \alpha_{n-1}, X_n) \in k[X_n]$ vanishes on $k^\times$, so, since k is infinite, it is identically zero. We deduce that $Q_i(X_1, \ldots, X_{n-1}) = 0$ for $0 \leq i \leq t$, so $P_r = 0$, contradiction. □

Theorem 4.4. *(Hilbert's Nullstellensatz) Let k be a field and $n \geq 0$ an integer.*

1. *Let $\mathfrak{m} \subset k[X_1, \ldots, X_n]$ be a maximal ideal. The quotient $k[X_1, \ldots, X_n]/\mathfrak{m}$ is a finite extension of k.*

2. *If k is algebraically closed, then every maximal ideal of $k[X_1, \ldots, X_n]$ is of the form $(X_1 - a_1, \ldots, X_n - a_n)$ with $(a_1, \ldots, a_n) \in k^n$.*

Proof. 1. The quotient $A = k[X_1, \ldots, X_n]/\mathfrak{m}$ is a finitely generated k-algebra, so by Theorem 4.3 there exists $d \geq 0$ and an injective homomorphism $k[X_1, \ldots, X_d] \to A$ such that A is a finite $k[X_1, \ldots, X_d]$-algebra. By Lemma 2.18 $k[X_1, \ldots, X_d]$ is a field, so $d = 0$.

2. Since k is algebraically closed, point 1. implies that $k[X_1, \ldots, X_n]/\mathfrak{m} \simeq k$. If $a_i \in k$ denotes the image of X_i, then $(X_1 - a_1, \ldots, X_n - a_n) \subset \mathfrak{m}$, so we have equality because both ideals are maximal.

□

4.2 Algebra-geometry dictionary

Definition 4.5.

1. *Let A be a ring and $I \subset A$ an ideal. The radical of I is the set $\sqrt{I} = \{a \in A \mid \exists k \geq 1 : a^k \in I\}$.*
2. *Let k be an algebraically closed field. An algebraic set in k^n is a subset of the form $Z_k(I) = \{x \in k^n \mid \forall P \in I, P(x) = 0\}$ for some ideal $I \subset k[X_1, \ldots, X_n]$.*

Remark 4.6. *The radical of an ideal I is the inverse image of the radical of the quotient ring A/I, so it is an ideal.*

Geometrically, Hilbert's Nullstellensatz tells us that the maximal ideals of $k[X_1, \ldots, X_n]$ with k algebraically closed correspond to the simplest algebraic sets in k^n, i.e., points. More generally, there is a close link between ideals of $k[X_1, \ldots, X_n]$ and algebraic sets in k^n.

Corollary 4.7. *Let k be an algebraically closed field, $I \subset k[X_1, \ldots, X_n]$ an ideal and $A = k[X_1, \ldots, X_n]/I$. The map*

$$\begin{aligned} Z_k(I) &\to \mathrm{MaxSpec}(A) \\ (x_1, \ldots, x_n) &\mapsto (X_1 - x_1, \ldots, X_n - x_n) \end{aligned}$$

is bijective.

Proof. The bijection from Lemma 1.3(3) induces a bijection between $\mathrm{SpecMax}(A)$ and the set $\{\mathfrak{m} \in \mathrm{MaxSpec}(k[X_1, \ldots, X_n]) \mid \mathfrak{m} \supset I\}$. For $(x_1, \ldots, x_n) \in k^n$, we have $(X - x_1, \ldots, X - x_n) \supset I$ if and only if $P(x_1, \ldots, x_n) = 0$ for all $P \in I$, i.e., if and only if $(x_1, \ldots, x_n) \in Z_k(I)$. The corollary thus follows from Theorem 4.4. □

In the proof of Theorem 4.9 below we will use the following fact, which can be understood more conceptually later in terms of ring localization.

Lemma 4.8. *Let A be a ring, $a \in A$ and $B = A[X]/(aX - 1)$. If $a \in A$ is not nilpotent then B is not the zero ring.*

Proof. Suppose by contradiction that $1 = (aX - 1)Q(X) \in A[X]$ with $Q(X) = a_d X^d + \ldots + a_0 \in A[X]$. Comparing constant terms gives $1 = -a_0$. Looking at the coefficients of X we find $0 = aa_0 - a_1$ so $a_1 = -a$. Similarly, comparing coefficients of $X^2, X^3, \ldots, X^d$ shows that $aa_{i-1} - a_i = 0$ so $a_i = -a^i$ for $2 \leq i \leq d$. But the term of degree $d+1$ of $(aX-1)Q(X)$ is then $-a^{d+1}X^{d+1}$, which is nonzero because a is not nilpotent. □

Theorem 4.9. *(Nullstellensatz, strong version) Let k be an algebraically closed field and $A = k[X_1, \ldots, X_n]$.*

1. *Let I be an ideal and $P \in A$ such that $P(x) = 0$ for all $x \in Z_k(I)$. Then $P \in \sqrt{I}$.*

2. *The map $I \mapsto Z_k(I)$ induces a bijection between ideals $I \subset A$ such that $\sqrt{I} = I$ (i.e., the ring A/I is reduced) and algebraic sets in k^n.*

Proof. 1. Let $B = A/I$. If $P \notin \sqrt{I}$ then P is not nilpotent in B, so $B[Y]/(PY - 1)$ is not the zero ring by Lemma 4.8. This is a finitely generated k-algebra, which has a maximal ideal by Proposition 1.16. Thanks to Theorem 4.4, such an ideal gives us a k-algebra homomorphism $\varphi : B[Y]/(PY - 1) \to k$. Consider the composition

$$A \to A/I = B \to B[Y]/(PY - 1) \xrightarrow{\varphi} k. \tag{4.1}$$

By Theorem 4.4 its kernel $\mathfrak{m}$ is of the form $(X - x_1, \ldots, X - x_n)$ for $x = (x_1, \ldots, x_n) \in k^n$. We have $I \subset \mathfrak{m}$ so $x \in Z_k(I)$. On the other hand, the image of $P \in A$ under the composition of maps in (4.1) is a unit in k, so $P(x) \neq 0$.

2. We have $Z_k(I) = Z_k(\sqrt{I})$, so the map is surjective. Let I, J be two ideals such that $Z_k(I) = Z_k(J)$ and $\sqrt{I} = I, \sqrt{J} = J$. For every $P \in J$ we have $P \in \sqrt{I}$ by 1., so $J \subset \sqrt{I} = I$. Exchanging the roles of I and J we find that $I \subset J$, so $I = J$.

□

Remark 4.10. *The results of this section tell us that the ring $k[X_1, \ldots, X_n]$ contains enough information to recover the set of points of any algebraic set. This is only the beginning of the story:*

- *we would like to give more structure - for example a topology - to algebraic sets;*

- *In passing from ideals to algebraic sets we lose information - roughly, we "forget the nilpotents". However, even if we are only interested in algebraic sets, rings like $k[T]/(T^2)$ can be very useful: for example, what are the k-algebra homomorphisms $k[X, Y]/(Y^2 - X) \to k[T]/(T^2)$?*

Finite extensions of finitely generated k-algebras. Let k be an algebraically closed field, and let $A = k[X_1, \ldots, X_n]/I$ and $B = k[X_1, \ldots, X_m]/J$ be two finitely generated k-algebras. Let $f : A \to B$ be a k-algebra homomorphism. First, for every $\mathfrak{m} \in \mathrm{MaxSpec}(B)$ we have $f^{-1}(\mathfrak{m}) \in \mathrm{MaxSpec}(A)$. Indeed, we have

$$k \to A/f^{-1}(\mathfrak{m}) \hookrightarrow B/\mathfrak{m} \simeq k$$

so every map above is an isomorphism. Consequently, the homomorphism f induces a map $f^* : \mathrm{MaxSpec}(B) \to \mathrm{MaxSpec}(A)$ which, via the bijection of Corollary 4.7, gives a map

$$\tilde{f} : Z_k(J) \to Z_k(I).$$

Corollary 4.11. *If $f : A \to B$ is injective and B is a finite A-algebra, then for every $(x_1, \ldots, x_n) \in Z_k(I)$ the inverse image $\tilde{f}^{-1}(x_1, \ldots, x_n)$ is finite and non-empty.*

Proof. We identify A with its image in B. Let $\mathfrak{m} = (X - x_1, \ldots, X - x_n) \in \mathrm{MaxSpec}(A)$. Then

$$(f^*)^{-1}(\mathfrak{m}) = \{\mathfrak{m}' \in \mathrm{MaxSpec}(B) \mid \mathfrak{m}' \supset \mathfrak{m}\} \simeq \mathrm{MaxSpec}(B/\mathfrak{m}B).$$

Since $B/\mathfrak{m}B$ is a finite $A/\mathfrak{m}A \simeq k-$algebra, Proposition 2.19 implies that $(f^*)^{-1}(\mathfrak{m})$ is finite. The fact that it is non-empty is a consequence of Proposition 2.16. □

5 Reminders of general topology

Definition 5.1. *A topological space is a pair $(X, \mathcal{T})$ where X is a non-empty set and $\mathcal{T}$ is a set of subsets of X such that*

1. *$(\emptyset, X) \in \mathcal{T}^2$;*
2. *$\mathcal{T}$ is stable under arbitrary union;*
3. *$\mathcal{T}$ is stable under finite intersection.*

The elements of $\mathcal{T}$ are called the open sets of the topology $\mathcal{T}$ and the complements of the open sets in X are the closed sets of the topology $\mathcal{T}$.

Example 5.2. *We always have on a non-empty set X two extreme topologies:*

1. *the trivial topology, for which $\mathcal{T} = \{\emptyset, X\}$;*
2. *the discrete topology, for which $\mathcal{T} = \mathcal{P}(X)$.*

The discrete topology is the finest topology (every subset of X is open) while the trivial topology is the coarsest possible. We have presented here the most classical viewpoint, where the topology $\mathcal{T}$ consists of the open sets. We can define a topology - we will do so later - by constructing a set $\mathcal{F}$ of closed sets, which satisfy condition 1. above, such that $\mathcal{F}$ is stable under arbitrary intersection and finite union, and taking for $\mathcal{T}$ the complements of the elements of $\mathcal{F}$.

Definition 5.3. *If $(X, \mathcal{T})$ is a topological space and $Y \subset X$ is a subset, the set*

$$\mathcal{T}_Y := \{U \cap Y,\ U \in \mathcal{T}\}$$

defines a topology on Y, called the induced topology.

Definition 5.4. *If $(X, \mathcal{T})$ is a topological space and $Y \subset X$ is a subset, the closure of Y, denoted $\overline{Y}$, is the smallest closed set that contains Y.*
The subset $Y \subset X$ is dense in X if $\overline{Y} = X$.

Definition 5.5. *If $(X, \mathcal{T})$ is a topological space, a subset $\mathcal{B} \subset \mathcal{T}$ is a base of open sets if every element of $\mathcal{T}$ is a union of elements of $\mathcal{B}$.*

Example 5.6. *In the context of a metric space (X, d), by definition the topology associated to d is given by*

$$\mathcal{T}_d = \{U \in \mathcal{P}(X),\ \forall x \in U, \exists r > 0,\ B_d(x, r) \subset U\}$$

where $B_d(x, r)$ denotes the open ball with center x and radius r. It is easy to show that the open balls form a base of the topology $\mathcal{T}_d$.

Definition 5.7. *A topological space $(X, \mathcal{T})$ is Hausdorff if*

$$\forall (x, y) \in X^2,\ x \neq y,\ \exists (U_1, U_2) \in \mathcal{T}^2,\ (x \in U_1,\ y \in U_2 \text{ and } U_1 \cap U_2 = \emptyset)$$

Metric spaces always satisfy this property since points can be separated by open balls. The topologies we will encounter later will rarely satisfy this (the spaces we will deal with will therefore not be "metrizable").

Definition 5.8. *A topological space $(X, \mathcal{T})$ is quasi-compact if from every covering*

$$E = \bigcup_{i \in \mathcal{I}} U_x$$

by open sets, we can extract a finite subcovering $E = \bigcup_{j=1}^{n} U_j$.

A topological space $(X, \mathcal{T})$ is compact if it is both quasi-compact and Hausdorff. We can of course equivalently define quasi-compactness via closed sets, by taking complements: a topological space $(X, \mathcal{T})$ is quasi-compact if from every family of closed sets with empty intersection, we can extract a *finite* family of closed sets with empty intersection.

Definition 5.9. *A topological space $(X, \mathcal{T})$ is connected if X cannot be written as the disjoint union of two non-empty open sets (or equivalently of two non-empty closed sets).*

Definition 5.10. *Let $(X, \mathcal{T})$ and $(X, \mathcal{T}')$ be two topological spaces. A map $f : X \longrightarrow X'$ is continuous if for every open set $U \in \mathcal{T}'$, we have $f^{-1}(U) \in \mathcal{T}$.*

A homeomorphism between the spaces $(X, \mathcal{T})$ and $(X, \mathcal{T}')$ is a continuous map $f : X \longrightarrow X'$ bijective with inverse $f^{-1} : X' \longrightarrow X$ continuous.

6 Zariski topologies

Given a ring A, we denote by $\mathrm{MaxSpec}(A)$ the set of its maximal ideals. As you have seen in the first part of the course, Hilbert's Nullstellensatz gives an identification

$$\mathbb{C}^n \simeq \mathrm{MaxSpec}(\mathbb{C}[X_1, ..., X_n])$$

between the "affine space" $\mathbb{C}^n$ and the maximal ideals of the ring $\mathbb{C}[X_1, .., X_n]$. Corollary 4.7 pushes the analogy further for subsets of $\mathbb{C}^n$ that are solutions of a system of algebraic equations $\mathcal{S}$: the set

$$Z(\mathcal{S}) = \{(x_1, ..., x_n) \in \mathbb{C}^n, \forall P \in \mathcal{S},\ P(x_1, ..., x_n) = 0\}$$

then corresponds to $\mathrm{MaxSpec}(\mathbb{C}[X_1, ..., X_n]/I)$, where I is the ideal of $\mathbb{C}[X_1, ..., X_n]$ generated by the elements of $\mathcal{S}$.

The result holds for any algebraically closed field, and builds a bridge between algebraic problems (ideals in a ring) and geometric intuition (points in a space). The generalization of this philosophy to any ring is a great challenge undertaken by algebraic geometry, which we will approach in this second part of the course.

A first difference, as soon as we consider arbitrary rings, is the lack of functoriality of MaxSpec: if $\varphi : A \longrightarrow B$ is a ring homomorphism, the inverse image of a maximal ideal of B is not always a maximal ideal of A. For lack of considering the set MaxSpec in the sequel, we will rather associate to a ring A its spectrum, that is, the set of its *prime* ideals.

Exercise 6.1. *Show that if A and B are two rings, then*

$$\mathrm{Spec}(A \times B) = \mathrm{Spec}(A) \sqcup \mathrm{Spec}(B).$$

Definition 6.2. *If A is a ring, we associate to every ideal I of A the set*

$$V(I) := \{\mathfrak{p} \in \mathrm{Spec}(A),\ I \subset \mathfrak{p}\}$$

of prime ideals of A that contain it.

Theorem 6.3 (Krull)**.** *Every proper ideal of a ring A is contained in a maximal ideal. In particular, $V(I)$ is empty if and only if $I = A$.*

Proof. This is Proposition 1.16 applied to the ring A/I (one can also do the proof similarly to the proof of Proposition 1.16, by choosing for $\mathcal{I}$ the set of proper ideals that contain I). Thus if $I \neq A$, the ideal I is contained in a maximal ideal and $V(I) \neq \emptyset$. □

We will see that the sets $V(I)$, where I runs over the ideals of A, play the role of algebraic sets given by polynomial equations.

Proposition 6.4. *Let A be a ring. The sets $V(I)$, where I runs over all ideals of A, are the closed sets of a topology on* $\mathrm{Spec}(A)$.

Proof. On the one hand, the two sets $\mathrm{Spec}(A) = V(\{0\})$ and $\emptyset = V(A)$ are indeed of this form. Moreover, if $\{V(I_x)\}_{x\in\mathfrak{X}}$ is a family of such subsets, then

$$\bigcap_{x\in\mathfrak{X}} V(I_x) = V(< I_x >_{x\in\mathfrak{X}}).$$

Indeed if $\mathfrak{p}$ contains the ideal generated by the I_x, then $I_x \subset \mathfrak{p}$ for every $x \in \mathfrak{X}$. Conversely if $\mathfrak{p}$ is a prime ideal that contains the I_x, for every $x \in \mathfrak{X}$, then it contains the ideal they generate.

Finally, let us show that if I and J are two ideals of A, then

$$V(I) \cup V(J) = V(IJ).$$

$\boxed{\subset}$ If $\mathfrak{p}$ is a prime ideal that contains say I, then it contains $I \cap J$. Since we have $IJ \subset I \cap J$, we indeed have $\mathfrak{p} \in V(IJ)$.
$\boxed{\supset}$ Let $\mathfrak{p}$ be a prime ideal that contains IJ. If I is not contained in $\mathfrak{p}$, then taking an element $i \in I \setminus \mathfrak{p}$, we have $ij \in \mathfrak{p}$ for every $j \in J$. The ideal $\mathfrak{p}$ being prime we thus have $J \subset \mathfrak{p}$. □

Definition 6.5. *The topology defined by the closed sets $V(I)$ on* $\mathrm{Spec}(A)$ *is the Zariski topology. We say that a topological space $(X, \mathcal{T})$ is spectral if it is homeomorphic to the spectrum of a ring, endowed with the Zariski topology.*

The open sets for the Zariski topology on $\mathrm{Spec}(A)$ are thus of all the shape $\mathrm{Spec}(A) \setminus V(I)$, for an ideal $I \subset A$. If a is an element of A, we set

$$D(a) = \{\mathfrak{p} \in \mathrm{Spec}(A),\ a \notin \mathfrak{p}\} = \mathrm{Spec}(A) \setminus V(< a >).$$

The open sets of this form are called the *standard open sets*. The standard open sets form a base for the Zariski topology since we have the equality

$$V(I) = \bigcap_{i\in I} V(< i >),$$

for every ideal I of A.

Remark 6.6. *For the Zariski topology, $V(\mathfrak{p})$ is naturally the closure of the prime ideal $\mathfrak{p} \in \mathrm{Spec}(A)$.*

Example 6.7. *The Zariski topology on the spectrum* $\mathrm{Spec}(A \times B)$ *of a product of rings is the natural topology on the disjoint union of* $\mathrm{Spec}(A)$ *and* $\mathrm{Spec}(B)$.

Proposition 6.8. *For every ideal I of a ring A, we have*

$$V(I) = V(\sqrt{I}).$$

Proof. On the one hand the inclusion $I \subset \sqrt{I}$ implies that $V(\sqrt{I}) \subset V(I)$.

Conversely, let $\mathfrak{p}$ be a prime ideal that contains I. If $x \in \sqrt{I}$, then for some $n \in \mathbb{N}^*$, $x^n \in I \subset \mathfrak{p}$. In particular $x \in \mathfrak{p}$ since $\mathfrak{p}$ is prime and $\sqrt{I} \subset \mathfrak{p}$. □

6.1 Topological properties

The Zariski topology naturally appears to study algebraic sets, but it is in many respects far from the topologies you have encountered so far, notably metric spaces.

Proposition 6.9. *The spectrum of any ring A is quasi-compact.*

Proof. Let $(I_x)_{x\in\mathfrak{X}}$ be a family of ideals such that $\bigcap_{x\in\mathfrak{X}} V(I_x) = \emptyset$. Then by Lemma 6.3 and Proposition 6.4 we have

$$< (I_x)_{x\in\mathfrak{X}} >= A.$$

Thus there exists a finite family of indices $x_1, ..., x_n$ from $\mathfrak{X}$ and elements $i_1, ..., i_n$ from $I_{x_1}, ..., I_{x_n}$ such that $i_1+i_2+...+i_n = 1$. Then we have $\bigcap_{i=1}^{n} V(I_x) = V(A) = \emptyset$, which allows us to extract a finite subcovering from the open covering

$$\mathrm{Spec}(A) = \bigcup_{x\in\mathfrak{X}} \mathrm{Spec}(A) \setminus V(I_x).$$

□

Définition 0.1. A topological space $(X, \mathcal{T})$ is Noetherian if every descending chain of closed sets

$$X \supset F_1 \supset F_2 \supset F_3 \supset ...$$

is stationary.

Proposition 6.10. *Endowed with the Zariski topology, the spectrum of a Noetherian ring is a Noetherian space.*

Proof. The assignment $I \mapsto V(I)$ reverses the direction of inclusions. □

Example 6.11. *The converse to Proposition 6.10 is false, by considering*

$$A = \mathbb{C}[x_1, x_2, x_3, ...]/ < x_1^2, x_2^2, x_3^2, ... > .$$

We will indeed see later (Proposition 6.20) that here $\mathrm{Spec}(A)$ *is reduced to* 1 *point. However, A is not Noetherian since the chain of ideals*

$$< x_1 >\subset< x_1, x_2 >\subset< x_1, x_2, x_3 >\subset ...$$

is not stationary.

The following result shows that the Zariski topology on the spectrum of a ring is rarely metrizable.

Proposition 6.12. *Endowed with the Zariski topology,* $\mathrm{Spec}(A)$ *is Hausdorff if and only if every prime ideal of A is maximal.*

Proof. Assume that every prime ideal $\mathfrak{p}$ of A is maximal. If $\mathfrak{q}$ is another prime ideal of A, take an element $a \in \mathfrak{p}$ such that $a \notin \mathfrak{q}$. We will see in a TD exercise that then there exists an element $s \in A \setminus \mathfrak{p}$ and an integer $n \in \mathbb{N}^*$ such that $sa^n = 0$. Then we indeed have $\mathfrak{q} \in D(a)$, $\mathfrak{p} \in D(s)$, and

$$D(a) \cap D(s) = D(sa) = D(sa^n) = D(0) = \emptyset.$$

We indeed have $D(sa) = D(sa^n)$: if a prime ideal $\mathfrak{r}$ contains sa, it contains sa^n so $D(sa^n) \subset D(sa)$. Conversely if $\mathfrak{r}$ is a prime ideal that contains sa^n, then it contains s or a, so in both cases it contains sa and $D(sa) \subset D(sa^n)$. The spectral space $\mathrm{Spec}(A)$ is thus Hausdorff.

Conversely, assume that A contains a prime ideal $\mathfrak{p}$ that is not maximal, and denote $\mathfrak{m}$ a maximal ideal that contains it. If $U \subset \mathrm{Spec}(A)$ is an open set not containing $\mathfrak{p}$, then its complement U^c contains $\mathfrak{p}$, hence its closure $V(\mathfrak{p})$ which itself contains $\mathfrak{m}$. In particular $\mathfrak{m}$ is also not an element of U and $\mathrm{Spec}(A)$ is not Hausdorff. □

We recall that if A is a ring, an element $a \in A$ is an idempotent if it satisfies $a^2 = a$. The following definition allows us to characterize the connectedness of the topological space $\mathrm{Spec}(A)$ in terms of algebraic properties of A.

Definition 6.13. *A ring A is connected if the only idempotents of A are the trivial idempotents 0 and 1.*

Remark 6.14. *If a is an idempotent in A, $1 - a$ is also idempotent.*

Proposition 6.15. *A ring A is connected if and only if it is not isomorphic to the product $B \times C$ of two non-trivial rings.*

Proof. Seen in TD.

□

Theorem 6.16. *Let A be a ring. The following assertions are equivalent:*

1. *endowed with the Zariski topology,* $\mathrm{Spec}(A)$ *is connected;*
2. *A is connected*
3. *A does not decompose as a product $B \times C$ of non-trivial rings.*

Proof. Seen in TD. □

6.2 Spectra and quotients

The choice of prime ideals at the beginning of this course allows in particular to make the association $A \mapsto \mathrm{Spec}(A)$ functorial.

Proposition 6.17. *If $\varphi : A \longrightarrow B$ is a ring homomorphism, then the induced map $\varphi^\sharp : \mathrm{Spec}(B) \longrightarrow \mathrm{Spec}(A)$ given by $\varphi^\sharp(\mathfrak{p}) = \varphi^{-1}(\mathfrak{p})$ is continuous for the Zariski topology.*

Proof. The inverse image of a prime ideal remains a prime ideal, so the map $\varphi^\sharp$ is well-defined.

If I is an ideal of A, we have

$$\begin{aligned}(\varphi^\sharp)^{-1}(V(I)) &= \{\mathfrak{p} \in \mathrm{Spec}(B),\ \varphi^\sharp(\mathfrak{p}) \in V(I)\} \\ &= \{\mathfrak{p} \in \mathrm{Spec}(B),\ I \subset \varphi^{-1}(\mathfrak{p})\} \\ &= \{\mathfrak{p} \in \mathrm{Spec}(B),\ \varphi(I) \subset \mathfrak{p}\} \\ &= V(< \varphi(I) >)\end{aligned}$$

The inverse image of a closed set is thus closed and $\varphi^\sharp$ is continuous. □

Theorem 6.18. *If A is a ring and I an ideal of A, then $V(I)$ endowed with the topology induced by the Zariski topology on* $\mathrm{Spec}(A)$ *is a spectral space, homeomorphic to* $\mathrm{Spec}(A/I)$.

Proof. Denoting $\pi : A \longrightarrow A/I$ the canonical projection, Lemma 1.13 (2) ensures that the maps $\mathfrak{p} \mapsto \pi(\mathfrak{p})$ and $\pi^\sharp$ are mutually inverse bijections, continuous by Proposition 6.17. □

Remark 6.19. *We will show later that the standard open sets $D(a)$ of* $\mathrm{Spec}(A)$ *are also spectral spaces.*

We deduce that the Zariski topology does not "see" nilpotent elements... We will not address this subject in more detail in the course, to learn more you will need to continue studying algebraic geometry.

Corollary 6.20. *If A is a ring, then* $\mathrm{Spec}(A)$ *and* $\mathrm{Spec}(A/\sqrt{0})$ *are homeomorphic.*

Proof. As seen in the first part of the course, the nilradical $\sqrt{0}$ of A is the intersection of all its prime ideals. Every prime ideal $\mathfrak{p}$ contains $\sqrt{0}$ and the map induced by the quotient $A \longrightarrow A/\sqrt{0}$ is a homeomorphism. □

Exercise 6.21. *Let k be a field. Consider the algebra of dual numbers*

$$k[\varepsilon] := \{a + b\varepsilon,\ (a, b) \in k^2\}$$

obtained by adjoining the element ε subject to the relation $\varepsilon^2 = 0$.

1. *Give the ring structure of $k[\varepsilon]$. Is it a field?*

2. *Determine the units of $k[\varepsilon]$.*

3. *Describe* $\mathrm{Spec}(k[\varepsilon])$ *and its Zariski topology.*

6.3 Irreducible spectra, components

Definition 6.22. *A topological space $(X, \mathcal{T})$ is irreducible if X cannot be decomposed into a union of two proper non-empty closed sets.*

An irreducible topological space is necessarily connected since the union in definition 6.22 is not disjoint.

Définition 0.2. An irreducible component of a topological space X is an irreducible closed set (for the induced topology) that is maximal for inclusion.

Proposition 6.23. *Every topological space is covered by its irreducible components.*

Proof. For $x \in X$, apply Zorn's lemma to the set $\mathfrak{I}_x$ of irreducible subsets (for the induced topology) of X that contain x. On the one hand $\mathfrak{I}_x$ contains the singleton $\{x\}$, so it is non-empty. Let $(X_j)_{j\in J}$ be a totally ordered family in $\mathfrak{I}_x$; set

$$X' = \bigcup_{j\in J} X_j.$$

Let $X' = Y \cup Z$ be a decomposition of X' into two closed sets. Fixing an element $j_0 \in J$, we have either $X_{j_0} \subset Y$, or $X_{j_0} \subset Z$ because X_{j_0} is irreducible. Then since all X_j satisfy this property, if we have say $X_{j_0} \subset Y$, then $X_j \in Y$ for all $j \in J$ because the family $(X_j)_{j\in J}$ is totally ordered and all its elements intersect Y. So $X' = Y$ and the space X' is irreducible. The family $\mathfrak{I}_x$ thus contains a maximal element and x is contained in an irreducible component. □

Lemma 6.24. *Let X be a topological space.*

1. *If Y is an irreducible subset of X, its closure is irreducible.*

2. *The irreducible components of X are closed.*

3. *If X is irreducible, every non-empty open subset of X is dense.*

Proof. 1. Consider a decomposition $\overline{Y} = Y_1 \cup Y_2$ of the closure of Y into two closed sets. We have $Y = (Y \cap Y_1) \cup (Y \cap Y_2)$ so by irreducibility, say $Y = Y \cap Y_1$, and thus $\overline{Y} = \overline{Y \cap Y_1} \subset Y_1$.

2. Immediate from 1. by maximality.

3. Let O be a non-empty and non-dense open subset of X, the complement O' of its closure is a non-empty open set, because $\overline{O} \neq X$. We then see that $O \cap O' = \emptyset$, i.e., $O^c \cup O'^c = X$, which contradicts the irreducibility of X.

□

Proposition 6.25. *Let A be a ring and I an ideal of A.*

1. *The closed points of* $\mathrm{Spec}(A)$ *correspond to maximal ideals.*

2. *$V(I) \subset \mathrm{Spec}(A)$ is irreducible if and only if I is prime.*

Proof. 1. The closure of a prime ideal $\mathfrak{p} \in \mathrm{Spec}(A)$ is $V(\mathfrak{p})$. It is thus clear that $\mathfrak{p}$ is a closed point if and only if $V(\mathfrak{p}) = \{\mathfrak{p}\}$, i.e., if the ideal $\mathfrak{p}$ is maximal.

2. If $\mathfrak{p}$ is a prime ideal, we have $V(\mathfrak{p}) = \overline{\{\mathfrak{p}\}}$ irreducible, by Lemma 6.24. Now consider $V(I)$ irreducible. By virtue of Proposition 6.8, we may assume that I is radical (i.e., $\sqrt{I} = I$).

   Suppose that I is not prime and take a, b in A not belonging to I, but such that $ab \in I$. Then

$$V(I) = V(< I, a >) \cup V(< I, b >)$$

   (if $\mathfrak{p}$ contains I, it then contains ab, so either a or b).

   Moreover we have $V(< I, a >) \subsetneq V(I)$, because otherwise a belongs to every prime ideal containing I and a is an element of

$$\bigcap_{I \subset \mathfrak{p}} \mathfrak{p} = \sqrt{I} = I,$$

   which contradicts the irreducibility of $V(I)$. The ideal I is thus prime.

□

We can thus obtain a purely algebraic characterization of irreducible components for the Zariski topology.

Theorem 6.26. *Every irreducible closed set of* $\mathrm{Spec}(A)$ *is the closure of a unique prime ideal $\mathfrak{p}$ of A. We thus obtain a bijection*

$$\{\textit{prime ideals of } A\} \simeq \{\textit{irreducible closed sets of } \mathrm{Spec}(A)\}.$$

The irreducible components of $\mathrm{Spec}(A)$ *are of the form $V(\mathfrak{p})$, where $\mathfrak{p}$ is a minimal prime ideal of A.*

Proof. By Proposition 6.25, every irreducible closed set of $\mathrm{Spec}(A)$ is of the form $\overline{\{\mathfrak{p}\}} = V(\mathfrak{p})$, where $\mathfrak{p}$ is a prime ideal. The uniqueness of $\mathfrak{p}$ is clear since $V(\mathfrak{p}) = V(\mathfrak{q})$ implies $\mathfrak{p} = \mathfrak{q}$ (both are prime).

The obtained bijection is decreasing, so the irreducible components of $\mathrm{Spec}(A)$ correspond to the minimal prime ideals of A. □

Corollary 6.27. *The spectrum* $\mathrm{Spec}(A)$ *of a ring* A *is irreducible if and only if the nilradical of* A *is a prime ideal.*

Proof. By virtue of Theorem 6.26, $\mathrm{Spec}(A)$ is irreducible if and only if it has a unique minimal prime ideal. The equality

$$\bigcap_{\mathfrak{p}\in\mathrm{Spec}(A)} \mathfrak{p} = \sqrt{0}$$

indicates that this situation corresponds to the case where the nilradical of A is prime. □

7 Localization

The field of rational numbers is formally constructed from $\mathbb{Z}$, by inverting all non-zero integers. The construction you know generalizes to any integral domain A and leads to its *fraction field*.

The generalization of this process for arbitrary rings is *localization*. In this part we define the localizations of a ring with respect to a multiplicative subset. This description allows us to show that, endowed with the Zariski topology, the standard open sets are spectral spaces.

7.1 Definition and universal property

Definition 7.1. *A subset* S *of a ring* A *is a multiplicative subset if* S *is stable under multiplication, contains* 1 *but does not contain* 0.

Example 7.2.

1. *The set* $A^\times$ *of invertible elements of* A *is a multiplicative subset (which turns out to be uninteresting for localization).*
2. *If* $a \in A$ *is not nilpotent, the subset* $S_a = \{1, a, a^2, ...\}$ *of powers of* a *is a multiplicative subset.*

If A is a ring and S is a multiplicative subset of A, we want to mimic the construction of the fraction field. We would thus like to consider the set $S^{-1}A$ of "fractions" $\frac{a}{s} = (a, s) \in A \times S$ with denominator in S, endowed with the usual addition and multiplication, such that $(a, s) = (b, t)$ whenever $at = bs$.

However, note that we must be careful: if s and a are elements of S and A respectively such that $sa = 0$, then we want a to be zero in any ring where s is invertible, i.e.,

$$(a, 1) = (0, 1)$$

without necessarily having $a = 0$, which is immediate with the classical fraction relation. To avoid this pitfall, we thus define $S^{-1}A$, the localization of A by S, by setting $S^{-1}A = A \times S$, with the usual additions and multiplications, but modulo the relation

$$(a, s) \sim (b, t) \Leftrightarrow \text{there exists } x \in S \text{ such that } x(at - bs) = 0.$$

Lemma 7.3. *The relation $\sim$ above on $A \times S$ is an equivalence relation.*

Proof. The relation is clearly reflexive and symmetric. If we have

$$(a, s) \sim (b, t) \sim (c, u),$$

with thus x and y in A such that $x(at - bs) = 0 = y(bu - ct)$, then by focusing on the element b and saturating with elements of S, we see that

$$bsxyu = atxyu \text{ and } bsxyu = ctysx,$$

so we indeed have $txy(au - sc) = 0$, with $txy \in S$ since the latter is multiplicative. □

Definition 7.4. *The quotient set of $A \times S$ by the above equivalence relation is denoted $S^{-1}A$, and called the localization of A at the multiplicative subset S.*

For every $(a, s) \in A \times S$, we denote in the sequel $[a, s]$ the equivalence class in $S^{-1}A$. We may also write these classes as fractions, which is sometimes practical for computations.

Proposition 7.5. *Endowed with the laws*

$$[a, s] \cdot [b, t] = [ab, st] \text{ and } [a, s] + [b, t] = [at + bs, st]$$

the set $S^{-1}A$ is endowed with a ring structure. The map

$$\begin{array}{rccc} \iota : & A & \longrightarrow & S^{-1}A \\ & a & \longmapsto & [a, 1] \end{array}$$

is a ring homomorphism.

Proof. We must verify that these laws are well-defined. If we have $[a, s] = [a', s']$, i.e., $x(as' - a's) = 0$ for some $x \in S$, then we have

$$abs'tx = a'bstx$$

and thus $[a'b, s't] = [ab, st]$. Moreover the equality

$$(at + bs)s'x = ats'x + bss'x = ta'sx + bss'x = (at' + bs')sx$$

indicates that $(at + bs)s'tx = (a't + bs')stx$, i.e.,

$$[at + bs, st] = [a't + bs', s't].$$

The same reasoning by choosing another representative for $[b, t]$ shows that these operations are well-defined. In the same way as for the construction of $\mathbb{Q}$ or fraction fields, we easily see that endowed with these laws, $S^{-1}A$ is a ring, whose 0 is the class $[0, 1]$ and whose unit is the class $[1, 1]$. The map ι is thus naturally a ring homomorphism. □

Remark 7.6. *The ring $S^{-1}A$ cannot be the zero ring under our hypotheses, because $[1, 1] \neq 0$ (otherwise 0 would belong to S).*

Lemma 7.7. *Let A be a ring and S a multiplicative subset of A. Then*

$$\ker(\iota) = \{a \in A,\ \exists s \in S, sa = 0\}.$$

In particular if A is an integral domain, the homomorphism ι is injective.

Proof. We have that $a \in \ker(\iota)$ if and only if $[a, 1] = [0, 1]$, i.e., there exists an element $s \in S$ such that $sa = 0$. When A is an integral domain, knowing that S does not contain 0, we obtain that a is zero. □

Examples 7.8. *1. If $A = \mathbb{Z}$ and $S = A^*$, we obtain $S^{-1}A = \mathbb{Q}$.*

2. *If the chosen multiplicative subset of A is the set $S = A^\times$ of units of A, the map*

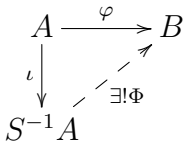
$$\iota : A \longrightarrow S^{-1}A$$

is a ring isomorphism.

3. *an example $\mathbb{Z}$ localized at a prime number.*

4. *If k is a field, then $A = k[X]$ is an integral domain and setting $S = k[X]^*$, we obtain for $S^{-1}A$ the field $k(X)$ of rational functions.*

Theorem 7.9 (Universal property of localization)**.** *Let $\varphi : A \longrightarrow B$ be a ring homomorphism and $S \subset A$ a multiplicative subset. If $\varphi(s)$ is invertible for every $s \in S$, then there exists a unique ring homomorphism $\Phi : S^{-1}A \longrightarrow B$ such that $\Phi \circ \iota = \varphi$, i.e., which completes the diagram*



Proof. (Uniqueness) If such a Φ exists then for $a \in A$, we have $\varphi(a) = \Phi([a, 1])$. In particular for every $(a, s) \in A \times S$ we have

$$\varphi(a) = \Phi([a, 1]) = \Phi([s, 1])\Phi([a, s]) = \varphi(s)\Phi([a, s])$$

and $\varphi(s)$ being invertible the element $\Phi([a, s]) = \varphi(a)\varphi(s)^{-1}$ is uniquely determined.

(Existence) We show that the formula

$$\Phi([a, s]) = \varphi(a)\varphi(s)^{-1}$$

indeed defines a ring homomorphism $\Phi : S^{-1}A \longrightarrow B$. Suppose that $[a, s] = [b, t]$, i.e., there exists $x \in S$ such that $x(at - bs) = 0$. Then we have

$$\varphi(x)\varphi(a)\varphi(t) = \varphi(x)\varphi(b)\varphi(s),$$

so $\varphi(a)\varphi(s)^{-1} = \varphi(b)\varphi(t)^{-1}$. The fact that this defines a ring homomorphism follows directly from the properties of φ. □

The denomination "universal property" comes from the fact that this property characterizes the ring $S^{-1}A$ as the solution of a universal problem.

Corollary 7.10. *Let $S \subset A$ be a multiplicative subset of a ring A and a ring homomorphism $\tilde{\iota} : A \longrightarrow \tilde{A}$ such that for every $s \in S$, $\tilde{\iota}(s)$ is invertible, and satisfying the previous universal property. Then there exists a unique ring homomorphism*

$$\Phi : S^{-1}A \longrightarrow \tilde{A}$$

such that $\Phi \circ \iota = \iota'$, and Φ is an isomorphism.

Proof. By Theorem 7.9 for $\varphi = \tilde{\iota}$ and $B = \tilde{A}$, we obtain a unique homomorphism $\Phi : S^{-1}A \longrightarrow \tilde{A}$ such that $\tilde{\iota} = \Phi \circ \iota$ (universal property of $S^{-1}A$).

Similarly by hypothesis, $\tilde{A}$ satisfying the universal property, there exists a homomorphism $\Psi : \tilde{A} \longrightarrow S^{-1}(A)$ such that $\iota = \Psi \circ \tilde{\iota}$. The (trivial) diagram

$$\begin{array}{ccc} A & \xrightarrow{\iota} & S^{-1}A \\ {\scriptstyle \iota}\downarrow & & \\ S^{-1}A & & \end{array}$$

is obviously completed by the identity map $S^{-1}A \longrightarrow S^{-1}A$, but also by $\Psi \circ \Phi$, since

$$\Psi \circ \Phi \circ \iota = \Psi \circ \tilde{\iota} = \iota.$$

The uniqueness for the universal property of $S^{-1}A$ thus indicates that $\Psi \circ \Phi = \mathrm{id}_{S^{-1}A}$.

The same reasoning by replacing $S^{-1}A$ by $\tilde{A}$, ι by $\tilde{\iota}$ and invoking the universal property of $\tilde{A}$ shows that $\Phi \circ \Psi = \mathrm{id}_{\tilde{A}}$. □

The uniqueness in the universal property of Theorem 7.9 plays a decisive role in the last proof. Without imposing this uniqueness, the localization $S^{-1}A$ is no longer characterized by this property.

7.2 Ideals and prime ideals of localizations

Let A be a ring and $S \subset A$ a multiplicative subset. If I is an ideal of A, we denote

$$S^{-1}I = \{[a, s] \in S^{-1}A,\ a \in I\}.$$

This is certainly an ideal of $S^{-1}A$. The following theorem indicates that all ideals of $S^{-1}A$ are of this form, and even more so if they are prime.

Proposition 7.11. *Let A be a ring and $S \subset A$ a multiplicative subset. We denote $\iota : A \longrightarrow S^{-1}A$ the natural homomorphism above.*

1. *Every ideal I of $S^{-1}A$ is equal to $S^{-1}J$, where $J = \iota^{-1}(I)$.*
2. *The set of prime ideals of $S^{-1}A$ is in bijection with the prime ideals of A that do not meet S, via*

$$\begin{array}{ccc} \mathrm{Spec}(S^{-1}A) & \longleftrightarrow & \left\{ \begin{array}{c} \text{prime ideals of } A \\ \text{not meeting } S \end{array} \right\} \\ I & \longmapsto & \iota^{-1}(I) \\ S^{-1}J & \longleftarrow\!\shortmid & J \end{array}$$

Proof. 1. Being the inverse image of I under the homomorphism ι, J is an ideal. If $[a, s]$ is an element of I, then

$$[a, 1] = [s, 1] \cdot [a, s]$$

is also in it, so $a \in J$ and $I \subset S^{-1}J$.

Conversely by definition of J we have $\iota(j) = [j, 1] \in I$ for every $j \in J$, so for every $(j, s) \in J \times S$ we have $[j, s] = [j, 1] \cdot [1, s]$ in I, i.e., $S^{-1}J = I$.

2. Let $I \in \mathrm{Spec}(S^{-1}A)$ a prime ideal. On the one hand the inverse image $\iota^{-1}(I)$ is a prime ideal of A. Moreover if $s \in \iota^{-1}(I) \cap S$, then

$$[1, s] \cdot \iota(s) = [1, 1]$$

is an element of I and $I = S^{-1}A$, which contradicts the fact that it is prime. The ideal $\iota^{-1}(I)$ thus does not meet S.

Conversely, let $J \in A$ a prime ideal with empty intersection with S. Let us show that the ideal $S^{-1}J$ is prime: on the one hand it is a proper ideal because if $a \in A \setminus J$, then $[a, 1] \in S^{-1}J$ implies that there exists an element $j \in J$ such that $[a, 1] = [j, s]$, i.e., an element $t \in S$ such that $t(as - j) = 0$. But this is not possible, because then we would have $tsa = tj \in J$, and since J is prime and $J \cap S = \emptyset$, $a \in J$.

If the product of two elements

$$[a, s] \cdot [b, t] = [ab, st]$$

belongs to $S^{-1}J$, then $[ab, 1] = [st, 1] \cdot [ab, st]$ similarly. So we have two elements $j \in J$ and $u \in S$ such that

$$[ab, 1] = [j, u],$$

i.e., an $x \in S$ such that $x(abu - j) = 0$. The element $(ab)(ux)$ thus belongs to J but the latter is prime and does not meet S, so $ux \notin J$ and finally $ab \in J$. Invoking again the fact that J is prime, we have either $a \in J$, or $b \in J$, i.e., $[a, s] \in S^{-1}J$ or $[b, t] \in S^{-1}J$. The ideal $S^{-1}J \subset S^{-1}A$ is prime and the second map is well-defined. The sets $\mathrm{Spec}(S^{-1}A)$ and of prime ideals of $\mathrm{Spec}(A)$ not meeting S are thus in bijection.

□

Corollary 7.12. *If A is a Noetherian ring and $S \subset A$ is a multiplicative subset, then $S^{-1}A$ is also Noetherian.*

Proof. Let

$$\mathcal{C} = I_1 \subset I_2 \subset ...$$

be an increasing sequence of ideals of $S^{-1}A$. Theorem 7.11 indicates that $I_k = S^{-1}J_k$, where $J_k = \{a \in A, \iota(a) \in I_k\}$. These ideals of A are also nested: $\mathcal{C}$ thus gives rise to a chain of ideals $J_1 \subset J_2 \subset ...$ of A, stationary because the latter is Noetherian. The same holds for $\mathcal{C}$. □

Corollary 7.13. *Let A be a ring and $S \subset A$ a multiplicative subset. The subset $U_S \subset \mathrm{Spec}(A)$ of prime ideals of A not meeting S is spectral for the topology induced by the Zariski topology.*

Proof. We show that U_S is homeomorphic to $\mathrm{Spec}(S^{-1}A)$, endowed with the Zariski topology. Proposition 7.11 indicates that U_S and $\mathrm{Spec}(S^{-1}A)$ are in bijection, via $I \mapsto \iota^{-1}(I)$. This map is continuous because it preserves inclusions and the inverse image of $V(\mathfrak{p}) \cap U_S \subset U_S$ on the set of prime ideals of $S^{-1}A$ that contain $S^{-1}\mathfrak{p}$, i.e., $V(S^{-1}\mathfrak{p})$.

Similarly for the inverse map $J \longrightarrow S^{-1}J$: the inverse image of the closed set $V(\mathfrak{p}')$ of $\mathrm{Spec}(S^{-1}A)$ is $V(\iota^{-1}(\mathfrak{p}')) \cap U_S$, a closed set of U_S. The bijection of the theorem is thus a homeomorphism. □

Corollary 7.14. *Every standard open set $D(a) \subset \mathrm{Spec}(A)$ (with a non-nilpotent) is a spectral topological space, for the topology induced by the Zariski topology.*

Proof. The subset $S_a = \{1, a, a^2, ...\}$ is a multiplicative subset of A. The standard open set $D(a)$ corresponds to the prime ideals of $\mathrm{Spec}(A)$ that do not contain a, i.e., to the set U_{S_a} of prime ideals that do not meet S_a. Indeed if $\mathfrak{p} \in U_{S_a}$, then a does not belong to $\mathfrak{p}$ and conversely if $\mathfrak{p} \in D(a)$, $a \notin \mathfrak{p}$ and the same holds for any power of a. The ideal $\mathfrak{p}$ not containing 1 either, $\mathfrak{p} \in U_{S_a}$. By virtue of Corollary 7.13, $D(a)$ is homeomorphic to $\mathrm{Spec}(S_a^{-1}A)$. □

7.3 Two fundamental examples

Fraction field

You have seen in the first part of the course (and in L3) the very classical construction of the *fraction field* of an integral domain. This corresponds to a special case of localization: indeed if A is an integral domain, $S = A \setminus \{0\}$ is a multiplicative subset. The localization $S^{-1}A$ is naturally a field containing A: the map ι is injective and we always have $[a, s]^{-1} = [s, a]$. We denote $\mathrm{Frac}(A) := S^{-1}A$ this field called the *fraction field of A*.

Theorem 7.15. *If A is an integral domain, every ring homomorphism $\varphi : A \longrightarrow B$ such that $\varphi(a)$ is invertible for every nonzero $a \in A$ extends to a unique injective homomorphism $\Phi : \mathrm{Frac}(A) \longrightarrow B$.*

Proof. By the universal property of localization, the hypotheses imply that φ extends uniquely to a homomorphism

$$\Phi : \mathrm{Frac}(A) \longrightarrow B$$

given by $\Phi([a, s]) = \varphi(a)\varphi(s)^{-1}$, for every s nonzero. This homomorphism is clearly injective, because the ideal $\ker(\Phi)$ is reduced to 0. □

Corollary 7.16. *If A is an integral domain and K is a field containing A, then K contains a subfield isomorphic to* Frac(A).

Localization at a prime ideal

Definition 7.17. *A ring A is said to be local if it has a unique maximal ideal $\mathfrak{m}$. The quotient $A/\mathfrak{m}$ is called the residue field of A.*

The following characterization is convenient and even allows to generalize local rings without difficulty to the non-commutative setting.

Lemma 7.18. *A ring A is local if and only if the set of non-invertible elements of A is an ideal.*

Proof. If the set of non-invertible elements of A is an ideal, it is necessarily the unique maximal ideal of A. Conversely if A has a unique maximal ideal $\mathfrak{m}$, the latter corresponds to the non-invertible elements because if $a \in A$ is not invertible, we have $< a > \subset \mathfrak{m}$ by Krull's theorem. □

If A is a ring and $\mathfrak{p} \in \mathrm{Spec}(A)$ is a prime ideal, the subset $S_\mathfrak{p} = A \setminus \mathfrak{p}$ is a multiplicative subset of A. The localization $S_\mathfrak{p}A$ is denoted $A_\mathfrak{p}$ and is called the localization of A at $\mathfrak{p}$.

Proposition 7.19. *If A is a ring and $\mathfrak{p}$ a prime ideal of A, the ring $A_\mathfrak{p}$ is a local ring.*

Proof. By virtue of Theorem 7.11 the prime ideals of $A_\mathfrak{p}$ are the $S_\mathfrak{p}^{-1}\mathfrak{q}$, where $\mathfrak{q}$ is a prime ideal of A that does not meet $A \setminus \mathfrak{p}$, i.e., contained in $\mathfrak{p}$. All prime ideals of $A_\mathfrak{p}$ are thus contained in $S_\mathfrak{p}^{-1}\mathfrak{p}$, which is the unique maximal ideal. □

To every ring A and every prime ideal $\mathfrak{p} \in \mathrm{Spec}(A)$ we can thus associate the local ring $A_\mathfrak{p}$. This ring and its residue field $\kappa(\mathfrak{p})$, the *residue field of A at $\mathfrak{p}$*, will be essential if you continue next year the study of algebraic geometry.

8 Tensor product

As seen previously, the spectrum of the direct product $A \times B$ of two rings is not a very interesting object, it is simply given by the disjoint union of $\mathrm{Spec}(A)$ and $\mathrm{Spec}(B)$, and the Zariski topology turns out to be the disjoint topology.

Given two A-modules M and N, we now introduce another "product": their tensor product $M \otimes_A N$. The tensor product of M and N aims to provide a module generated by formal products of elements of M and N, the pure tensors, which we denote $m \otimes n$. We thus obtain a very versatile and useful object, associated with the following two classical problems:

1. (extension of scalars) Let V be an $\mathbb{R}$-vector space with basis $(e_i)_{i\in\mathcal{I}}$. How to construct the *complexification* of V, i.e., the "$\mathbb{C}$-vector space generated by the family $(e_i)_{i\in\mathcal{I}}$"? This situation can be studied by hand in a basis, but is resolved more conceptually by the tensor product $V \otimes_{\mathbb{R}} \mathbb{C}$, which applies in a much more general setting than $\mathbb{R}$ and $\mathbb{C}$.

2. (product of varieties) We would like to construct a notion of "product" for algebraic varieties, which corresponds to the product of algebraic sets. The problem already arises for the simplest case: the tensor product $\mathbb{C}[X]\otimes_{\mathbb{C}}\mathbb{C}[Y]$ should correspond to the polynomial ring $\mathbb{C}[X,Y]$. Not every element of $\mathbb{C}[X,Y]$ is the product of two polynomials from $\mathbb{C}[X]$ and $\mathbb{C}[Y]$, but the latter still has a basis formed by the monomials $(X^iY^j)_{(i,j)\in\mathbb{N}^2}$, which will correspond to the pure tensors $(X^i \otimes Y^j)_{(i,j)\in\mathbb{N}^2}$.

8.1 Definition and universal property

Let A be a ring and M, N, P be A-modules.

Definition 8.1. *A map $\varphi : M \times N \longrightarrow P$ is A-bilinear if for all elements a, a' of A, m, m' of M and n, n' of N we have*

$$\varphi(am + a'm', n) = a\varphi(m, n) + a'\varphi(m', n)$$
$$\varphi(m, an + a'n') = a\varphi(m, n) + a'\varphi(m, n').$$

If P is an A-module and X is a set, the set $\mathrm{Hom}_{\mathrm{Set}}(X, P)$ of set maps from X to P is naturally endowed with an A-module structure, via the laws

$$(\varphi + \psi)(x) = \varphi(x) + \psi(x) \text{ and } (a \cdot \varphi)(x) = a\varphi(x).$$

The same holds for A-module homomorphisms, which we denote Hom_A.

Lemma 8.2. *The set $\mathrm{Bil}_A(M \times N, P)$ of maps $M \times N \longrightarrow P$ that are A-bilinear is an A-submodule of $\mathrm{Hom}_{\mathrm{Set}}(M, N)$.*

Proof. If $b \in A$ and $\varphi : M \times N \longrightarrow P$, $\psi : M \times N \longrightarrow P$ are two A-bilinear maps, we show that $b\varphi + \psi$ is A-bilinear.

Indeed if $(a, a') \in A^2$, $(m, m') \in M^2$ and $(n, n') \in N^2$, we immediately have

$$(b\varphi + \psi)(am + a'm', n) = a(b\varphi + \psi)(m, n) + a'(b\varphi + \psi)(m', n)$$
$$(b\varphi + \psi)(m, an + a'n') = a(b\varphi + \psi)(m, n) + a'(b\varphi + \psi)(m, n').$$

□

We will now construct the module that satisfies the desired properties above, and show that it is the solution of a universal problem. Denote $A^{(M\times N)}$ the free A-module associated to the set $M \times N$. The elements of $A^{(M\times N)}$ are the linear combinations

$$\sum_{(m,n)\in M\times N} a_{m,n}\delta_{m,n},$$

i.e., linear combinations in the elements $(\delta_{m,n})_{(m,n)\in M\times N}$, with coefficients $(a_{m,n})_{(m,n)\in M\times N}$ in A (so these are finite sums).

The free module $A^{(M\times N)}$ describes pointwise the A-module homomorphisms $M \times N \longrightarrow A$. To force bilinearity, we consider the ideal $I \subset A^{(M\times N)}$ generated by elements of the form

$$\delta_{am+m',n} - a\delta_{m,n} - \delta_{m',n} \tag{8.1}$$
$$\delta_{m,an+n'} - a\delta_{m,n} - \delta_{m,n'} \tag{8.2}$$

with a belonging to A, m, m' to M and n, n' to N.

Definition 8.3. *We denote $M \otimes_A N = A^{(M\times N)}/I$ the associated quotient A-module, and $m \otimes n$ the class of $\delta_{m,n}$ in $M \otimes_A N$.*

By definition of $M \otimes_A N$, we have the relations

$$(am) \otimes n = a(m \otimes n) = m \otimes (an) \tag{8.3}$$

and every element of $M \otimes_A N$ is a finite sum of elements of the form $m \otimes n$.

Remark 8.4. *The elements of $M \otimes_A N$ of the form $m \otimes n$ are the pure tensors of $M \otimes_A N$. They generate $M \otimes_A N$, but not all elements of $M \otimes_A N$ are pure tensors.*

Proposition 8.5. *If two A-modules M and N are respectively generated by $(e_i)_{i\in I}$ and $(f_j)_{j\in J}$, then their tensor product $M \otimes_A N$ is generated by the pure tensors $(e_i \otimes f_j)_{(i,j)\in I\times J}$.*

Proof. If $m \otimes n \in M \otimes_A N$ is a pure tensor, then decomposing $m = \sum_{k=1}^{s} m_{i_k} e_{i_k}$ and $n = \sum_{l=1}^{t} n_{j_l} f_{j_l}$, we obtain

$$m \otimes n = \sum_{k=1}^{s}\sum_{l=1}^{t} m_{i_k} n_{j_l} (e_{i_k} \otimes f_{j_l})$$

Every element of $M \otimes_A N$ is a finite sum of pure tensors, and thus the family $(e_i \otimes f_j)_{(i,j)\in I\times J}$ generates $M \otimes_A N$. □

Remark 8.6. *In particular, if M and N are finitely generated A-modules, the same holds for their tensor product.*

Theorem 8.7 (Universal property of the tensor product)**.** *Let A be a ring and M, N be A-modules. For every A-module P we have a bijection*

$$\begin{array}{ccc} \mathrm{Hom}_A(M \otimes_A N, P) & \xleftrightarrow{\sim} & \mathrm{Bil}_A(M \times N, P) \\ \varphi & \longmapsto & \Psi(\varphi) : (m,n) \mapsto \varphi(m \otimes n) \\ \Phi(\psi) & \longmapsfrom & \psi \end{array}$$

where $\Phi(\psi) : M \otimes_A N \longrightarrow P$ is the A-module homomorphism given on pure tensors by $\Phi(\psi)(m \otimes n) = \psi(m,n)$.

Proof. The first map is well-defined: given a map $\varphi \in \mathrm{Hom}_A(M \otimes_A N, P)$, the relations (8.3) ensure that $\Psi(\varphi)$ is A-bilinear.

Let us show that the map Φ is well-defined. If $\psi \in \mathrm{Bil}_A(M \times N, P)$, consider the A-module homomorphism $\tilde{\psi} : A^{(M \times N)} \longrightarrow P$ defined by the images $\tilde{\psi}(\delta_{m,n}) = \psi(m,n)$. The map $\tilde{\psi}$ being bilinear, $\tilde{\psi}$ vanishes on the generators of $I \subset A^{(M \times N)}$ (8.1):

$$\tilde{\psi}(\delta_{am+m',n} - a\delta_{m,n} - \delta_{m',n}) = \psi(am + m', n) - a\psi(m,n) - \psi(m',n) = 0.$$
$$\tilde{\psi}(\delta_{m,an+n'} - a\delta_{m,n} - \delta_{m,n'}) = \psi(m, an + n') - a\psi(m,n) - \psi(m,n') = 0.$$

The map $\tilde{\psi}$ thus passes to the quotient and there exists a homomorphism

$$\Phi(\psi) : M \otimes_A N \longrightarrow P$$

given on pure tensors by $\Phi(\psi)(m \otimes n) = \tilde{\psi}(\delta_{m,n}) = \psi(m,n)$.

Let $\varphi \in \mathrm{Hom}_A(M \otimes_A N, P)$ and $\psi \in \mathrm{Bil}_A(M \times N, P)$.
For every $(m,n) \in M \times N$ we have

$$\Phi \circ \Psi(\varphi)(m \otimes n) = \Psi(\varphi)(m,n) = \varphi(m \otimes n)$$

and similarly

$$\Psi \circ \Phi(\psi)(m,n) = \Phi(\psi)(m \otimes n) = \psi(m,n)$$

and Φ, Ψ are mutual inverses. □

8.2 Properties of the tensor product

The universal property of the tensor product is the usual tool to study homomorphisms $M \otimes_A N \longrightarrow P$ from A-bilinear maps $M \times N \longrightarrow P$. It is thus constantly used, especially when identifying the tensor product of two modules.

Proposition 8.8 (Associativity and commutativity)**.** *Let A be a ring and M, N, P be A-modules. We have isomorphisms of A-modules*

$$M \otimes_A N \simeq N \otimes_A M \tag{8.4}$$
$$(M \otimes_A N) \otimes_A P \simeq M \otimes_A (N \otimes_A P) \tag{8.5}$$

Proof. (8.4) The A-bilinear map

$$\begin{array}{ccc} M \times N & \longrightarrow & N \otimes_A M \\ (m,n) & \longmapsto & n \otimes m \end{array}$$

induces by the universal property of the tensor product an A-module homomorphism $\varphi_1 : M \otimes_A N \longrightarrow N \otimes_A M$ given on pure tensors by $\varphi(m \otimes n) = n \otimes m$. The same reasoning by swapping the roles of M and N gives a homomorphism $\varphi_2 : N \otimes_A M \longrightarrow M \otimes_A N$ given by $n \otimes m \mapsto m \otimes n$, which is the inverse of φ_1.

(8.5) Fixing an element p of P, the map

$$\begin{array}{ccc} M \times N & \longrightarrow & M \otimes_A (N \otimes_A P) \\ (m,n) & \longmapsto & m \otimes (n \otimes p) \end{array}$$

is A-bilinear, and thus induces $\varphi_p : M \otimes_A N \longrightarrow M \otimes_A (N \otimes_A P)$ given by $\varphi_p(m \otimes n) = m \otimes (n \otimes p)$.

We thus obtain in particular an A-bilinear map

$$\varphi : (M \otimes_A N) \times P \longrightarrow M \otimes_A (N \otimes_A P)$$

by setting $(m \otimes n, p) \mapsto \varphi_p(m \otimes n) = m \otimes (n \otimes p)$, which itself gives by the universal property the A-module homomorphism

$$f : (M \otimes_A N) \otimes_A P \longrightarrow M \otimes_A (N \otimes_A P)$$

given by $f((m \otimes n) \otimes p) = m \otimes (n \otimes p)$. The inverse of f is constructed in the same way, by constructing via the universal property the homomorphism

$$g : M \otimes_A (N \otimes_A P) \longrightarrow (M \otimes_A N) \otimes_A P$$

given by $g(m \otimes (n \otimes p)) = (m \otimes n) \otimes p$. □

Proposition 8.9. *If M is an A-module, we have $M \simeq A \otimes_A M$.*

Proof. Consider the A-module homomorphism $f : A \otimes_A M \longrightarrow M$ given by $f(a \otimes m) = am$, induced by the universal property from the A-bilinear map

$$\begin{array}{ccc} A \times M & \longrightarrow & M \\ (a,m) & \longmapsto & am \end{array}.$$

The map $g : M \longrightarrow A \otimes_A M$ given by $g(m) = 1 \otimes m$ is also an A-module homomorphism and the inverse of f, since $f(g(m)) = f(1 \otimes m) = m$ and $g(f(a \otimes m)) = g(am) = 1 \otimes am = a \otimes m$. □

Remark 8.10. *by replacing bilinear maps by multilinear maps, it is possible to adapt the construction of the tensor product to directly construct the tensor product $M_1 \otimes_A ... \otimes_A M_n$ of a family $M_1 ... M_k$ of A-modules.*

Theorem 8.11. *If M, N are two free A-modules with respective bases $(e_i)_{i\in\mathcal{I}}$ and $(f_j)_{j\in\mathcal{J}}$, their tensor product $M \otimes_A N$ is free with basis $(e_i \otimes f_j)_{(i,j)\in\mathcal{I}\times\mathcal{J}}$*

Proof. This follows from the universal property of free modules. Let

$$C = A^{(\mathcal{I}\times\mathcal{J})} =< (\delta_{i,j})_{(i,j)\in\mathcal{I}\times\mathcal{J}} >$$

be the free A-module with basis $\mathcal{I} \times \mathcal{J}$. On the one hand consider the A-linear map

$$\varphi : C \longrightarrow M \otimes_A N$$

defined by $\varphi(\delta_{i,j}) = e_i \otimes f_j$.

Conversely, the map

$$\begin{array}{rccc} \tilde{\psi} : & M \times N & \longrightarrow & C \\ & \left(\sum_{i\in\mathcal{I}} a_i e_i, \sum_{j\in\mathcal{J}} b_j f_j\right) & \longmapsto & \sum_{(i,j)\in\mathcal{I}\times\mathcal{J}} a_i b_j \delta_{i,j} \end{array}$$

is A-bilinear (it is defined by $\tilde{\psi}(e_i, f_j) = \delta_{i,j}$). It thus induces by the universal property of the tensor product the A-module homomorphism $\psi : M \otimes_A N \longrightarrow C$ given on pure tensors by $\psi(e_i \otimes e_j) = \delta_{i,j}$.

The maps φ and ψ are mutual inverses. □

Corollary 8.12. *If M and N are free A-modules of finite ranks m and n respectively, their tensor product $M \otimes_A N$ is free of rank mn.*

8.3 Tensor product of algebras

Definition 8.13. *Let A be a ring and B a set. We say that B is an A-algebra if it is endowed with composition laws $(E, +, \cdot, \times)$*
($+$ and $\times$ internal, $\cdot$ external by A) such that

1. *$(B, +, \cdot)$ is an A-module;*
2. *$(B, \times)$ is a ring;*
3. *the multiplication $\times : B \times B \longrightarrow B$ is A-bilinear.*

A homomorphism of A-algebras $B \longrightarrow C$ is a homomorphism both of A-modules and of rings for the respective structures of B and C. A $\mathbb{Z}$-module being simply an abelian group, a $\mathbb{Z}$-algebra is a ring. We say that an A-algebra B is commutative if $(B, \times)$ is commutative. In the sequel, unless otherwise stated, we only consider commutative A-algebras.

Proposition 8.14. *Let A be a ring and B, C two A-algebras. The formula on pure tensors*

$$(b \otimes c) \cdot (b' \otimes c') = bb' \otimes cc'.$$

endows the tensor product $B \otimes_A C$ with a unique A-algebra structure.

Proof. By the universal property, the A-multilinear map

$$\begin{array}{rccc} \tilde{\varphi}: & B \times C \times B \times C & \longrightarrow & B \times_A C \\ & (b, c, b', c') & \longmapsto & bb' \otimes cc' \end{array}$$

induces the map $\varphi : B \otimes_A C \otimes_A B \otimes_A C \longrightarrow B \otimes_A C$ given on pure tensors by $\varphi(b \otimes c \otimes b' \otimes c') = bb' \otimes cc'$.

Since by associativity of the tensor product we also have

$$B \otimes_A C \otimes_A B \otimes_A C \simeq (B \otimes_A C) \otimes_A (B \otimes_A C),$$

the map φ also corresponds to the A-bilinear map

$$\psi : (B \otimes_A C) \times (B \otimes_A C) \longrightarrow B \otimes_A C$$

given on pure tensors by $\psi((b \otimes c) \otimes (b' \otimes c')) = bb' \otimes cc'$, which thus indeed endows $B \otimes_A C$ with a unique A-algebra structure. □

8.4 Applications

Extension of scalars

Let V be an $\mathbb{R}$-vector space of finite dimension and $(e_i)_{i=1}^n$ a basis of V. The tensor product $\mathbb{C} \otimes_{\mathbb{R}} V$ is an $\mathbb{R}$-vector space of dimension $2n$, and the family of pure tensors $1 \otimes e_1$, ..., $1 \otimes e_n$, $i \otimes e_1$,..., $i \otimes e_n$ is a basis. It can be endowed with a vector space structure over $\mathbb{C}$, by setting for pure tensors

$$z \cdot (z' \otimes v) = zz' \otimes v.$$

We can verify that the $\mathbb{C}$-vector space thus obtained corresponds to those envisioned at the beginning of the section. A great advantage of this process is that it is *canonical* (it does not depend on the choice of a basis of $\mathbb{C}$ as an $\mathbb{R}$-vector space) and that it generalizes very well as follows.

Proposition 8.15. *Let B be an A-algebra and C an A-module. Then the A-module $B \otimes_A C$ admits a B-module structure, uniquely determined on pure tensors by*

$$b \cdot (b' \otimes c) = bb' \otimes c$$

Proof. The map

$$\begin{array}{rccc} \tilde{\varphi}: & B \times B \times C & \longrightarrow & B \otimes_A C \\ & (b, b', c) & \longmapsto & bb' \otimes c \end{array}$$

is multilinear and thus induces by the universal property the A-linear map

$$\begin{array}{rccc} \varphi: & B \otimes_A B \otimes_A C & \longrightarrow & B \otimes_A C \\ & b \otimes b' \otimes c & \longmapsto & bb' \otimes c \end{array}.$$

Again, we obtain an A-bilinear map $\psi : B \times (B \otimes_A C) \longrightarrow B \otimes_A C$, given by $(b, b' \otimes c) \mapsto bb' \otimes c$ on pure tensors. We easily deduce by writing every element $x \in B \otimes_A C$ as a sum of pure tensors that $1 \cdot x = \psi(1, x) = x$, and that $b \cdot (b' \cdot x) = bb' \cdot x$. □

Product of affine varieties

We realize in this section the program outlined at the beginning of this part: constructing products of algebraic sets via the tensor product.

Proposition 8.16. *There exists an algebra isomorphism* $\mathbb{C}[X] \otimes_{\mathbb{C}} \mathbb{C}[Y] \simeq \mathbb{C}[X, Y]$.

Proof. The $\mathbb{C}$-bilinear map

$$\begin{array}{rccc} \tilde{\varphi}: & \mathbb{C}[X] \times \mathbb{C}[Y] & \longrightarrow & \mathbb{C}[X, Y] \\ & (P(X), Q(Y)) & \longmapsto & P(X)Q(Y) \end{array}$$

induces the $\mathbb{C}$-vector space homomorphism $\varphi : \mathbb{C}[X] \otimes_{\mathbb{C}} \mathbb{C}[Y] \longrightarrow \mathbb{C}[X, Y]$ given by the images $\varphi(P(X) \otimes Q(Y)) = P(X)Q(Y)$.

By virtue of Theorem 8.11, the $\mathbb{C}$-vector space $\mathbb{C}[X] \otimes_{\mathbb{C}} \mathbb{C}[Y]$ has basis the pure tensors $(X^n \otimes Y^m)_{(n,m)\in\mathbb{N}^2}$. These are sent via φ to the monomials $(X^n Y^m)_{(n,m)\in\mathbb{N}^2}$, a basis of the $\mathbb{C}$-vector space $\mathbb{C}[X, Y]$; φ is thus an isomorphism of $\mathbb{C}$-vector spaces. To show that φ is an algebra homomorphism, it suffices to show multiplicativity on pure tensors, which is clear. □

Remark 8.17. *The previous result still holds (with the same proof) if* $\mathbb{C}$ *is replaced by any ring* A*. It also extends of course by associativity or by multilinearity to any number of variables.*

Let $V = Z(P_1, ..., P_k) \subset \mathbb{C}[X_1, ..., X_n]$ and $W = Z(Q_1, ..., Q_s) \subset \mathbb{C}[Y_1, ..., Y_m]$ be two algebraic subsets and

$$\begin{cases} \mathcal{I} =< P_1, ..., P_k > \\ \mathcal{J} =< Q_1, ..., Q_s > \end{cases}$$

the associated ideals. The subset $V \times W \subset \mathbb{C}[X_1, ..., X_n, Y_1, ..., Y_m]$ is also algebraic, with associated ideal $\mathcal{K} =< P_1, ..., P_k, Q_1, ..., Q_s >$.

Proposition 8.18. *We have an algebra isomorphism*

$$\mathbb{C}[X_1, ..., X_n]/\mathcal{I} \otimes_{\mathbb{C}} \mathbb{C}[Y_1, .., Y_m]/\mathcal{J} \simeq \mathbb{C}[X_1, ..., X_n, Y_1, ..., Y_m]/\mathcal{K}.$$

Proof. Since $\mathcal{K}$ contains the images of $\mathcal{I}$ and $\mathcal{J}$ in $\mathbb{C}[X_1, ..., X_n, Y_1, ..., Y_m]$, the $\mathbb{C}$-bilinear map

$$\begin{array}{rccc} \tilde{\varphi}: & \mathbb{C}[X_1, ..., X_n]/\mathcal{I} \times \mathbb{C}[Y_1, .., Y_m]/\mathcal{J} & \longrightarrow & \mathbb{C}[X_1, ..., X_n, Y_1, ..., Y_m]/\mathcal{K} \\ & (f \bmod \mathcal{I}, g \bmod \mathcal{J}) & \longmapsto & fg \bmod \mathcal{K} \end{array}$$

is well-defined and induces the homomorphism

$$\varphi : \mathbb{C}[X_1, ..., X_n]/\mathcal{I} \otimes_{\mathbb{C}} \mathbb{C}[Y_1, .., Y_m]/\mathcal{J} \simeq \mathbb{C}[X_1, ..., X_n, Y_1, ..., Y_m]/\mathcal{K}$$

given by $\varphi(f \otimes g) = fg$, which is the algebra homomorphism of Proposition 8.16 (to lighten notation, we will no longer write the ideals).

The homomorphism φ is surjective, because $\varphi(X^\alpha \otimes Y^\beta) = X^\alpha Y^\beta$ and $\mathbb{C}[X_1, ..., X_n, Y_1, ..., Y_m]/\mathcal{K}$ is generated by these monomials.

It remains to show that φ is injective. On the one hand by fixing bases $(e_x)_{x\in\mathfrak{X}}$ and $(f_y)_{y\in\mathfrak{Y}}$ for the $\mathbb{C}$-vector spaces $\mathbb{C}[X_1, ..., X_n]/\mathcal{I}$ and $\mathbb{C}[Y_1, .., Y_m]/\mathcal{J}$, we can write every element of $\mathbb{C}[X_1, ..., X_n]/\mathcal{I} \otimes_{\mathbb{C}} \mathbb{C}[Y_1, .., Y_m]/\mathcal{J}$ as a linear combination of pure tensors of the form $e_i \otimes \cdot$ (by moving scalars to the right). Take an element $h \in \ker(\varphi)$ and write it

$$h = \sum_{x\in\mathfrak{X}} e_x \otimes h_x.$$

The fact that h belongs to the kernel of φ implies that for every pair $i_0 \in Z(\mathcal{I})$, $j_0 \in Z(\mathcal{J})$, we have $(i_0, j_0) \in Z(h) \subset \mathbb{C}^{n+m}$, i.e.,

$$0 = h(i_0, j_0) = \sum_{x\in X} e_x(i_0)h_x(j_0).$$

We first look at these equalities with j_0 fixed. The $(e_x)_{x\in\mathfrak{X}}$ forming a basis and i_0 being arbitrary, we obtain that for every $h_x(j_0) = 0$, for every $x \in \mathfrak{X}$. This being valid for every j_0, we actually get that h_x is the zero class, for every $x \in \mathfrak{X}$, and thus $h = 0$ and φ is an algebra isomorphism. □

9 Discrete valuation rings

9.1 Valuation rings

Definition 9.1. *An integral domain A is a valuation ring if it is not a field, and if for every $x \in \mathrm{Frac}(A)$, we have either $x \in A$, or $x^{-1} \in A$.*

Lemma 9.2. *A valuation ring is local.*

Proof. If I and J are two ideals of A, let us show that $I \subset J$ or $J \subset I$. Suppose $I \not\subset J$, and consider $i \in I \backslash J$. For every $j \in J$ nonzero, the element $[i, j] \in Frac(A)$ does not belong to A. Indeed otherwise we would have for some $a \in A$, $[a, 1] = [i, j]$ and $i = aj$ would be an element of J (we identify here A and $\iota(A)$). We thus have $[i, j]^{-1} = [j, i] \in A$, and $j = i \cdot [j, i]$ belongs to I, i.e., $J \subset I$.

Inclusion thus induces a total order on the set of ideals of A, which indeed has a unique maximal ideal. □

Proposition 9.3. *A valuation ring is integrally closed.*

Proof. Let $P(X) = X^n + a_{n-1}X^{n-1} + .. + a_0$ be a monic polynomial with coefficients in a valuation ring A and x a root of P in $Frac(A)$. If x is in A there is nothing to show. If not then x^{-1} belongs to A.

By hypothesis we have the equality

$$x^n + a_{n-1}x^{n-1} + ... + a_1x + a_0 = 0,$$

i.e., $x^n = -(a_{n-1}x^{n-1} + ... + a_1x + a_0)$. Dividing by x^{n-1} we obtain

$$x = -(a_{n-1} + a_{n-2}x^{-1} + ... + a_0x^{-n+1})$$

and x is indeed also an element of A. □

9.2 Definition and algebraic characterization

Definition 9.4. *A discrete valuation on a field K is a function*

$$v : K^* \longrightarrow \mathbb{Z}$$

that satisfies the following properties:

1. *v is surjective;*
2. *$v(xy) = v(x) + v(y)$;*
3. *if $x \neq y$, $v(x + y) \geq \min\{v(x), v(y)\}$.*

It is customary to further set $v(0) = \infty$ to extend property 3. to every pair $(x, y) \in (K^*)^2$.

Lemma 9.5. *If v is a discrete valuation on a field K, the set*

$$K_v = \{x \in K,\ v(x) \geq 0\}$$

is a valuation ring.

Proof. We show on the one hand that K_v is a subring of K. By hypothesis we have $0 \in K_v$, and by property 2. $1 \in K_v$ because $v(1) = 0$ by the equality

$$v(1) = v(1 \cdot 1) = v(1) + v(1).$$

Properties 2. and 3. ensure that K_v is stable under sum and product.

The ring K_v is an integral domain (since contained in K) and $\mathrm{Frac}(A)$ is contained in K. By 2. and $v(1) = 0$, we have $v(b) + v([1, b]) = 0$ so naturally

$$v([a, b]) = v(a) - v(b)$$

for every $[a, b] \in \mathrm{Frac}(A)$. In particular $v([a, b]) = -v([b, a])$ and K_v is a valuation ring because it is not a field (otherwise v would be identically zero, contradicting its surjectivity). □

Definition 9.6. *An integral domain A is a discrete valuation ring if there exists a valuation v on $\mathrm{Frac}(A)$ for which $A = \mathrm{Frac}(A)_v$.*

Lemma 9.7. *Let A be a discrete valuation ring. An element $a \in A^*$ is invertible if and only if $v(a) = 0$.*

Proof. We have seen that $v(1) = 0$. If $a \in A$ is invertible, we necessarily have $v(a) + v(a^{-1}) = v(1) = 0$, i.e., $v(a) = v(a^{-1}) = 0$.

Conversely if $a \in A^*$ has valuation zero, we compute in $\mathrm{Frac}(A)$

$$0 = v(1) = v(a \cdot [1, a]) = v(a) + v([1, a])$$

so $a^{-1} = [1, a]$ has valuation zero and a is indeed invertible in A. □

Proposition 9.8. *A discrete valuation ring is Euclidean, hence principal.*

Proof. Such a ring A is an integral domain, and v defines a Euclidean stathm. Let a, b be two elements of A^*, with b nonzero. If $v(b) \leq v(a)$, then the element $[a, b] \in \mathrm{Frac}(A)$ belongs to A, so we can set

$$a = b \cdot [a, b] + 0,$$

and if $v(b) > v(a)$, then we can simply set $a = 0 \cdot b + a$. □

Examples 9.9. *1. If k is a field, the ring $k[[X]]$ of formal power series is a discrete valuation ring.*

2. The p-adic integers form a discrete valuation ring.

Definition 9.10. *If A is a discrete valuation ring, an element a of A satisfying $v(a) = 1$ is called a uniformizing parameter.*

The valuation v being surjective by hypothesis, every discrete valuation ring admits a uniformizing parameter.

Proposition 9.11. *Let A be a discrete valuation ring, t a uniformizing parameter.*

1. *If $x \in \mathrm{Frac}(A)^*$, there exists a unit u such that $x = ut^{v(x)}$.*
2. *Every proper ideal of A is principal, generated by a power of t.*
3. *The ring A has unique maximal ideal $< t >= \{a \in A,\ v(a) > 0\}$ and its spectrum is $\mathrm{Spec}(A) = \{\{0\}, < t >\}$.*

Proof. 1. The element $u = xt^{-v(x)}$ has valuation 0, so it is an invertible element of A. We then indeed have $x = ut^{v(x)}$.

2. If I is an ideal of A, fix $i \in I$ an element of minimal valuation. If $v(i) = 0$ then $I = A$, and if $v(i) = n$, then $i = ut^n$ for u invertible, i.e., $< t^n > \subset I$. Conversely if $j \in I$ is nonzero, then $j = u't^m$ with $m \geq n$ and u' invertible so $I =< t^n >$.

3. The proper ideals of A are the $< t^n >$, with $n \geq 1$. These ideals are nested since for every integer k we have a strict inclusion $< t^{k+1} > \subsetneq < t^k >$ (A is an integral domain). The only nonzero prime ideal of A is thus $< t >$, which is maximal.

□

We will now establish a first algebraic characterization of discrete valuation rings.

Theorem 9.12. *Let A be a ring. The following assertions are equivalent.*

1. *A is a discrete valuation ring;*
2. *A is a local and principal ring, but not a field;*
3. *A is factorial with a unique irreducible element (up to association).*

Proof. $\boxed{1. \Rightarrow 2.}$ Follows from Lemmas 9.2 and 9.8.

$\boxed{2. \Rightarrow 3.}$ A is principal hence factorial. Moreover, up to association, the irreducible elements of A are in bijection with the nonzero maximal ideals of A. The ring A being local but not a field, it has a unique irreducible element (always up to association).

3. $\Rightarrow$ 1. Denoting t an irreducible element of A, every element of A^* is associated by factoriality to a power of t (zero for units). In particular if $x \in \mathrm{Frac}(A)$ belongs to its fraction field we have an integer n_x and a unit $u \in A$ such that $x = ut^{n_x}$. The map

$$\begin{array}{rccc} v: & \mathrm{Frac}(A) & \longrightarrow & \mathbb{Z} \\ & x & \longmapsto & n_x \end{array}$$

is clearly a valuation, with $A = \mathrm{Frac}(A)_v$. □

9.3 Nakayama's lemma

Theorem 9.13. *Let A be a ring and M a finitely generated A-module, $\varphi \in \mathrm{Hom}_A(M, M)$ and I an ideal of A such that $\varphi(M) \subset IM$. Then φ is annihilated by a monic polynomial with coefficients in I.*

Proof. Denoting $\{m_1, ..., m_n\}$ a generating system of M, we observe on the one hand that every element of IM can be written as a sum $i_1m_1 + ... + i_nm_n$, where the $(i_j)_{j=1}^n$ are elements of I.

By hypothesis for every $i = 1, ..., n$ we have $\varphi(m_i) \in IM$, i.e.,

$$\varphi(m_i) = \sum_{j=1}^{n} c_{ij}m_j$$

with $(c_{ij})_{j=1}^n$ in I. The homomorphism φ thus acts via the matrix $C = (c_{ij})_{i,j=1}^n$. The Cayley-Hamilton theorem thus implies that χ is a root of the characteristic polynomial of C which is indeed monic and with coefficients in I. □

Corollary 9.14. *Let A be a ring, M a finitely generated A-module and I an ideal of A such that $IM = M$. Then there exists $x \in 1 + I$ such that $xM = \{0\}$.*

Proof. We apply Theorem 9.13 to the map $\varphi = Id_M$.

Since we have $\varphi(M) = M = IM$, there exist elements $i_1, ..., i_n$ in I such that

$$\varphi^n + i_1\varphi^{n-1} + ... + i_{n-1}\varphi + i_n id_M = 0$$

but φ being the identity we obtain

$$(1 + i_1 + ... + i_n)\varphi = 0.$$

The element $x = 1 + i_1 + ... + i_n \in 1 + I$ thus satisfies

$$xM = x\varphi(M) = (x\varphi)(M) = 0.$$

□

Definition 9.15. *The intersection of all maximal ideals of a ring A is the Jacobson radical of A.*

Corollary 9.16 (Nakayama's lemma)**.** *Let A be a ring.*

1. *If A is local with maximal ideal $\mathfrak{m}$, then for every finitely generated A-module M, $M\mathfrak{m} = 0$ implies $M = 0$.*

2. *If $\mathfrak{R}$ is the Jacobson radical of A, then for every finitely generated A-module M, $\mathfrak{R}M = M$ implies $M = 0$.*

Proof. 1. Corollary 9.14 with $I = \mathfrak{m}$ indicates $(1 + a)M = 0$ for some $a \in \mathfrak{m}$, but $1 + a$ does not belong to $\mathfrak{m}$ so is invertible, and $M = 0$.

2. Again we have $a \in \mathfrak{R}$ such that $(1 + a)M = 0$, and it remains to show that $1 + a$ is invertible. If it were not, the ideal $< 1 + a >$ would be contained in a maximal ideal $\mathfrak{m}$, but $a \in \mathfrak{R} \subset \mathfrak{m}$ so 1 belongs to $\mathfrak{m}$, absurd.

□

9.4 A geometric characterization

Using Nakayama's lemma, we will now propose a new characterization of discrete valuation rings, with a more geometric flavor.

Definition 9.17. *If X is a topological space, a chain of irreducible closed sets of X of length n is a sequence*

$$Z_0 \subsetneq Z_1 \subsetneq ... \subsetneq Z_n \subset X$$

where $Z_0, ..., Z_n$ are irreducible closed sets of X. The dimension (or Krull dimension) of X is the supremum of the lengths of chains of irreducible closed sets of X; we denote it $\dim(X)$.

Theorem 6.26 justifies the following definition.

Definition 9.18. *The dimension (or Krull dimension) of a ring A is the dimension of the spectrum* $\mathrm{Spec}(A)$*, endowed with the Zariski topology; we denote it* $\dim(A)$*. It corresponds to the supremum of the lengths of chains of prime ideals*

$$\mathfrak{p}_0 \subsetneq \mathfrak{p}_1 \subsetneq ... \subsetneq \mathfrak{p}_n.$$

Examples 9.19. *1. A field k has dimension 0;*

2. *The ring $\mathbb{Z}$ has dimension 1;*

3. *The ring $k[X_1, ...X_n]$ of polynomials in n variables with coefficients in a field k has dimension n.*

Proposition 9.20. *The spectrum* $\mathrm{Spec}(A)$ *of a ring, endowed with the Zariski topology, is Hausdorff if and only if it has dimension* 0.

Proof. This is simply a translation of Proposition 6.12. □

Theorem 9.21. *Let A be a Noetherian ring and I an ideal of A. If $x \in \bigcap_{n=1}^{\infty} I^n$, then $x \in xI$.*

Proof. If $a_1, ..., a_m$ is a generating system of I and $x \in \bigcap_{n=1}^{\infty} I^n$, then for every $n \in \mathbb{N}^*$, there is a homogeneous polynomial $P_n \in A[X_1, ..., X_m]$ such that

$$x = P_n(a_1, ..., a_n).$$

For every $n \geq 1$, denote J_n the ideal of $A[X_1, ..., X_m]$ generated by the polynomials $P_1, ..., P_n$. The sequence of ideals $(J_n)_{n\geq 1}$ is increasing hence stationary, because $A[X_1, ..., X_m]$ is Noetherian. Choosing an integer N such that $J_N = J_{N+1}$, we thus have polynomials $Q_1, ..., Q_N$ such that

$$P_{N+1}(X_1, ..., X_m) = \sum_{k=0}^{N} Q_k(X_1, ..., X_m)P_k(X_1, ..., X_m).$$

Evaluation at $(a_1, ..., a_m)$ thus gives

$$x = P_{N+1}(a_1, ..., a_m) = x\left(\sum_{k=0}^{N} Q_k(a_1, ..., a_m)\right)$$

is indeed an element of xI. □

Corollary 9.22 (Krull's intersection theorem)**.** *Let A be a Noetherian ring. In the following two situations*

1. *A is an integral domain and I is a proper ideal;*
2. *A is arbitrary and I is contained in the Jacobson radical of A*

we have $\bigcap_{n=1}^{\infty} I^n = 0$.

Proof. By Theorem 9.21 we know that if $x \in \bigcap_{n=1}^{\infty} I^n$, then there exists $i \in I$ such that $x = xi$.

1. If A is an integral domain, we indeed have $x(1 - i) = 0$ and $i \neq 1$ (I is proper) so $x = 0$.

2. We saw during the proof of Corollary 9.16, 2. that if $a \in A$ belongs to the Jacobson radical $\mathfrak{R}$, then $1 + a$ is invertible. The equality $x(1 - i)$ with $i \in I \subset \mathfrak{R}$ thus indeed gives $x = 0$.

□

Remark 9.23. *Other more classical proofs of Krull's intersection theorem rely on Nakayama's lemma.*

Theorem 9.24. *For A an integral domain, the following conditions are equivalent.*

1. *A is a discrete valuation ring.*

2. *A is Noetherian, integrally closed, local and of dimension 1.*

3. *A is Noetherian, local and with monogenic maximal ideal, but not a field.*

Proof. $\boxed{1. \Rightarrow 2.}$ We have indeed shown previously that a discrete valuation ring is integrally closed (Proposition 9.3), local (Lemma 9.2) and of dimension 1 (Proposition 9.11).

$\boxed{2. \Rightarrow 3.}$ Since A has dimension 1, it is not a field. It thus remains to show that the maximal ideal $\mathfrak{m}$ of A is monogenic. On the one hand since A is local and Noetherian $\mathfrak{m}$ is finitely generated and equal to its Jacobson radical. By Nakayama's lemma, we have $\mathfrak{m}^2 \neq \mathfrak{m}$. We thus choose an element $t \in \mathfrak{m} \setminus \mathfrak{m}^2$ and show that t generates $\mathfrak{m}$.

On the one hand, we have $\mathfrak{m} = \sqrt{< t >}$ because $\mathrm{Spec}(A) = \{(0), \mathfrak{m}\}$ (the ring A is local and of dimension 1). Suppose that the minimal integer n_t such that $\mathfrak{m}^n \subset < t >$ is strictly greater than 1. If $x \in \mathfrak{m}^{n-1}$ not belonging to $< t >$, we still have $x\mathfrak{m} \subset \mathfrak{m}^n \subset < t >$.

Let us show that the element $y = [x, t] \in \mathrm{Frac}(A)$ is integral over A. Since we have $x\mathfrak{m} \subset < t >$, $y\mathfrak{m}$ is an ideal contained in A. On the one hand, it is a proper ideal because $1 = ym$ implies that $t = tym = xm$ belongs to $\mathfrak{m}^n \subset \mathfrak{m}^2$, which contradicts the definition of t. So $y\mathfrak{m}$ is a proper ideal, contained in $\mathfrak{m}$.

Let $m_1, ..., m_s$ be a generating system of $\mathfrak{m}$. For $1 \leq j \leq s$, we have elements $a_{ij} \in A$ such that

$$ym_j = \sum_{i=0}^{s} a_{ij} m_i,$$

i.e., for every j,

$$\sum_{i=0}^{s} (\delta_{ij} y - a_{ij}) m_i = 0,$$

where δ_{ij} is the Kronecker symbol. Denoting Δ the determinant of the matrix, Lemma 2.5 indicates that $\Delta\mathfrak{m} = 0$. Since A is an integral domain and $\mathfrak{m}$ is nonzero, we obtain $d = 0$, i.e., y is integral, a root of the polynomial

$$\Delta(X) = \det\left[((\delta_{ij}X - a_{ij})m_i)_{i,j}\right].$$

The ring A being integrally closed we have $y = [x, t] \in A$, so $x = at$ and $x \in < t >$, contradiction. We thus have $n = 1$ and $\mathfrak{m} =< t >$ is monogenic.

3. $\Rightarrow$ 1. On the one hand A is not a field, by hypothesis. Denote $< t >$ the maximal ideal of A. Consider a decreasing sequence of ideals

$$A =< 1 > \subset < t > \subset < t^2 > \subset < t^3 > \ldots$$

If a is an element of A^*, set $n_a = \max\{n,\ a \in < t^n >\}$, which is well-defined because $\bigcap_{n\geq 0} < t^n >= 0$ (Corollary 9.22). We have $a \in A^\times$ if and only if $n_a = 0$ and more generally by maximality of n_a, we have $a = ut^{n_a}$ for a unit u.

If I is an ideal of A, let $N = \min\{n_i,\ i \in I\}$. Every element $x \in I$ such that $n_x = N$ generates the ideal I. The ring A is thus local and principal, i.e., a discrete valuation ring by Theorem 9.12. □

Corollary 9.25. *An integral domain A is a discrete valuation ring if and only if it is local, Dedekind, and not a field.*

Corollary 9.26. *A valuation ring A is a discrete valuation ring if and only if A is Noetherian.*

Proof. If A is a discrete valuation ring, it is a principal ideal ring by Proposition 9.8, hence a Noetherian ring.

Conversely if A is Noetherian and $I =< a_1, \ldots, a_n >$ is an ideal of A, we show that I is actually monogenic. We have indeed seen during the proof of Lemma 9.2 that inclusion induces a total order on the ideals of A, so we have an ideal $< a_{i_0} >$ maximal among the $< a_i >_{i=1}^n$ and a_{i_0} generates I. The ring A is thus principal and local, hence a discrete valuation ring by Theorem 9.12. □

Corollary 9.27. *Let A be an integral domain, Noetherian and integrally closed. If $\mathfrak{p} \in \mathrm{Spec}(A)$ is minimal and nonzero, then $A_\mathfrak{p}$ is a discrete valuation ring.*

Proof. The localization $A_\mathfrak{p}$ is not a field because $\mathfrak{p}$ is nonzero, it is a Noetherian ring, integrally closed, local and of dimension 1. □

Bibliography

[1] Lang, S., *Algebra*, Graduate Texts in Mathematics 211, Springer (2002)