COMMUTATIVE ALGEBRA

Alfonso Zamora Saiz

Máster Universitario en Matemáticas Avanzadas (MUMAv)

May 8, 2026

Universidad Politécnica de Madrid, 2025

Lecture notes for the course ÁLGEBRA AVANZADA, from Máster Universitario en Matemáticas Avanzadas at Universidad Politécnica de Madrid, written by Alfonso Zamora Saiz for the academic year 2025-26.

Contents

Chapter 1

Rings and ideals

In these notes a **ring** $A := (A, +, \cdot)$ will always represent a commutative ring with unit 1_A, which is the neutral element for the product. The neutral element for the sum will be denoted by 0_A. We will drop the subscript when understood from the context. We will denote by k a field, i.e. a ring where every element by zero has a multiplicative inverse.

1.1 General theory of rings and ideals

1.1.1 Basic definitions

Definition 1. *A subset $I \subset A$ is an ideal if*

- $0 \in I$
- *For every $f, g \in I$, it is $f - g \in I$*
- *For every $f \in I$, $a \in A$, it is $af \in I$*

or, equivalently,

- $0 \in I$
- *For every $f, g \in I$, $a, b \in A$, it is $af + bg \in I$*

Given a subset $\Sigma \subset A$, we denote the ideal generated by Σ by (Σ), which is equal to the finite linear combinations of elements in Σ with coefficients in A:

$$(\Sigma) = \{a_1 f_1 + \cdots + a_n f_n \ : \ a_i \in A, f_i \in \Sigma\}.$$

We will call **principal ideals** to those ideals generated by a single element $f \in A$, and will be denoted by (f). In particular, (0) is an ideal, just the element zero, and $(1_A) = A$ is the total ring.

We can perform different operations with ideals. Given ideals $I, J \subset A$, we define:

Sum: $I + J = \{f + g \ : \ f \in I, g \in J\}$

Product: $IJ = I \cdot J := \{f_1 g_1 + \cdots + f_n g_n \ : \ f_i \in I, g_i \in J\}$

Intersection: $I \cap J = \{f \in A \ : \ f \in I, f \in J\}$

Definition 2. *We define the subset of* ***units*** *of a ring A as those elements with a multiplicative inverse:*

$$\mathcal{U}(A) := \{a \in A \ : \ \exists b \in A, ab = ba = 1\}$$

Note that, if A is a field, $\mathcal{U}(A) = A \backslash \{0\}$.

Definition 3. *We define the subset of* ***zero divisors*** *of a ring A as:*

$$\mathrm{Div}(A) := \{a \in A \ : \ a \neq 0, \exists b \in A, b \neq 0, ab = ba = 0\}$$

Definition 4. *We will say that a ring A is an* ***integral domain*** *(or a* ***domain****, for short), if it has no zero divisors, i.e.* $\mathrm{Div}(A) = \emptyset$.

For a domain A, we can construct its field of fractions:

$$\begin{array}{ccccc} A & \hookrightarrow & \mathrm{Frac}(A) & = \left\{\frac{a}{b} \ : \ a, b \in A, b \neq 0\right\} \\ a & \mapsto & \frac{a}{1} & \end{array} \tag{1.1}$$

which contains A as a subring.

Definition 5. *We say that an element $a \in A$ is* ***nilpotent*** *if there exists an integer $n \in \mathbb{N}$ such that $a^n = 0$.*

Exercise 1. *Show that, if a is nilpotent, then $1 - a$ is a unit. Deduce that the sum of a nilpotent and a unit is a unit.*

Definition 6. *We say that an element $a \in A$ is idempotent if $a^2 = a$.*

If $a \in A$ is idempotent, then $a(1 - a) = 0$ every $x \in A$ decomposes uniquely as $x = xa + x(1 - a)$, hence the ring splits as $A = Aa \oplus A(1 - a)$.

Definition 7. *Given rings A and B an application between them $\varphi : A \to B$ is a* ***ring homomorphism*** *if*

- *For every $a_1, a_2 \in A$, $\varphi(a_1 + a_2) = \varphi(a_1) + \varphi(a_2)$*
- *For every $a_1, a_2 \in A$, $\varphi(a_1 \cdot a_2) = \varphi(a_1) \cdot \varphi(a_2)$*
- $\varphi(1_A) = 1_B$

A ring homomorphism which is injective is called a ***ring monomorphism****. A ring homomorphism which is surjective is called a* ***ring epimorphism****. A ring homomorphism which is both injective and surjective is called a* ***ring isomorphism****.*

Let $f : A \to B$ be a ring homomorphism, and let $I \subset A$, $J \subset B$ be ideals. It can be shown that $f^{-1}(J) \subset A$ is an ideal. In particular, $\operatorname{Ker} f = f^{-1}((0)) = f^{-1}(0)$ is an ideal. However, $\operatorname{im}(I) \subset B$ and $\operatorname{im} \varphi \subset B$ are subrings but, in general, they are not ideals. To convert them into ideals we need to multiply by the ring B. Hence, this defines a correspondence between ideals of A and B:

$$\begin{aligned} &\text{each ideal } I \subset A \text{ gives an ideal } f(I)B \subset B \text{ called the } \textbf{extension} \text{ of } I \text{ and denoted by } e(I)\ , \\ &\text{each ideal } J \subset B \text{ gives an ideal } f^{-1}(J) \subset A \text{ called the } \textbf{restriction} \text{ of } J \text{ and denoted by } r(J)\ . \end{aligned} \tag{1.2}$$

Exercise 2. *Show that $I \subset r(e(I))$ and $e(r(J)) \subset J$, but equalities do not hold in general. Show that there is a bijection between ideals $I \subset A$ such that $I = r(e(I))$ and ideals $J \subset B$ such that $e(r(J)) = J$.*

Ideals in ring theory have a similar role as normal subgroups in group theory, they provide quotient rings. Given a ring A and an ideal $I \subset A$, we have the equivalence relation in A given by $a \sim_I b \Leftrightarrow a - b \in I$. Then we can construct the quotient ring

$$A/I = \{[a], +, \cdot\}$$

where each equivalence class is given by $[a] = a + I$. We have the surjective homomorphism $\varphi : A \to A/I$ whose kernel is $\operatorname{Ker} \varphi = I$.

There exists a bijective correspondence between ideals I, J of A with $I \subset J$ and ideals J/I of the quotient A/I:

$$\{I \subset J \subset A\} \overset{1:1}{\longleftrightarrow} \{J/I \subset A/I\} \tag{1.3}$$

Theorem 1. *We have the following three isomorphism theorems for rings:*

(1) Given a ring homomorphism $\varphi : A \to B$, it induces a ring isomorphism $\overline{\varphi} : A/\operatorname{Ker} \varphi \to \operatorname{im} \varphi$.

(2) Given ideals $I \subset J \subset A$, we have the ring isomorphism $\frac{A/I}{J/I} \to A/J$.

(3) Given an extension of rings $A \subset B$ and an ideal $J \subset B$, we have the ring isomorphism $A/A \cap J \to A + J/J$.

1.1.2 Prime and maximal ideals

Definition 8. *A subset $S \subset A$ is a **multiplicative set** if $1_A \in S$ and for every $f, g \in S$, it is $fg \in S$.*

Definition 9. *An ideal $\mathfrak{p} \subsetneq A$ is called a **prime ideal** if for every ideals $I, J \subset A$ such that $I \cdot J \subset \mathfrak{p}$, then either $I \subset \mathfrak{p}$ or $J \subset \mathfrak{p}$.*

Exercise 3. *Prove that $\mathfrak{p} \subset A$ is a prime ideal if and only if $A \backslash \mathfrak{p}$ is a multiplicative set if and only if $A/\mathfrak{p}$ is a domain.*

Given a prime ideal $\mathfrak{p} \subset A$ with denote by $k(\mathfrak{p}) = \operatorname{Frac}(A/\mathfrak{p})$ the **residue field** of $\mathfrak{p}$.

Definition 10. *An ideal $\mathfrak{m} \subsetneq A$ is a **maximal ideal** if there is no other ideal $I \subsetneq A$ with $\mathfrak{m} \subsetneq I \subsetneq A$.*

Exercise 4. *Prove that every maximal ideal is a prime ideal.*

Exercise 5. *Prove that if $\mathfrak{m} \subset A$ is a maximal ideal then $A/\mathfrak{m}$ is a field.*

Definition 11. *Define the **prime spectrum** (or just the **spectrum**) of a ring A as the set of prime ideals*

$$\operatorname{Spec} A = \{\mathfrak{p} \subsetneq A \ : \ \mathfrak{p} \text{ is a prime ideal}\}.$$

*Define the **maximal spectrum** of a ring A as the set of maximal ideals*

$$\operatorname{Specmax} A = \{\mathfrak{m} \subsetneq A \ : \ \mathfrak{m} \text{ is a maximal ideal}\}$$

Let us show the existence of prime and maximal ideals in any ring A.

Let $\Sigma = (\Sigma, \leq)$ be a partially ordered set. For a subset $\Lambda \subset \Sigma$ we say that $u \in \Sigma$ is an upper bound of Λ if $l \leq u$ for every $l \in \Lambda$. We say that $w \in \Sigma$ is maximal if there does not exists an element $u \in \Sigma$ with $w \leq u$ and $w \neq u$. We say that $\Lambda \subset \Sigma$ is a totally ordered set if for every $l, m \in \Lambda$, we have $l \leq m$ or $m \leq l$.

Lemma 1 (Zorn)**.** *Let $\Sigma \neq \varnothing$ be a partially ordered set such that every totally ordered subset Λ of Σ has an upper bound in Σ. Then Σ has a maximal element.*

Proof. Zorn's lemma is equivalent to the axiom of choice and to the principle of well-ordering (or Zermelo theorem) in set theory. □

Proposition 1. *Let S be a multiplicative set in a ring A, and let $I \subset A$ be an ideal disjoint with S. Then, there exists a prime ideal $\mathfrak{p}$ containing I and disjoint with S.*

Proof. Define the set $\Sigma := \{J \supset I \ : \ J \cap S = \emptyset\}$ of ideals containing I and disjoint from S. This set is non-empty because I itself belongs to Σ, and is partially-ordered with the inclusion. Let $\Lambda \subset \Sigma$ be a totally ordered subset. Then $K := \bigcup_{J_i \in \Lambda} J_i$ is an ideal which is an upper bound of Λ. By Zorn's Lemma 1 there exists a maximal element $\mathfrak{p} \in \Sigma$.

Let us show that $\mathfrak{p}$ is a prime ideal by showing that if $f, g \notin \mathfrak{p}$, then $fg \notin \mathfrak{p}$. Suppose that there are elements $f, g \in A$ such that $f, g \notin \mathfrak{p}$. Then, $\mathfrak{p} \subsetneq \mathfrak{p} + (f)$, $\mathfrak{p} \subsetneq \mathfrak{p} + (g)$ and, by maximality of $\mathfrak{p}$, these two bigger ideals intersect S in elements of the form $p + af$, $q + bg$, with $p, q \in \mathfrak{p}$, $a, b \in A$. Being S multiplicative, their product $(p + af) \cdot (q + bg) \in S$, and

$$(p + af) \cdot (q + bg) = pq + pbg + qaf + abfg$$

where $pq + pbg + qaf \in \mathfrak{p}$. Given that $\mathfrak{p} \cap S = \emptyset$, it is $abfg \notin \mathfrak{p}$, then $fg \notin \mathfrak{p}$, completing the proof. □

Proposition 2. *Let $I \subsetneq A$ be a proper ideal. Then, there exists a maximal ideal $\mathfrak{m}$ containing I.*

Proof. The proof is a similar application of Zorn's Lemma 1 as in Proposition 1, by considering the set $\Sigma := \{I \subset J \subsetneq A\}$. □

Exercise 6. *Complete the details of the proof of Proposition 2.*

Corollary 1. *Every ring is a disjoint union of its units and its maximal ideals,* $A = \mathcal{U}(A) \bigsqcup (\bigcup \mathfrak{m})$.

Proof. Exercise. □

Let us define the radical and the nilradical of an ideal.

Definition 12. *Let* $I \subset A$ *be an ideal. We define the* ***radical*** *of* I *as*

$$\sqrt{I} := \{f \in A \ : \ \exists n \in \mathbb{N}, \ f^n \in I\}.$$

We say that I *is a* ***radical*** *ideal if* $\sqrt{I} = I$.

Exercise 7. *Prove that the radical of an ideal is also an ideal.*

Proposition 3. *We have* $\sqrt{I} = \bigcap_{\mathfrak{p} \in \operatorname{Spec} A, I \subset \mathfrak{p}} \mathfrak{p}$.

Proof. Let $f \in \sqrt{I}$ and let $\mathfrak{p} \subset A$ a prime ideal such that $I \subset \mathfrak{p}$. Then, there exists an integer $n \in \mathbb{N}$ with $f^n \in I \subset \mathfrak{p}$. Since $\mathfrak{p}$ is a prime ideal, $f \in \mathfrak{p}$.

Conversely, let $f \notin \sqrt{I}$. If $f^n \notin I$ for any n, then $S = \{1, f, f^2, f^3, \dots\}$ is a multiplicative set disjoint from I. By Proposition 1 there exists a prime ideal $\mathfrak{p}$ which contains I and is disjoint with S, hence $f \notin \mathfrak{p}$. □

Definition 13. *The* ***nilradical*** *of a ring* A*, denoted by* nilrad A *is the set of nilpotent elements of* A*. We say that* A *is* ***reduced*** *if* $\operatorname{nilrad} A = 0$.

Observe that the nilradical of a ring A is the radical of its zero ideal, $\operatorname{nilrad} A = \sqrt{(0)}$.

Proposition 4. *We have* $\operatorname{nilrad} A = \bigcap_{\mathfrak{p} \in \operatorname{Spec} A} \mathfrak{p}$.

Proof. This is a consequence of Proposition 3, by taking $I = (0)$. □

Definition 14. *We define the* ***Jacobson radical*** *of a ring* A*, denoted by* $\mathfrak{R}$*, as* $\mathfrak{R} = \bigcap_{\mathfrak{m} \in \operatorname{Specmax} A} \mathfrak{m}$.

Exercise 8. *Prove that* $a \in \mathfrak{R}$ *if and only if* $1 - ab \in \mathcal{U}(A)$*, for every* $b \in A$.

We finish the section with the definition of local ring, a notion which will be further explored later in the course to study local geometric properties.

Definition 15. *A* ***local ring*** *is a ring* A *which has a unique maximal ideal* $\mathfrak{m}$*. We will often denote a local ring as* $(A, \mathfrak{m})$*. We will denote by* $k = A/\mathfrak{m}$ *its residue field.*

By Corollary 1 a ring is local if all the non-units form a maximal ideal, i.e. $(A, \mathfrak{m}) = \mathcal{U}(A) \bigsqcup \mathfrak{m}$.

Exercise 9. *Prove that if* $(A, \mathfrak{m})$ *is a local ring, then* $1 + \mathfrak{m} \subset \mathcal{U}(A)$.

1.2 Classes of domains

In this section we are going to recall the relevant classes of domains for the rest of the text. For this section A will always denote an integral domain.

1.2.1 ED, PID and UFD's

Let us begin by recalling the definition of prime and irreducible element Given two elements $a, b \in A$, we say that a divides b, denoted by $a \mid b$ if there exists an element $c \in A$ such that $ac = b$.

Definition 16. *An element $a \in A$, $a \neq 0$ is said to be **reducible** if there exist elements $b, c \in A \backslash \mathcal{U}(A)$ with $a = bc$. We say that a is **irreducible** if $a \notin \mathcal{U}(A)$ and a is not reducible.*

Definition 17. *An element $a \in A$ is said to be **prime** if $a \notin \mathcal{U}(A)$ and $a \mid bc$ implies $a \mid b$ or $a \mid c$.*

Remark 1. *Observe that if a is a prime element then (a) is a prime ideal.*

Proposition 5. *Let A be a domain. If $a \in A$ is prime, then a is irreducible.*

Proof. By definition $a \notin \mathcal{U}(A)$. Suppose that a is reducible, then there exist elements $b, c \notin \mathcal{U}(A)$ with $a = bc$. Then $bc \in (a)$, which is a prime ideal, therefore, for example, $b \in (a)$ (or $c \in (a)$). In this case, there exists $d \in A$ such that $b = ad$, then $a = bc = adc$, then $a(1 - dc) = 0$. Being A a domain, we get $1 = dc$, hence c is a unit, contradiction. □

We start with the definitions of Euclidean and Principal Ideal Domains.

Definition 18. *We say that a domain A is an **Euclidean Domain (ED)** if there exist an application $d : A\backslash\{0\} \to \mathbb{N}$, called **degree** such that*

- *For every $a, b \in A\backslash\{0\}$, $d(a) \leq d(ab)$.*
- *For every $a, b \in A$, $b \neq 0$, there exists $q, r \in A$ (called quotient and remainder, respectively), with $a = qb + r$ and either $r = 0$ or $r \neq 0$ and $d(r) < d(b)$.*

Definition 19. *We say that a domain A is a **Principal Ideal Domain (PID)** if every ideal $I \subset A$ is a principal ideal, i.e. $I = (a)$, $a \in A$.*

Proposition 6. *If A is a PID and $a \in A, a \neq 0$ is irreducible, then (a) is maximal. Therefore (a) is prime and a is prime.*

Proof. Suppose that there exists an ideal $(a) \subsetneq (b) \subsetneq A$. Then $a, b \notin \mathcal{U}(A)$ and there exist an element $c \in A$ such that $a = bc$, $c \notin \mathcal{U}(A)$, hence a is reducible, contradiction. □

Now we define the notion of Unique Factorization Domain.

Definition 20. *We say that a domain A is a **Unique Factorization Domain (UFD)** if every element $a \in A$, factors as $a = b\prod_i p_i^{n_i}$, with $b \in \mathcal{U}(A)$ and p_i irreducible elements such that p_i does not divide p_j for $i \neq j$, and this decomposition is unique up to units.*

Theorem 2. *Let A be an integral domain.*

(a) If A is an ED, then A is a PID.

(b) If A is a PID, then A is a UFD.

Proof. (a) Let $d : A\backslash\{0\} \to \mathbb{N}$ be the degree function. Let $(0) \neq I \subsetneq A$ be an ideal. Consider the set $M = \{d(a) : a \in I\backslash\{0\}\}$, which is non-empty, therefore it has a mininum $b \in I$ and $(b) \subset I$. Let us show that, indeed, $(b) = I$. Let $a \in I \subset A$, which is an ED, then there exists $q, r \in A$ with $a = qb + r$ with $r = 0$ or $r \neq 0$ and $d(r) < d(b)$. But $r = a - bq \in I$ and $d(b)$ is the minimum of M, then $r = 0$, $a = qb$ and $a \in (b)$. Therefore $I = (b)$ is principal and A is a PID.

(b) Let A be a PID, which is Noetherian. Consider the set

$$S := \{0 \neq a \in A \ : \ a \notin \mathcal{U}(A), a \text{ is not a finite product of irreducible elements}\}$$

and suppose that S is non-empty. Let $\Sigma := \{(a) \ : \ a \in S\}$, which has a maximal element by Proposition 8, say $J = (b)$, with $b \in S$ not being a finite product of irreducible elements, then b is reducible. Let $c_1, c_2 \notin \mathcal{U}(A)$ such that $b = c_1c_2$. Then, $J = (b) \subsetneq (c_1)$, $J = (b) \subsetneq (c_2)$, hence $c_1, c_2 \notin S$ and c_1, c_2 are products of irreducible elements, therefore b is a product of irreducible elements, which is a contradiction. Then we have shown that $S = \emptyset$ and every element $a \in A$ can be written as a product of irreducible elements, $a = p_1 \cdots p_r$.

Let us show the uniqueness of this factorization. Suppose that there exists other factorization $a = q_1 \cdots q_s$. Given that p_1 is irreducible, p_1 is prime by Proposition 6 and $p_1 \mid a = q_1 \cdots q_s$ then p_1 divides any of the $q's$, say, $p_1 \mid q_1$, both irreducible elements, then $p_1u_1 = q_1$, with $u_1 \in \mathcal{U}(A)$. Repeating the argument we arrive that $a = p_1 \cdots p_r = (u_1 \cdots u_r)p_1 \cdots p_rq_{r+1} \cdots q_s = up_1 \cdots p_rq_{r+1} \cdots q_s$, with $u \in \mathcal{U}(A)$. Then $p_1 \cdots p_r(1 - uq_{r+1} \cdots q_s) = 0$ in A domain, then $1 = uq_{r+1} \cdots q_s$ and $q_{r+1}, \cdots, q_s$ are units, then $r = s$.

□

Exercise 10. *Prove that in a UFD A, $a \in A$ is irreducible if and only if a is prime.*

Remark 2. *The three types of domains introduced reflect increasing properties in analogy with those of the ring of integers: being able to perform Euclidean division for a ED, having all their ideals generated by a single element or having a unique factorization in irreducibles (then in primes). Several familiar results for arithmetics in $\mathbb{Z}$ work in general in the different types of domains. In an ED, the Euclidean algorithm holds. In a PID, Bezout identity holds. In a UFD, there always exist the greatest common divisor (g.c.d) and the lowest common multiple (l.c.m).*

1.2.2 Gauss' Lemma

Next, we are going to prove the important Gauss' Lemma about rings of polynomials with coefficients in a UFD. We will say that $f(X) = a_0 + a_1X + a_2X^2 + \cdots + a_nX^n \in A[X]$ is a primitive polynomial if the greatest common divisor of its coefficients is one, i.e., $g.c.d(a_0, \ldots, a_n) = 1$.

Lemma 2. *Let A be a UFD. Let $f(X), g(X) \in A[X]$ be primitive polynomials. Then the product $f(X)g(X)$ is a primitive polynomial.*

Proof. Suppose that $f(X)g(X)$ is not a primitive polynomial and let $p \in A$ be an irreducible factor of the *g.c.d.* of the coefficients of $f(X)g(X)$, which is then a prime element because A is a UFD. Let

$$\pi : A[X] \longrightarrow A/(p)[X] \ , \ \sum a_i x^i \mapsto \sum (a_i + (p))x^i$$

be the map reducing the coefficients modulo p. Then, $\pi(f(X))\pi(g(X)) = \pi(f(X)g(X)) = 0$, because p divides all the coefficients of $f(X)g(X)$. Given that (p) is a prime ideal, $A/(p)$ is a domain and also is $A/(p)[X]$. Then p divides all the coefficients of $f(X)$, therefore $f(X)$ is not primitive, contradiction. □

Lemma 3. *Let A be a UFD with field of fractions $K = \mathrm{Frac}(A)$. A degree polynomial $f(X) \in A[X]$ of $\deg f \geq 1$ is irreducible in $A[X]$ if and only if $f(X)$ is irreducible in $K[X]$ and $f(X)$ is primitive in $A[X]$.*

Proof. Suppose that $f(X)$ of $\deg \geq 1$ is irreducible in $A[X]$ then, in particular, $f(X)$ is primitive in $A[X]$. Suppose that $f(X) = g(X)h(X)$ with $g(X), h(X) \in K[X]$ not units. Let $a, b \in A$ be the common denominators of the coefficients of $g(X)$ and $h(X)$, respectively. Then, $ag(X) = ug_1(X), bh(X) = vh_1(X) \in A[X]$, with $u, v \in A$ and $g_1(X), h_1(X)$ primitive in $A[X]$. Hence, $abf(X) = (ag(X))(bh(X)) = uvg_1(X)h_1(X)$. By Lemma 2, $g_1(X)h_1(X)$ is primitive in $A[X]$. This, together with $f(X)$ being primitive in $A[X]$ yields $f(X) = g_1(X)h_1(X)$. Given that $f(X)$ is irreducible in $A[X]$, $g_1(X)$ (or $h_1(X)$) has to be a unit in $A[X]$, therefore $g(X) = \frac{ug_1(X)}{a}$ is a unit in $K[X]$.

Conversely, suppose that $f(X)$ is irreducible in $K[X]$ and primitive in $A[X]$. Let $f(X) = g(X)h(X)$ in $A[X] \subset K[X]$. Then, $g(X)$ (or $h(X)$) is a unit in $K[X]$, hence $g(X) \in K\backslash\{0\} \cap A[X]$, therefore $g(X) \in A\backslash\{0\}$. Now, the *g.c.d.* of the coefficients of $f(X) = g(X)h(X)$ is 1, equal to the *g.c.d.* of the coefficients of $h(X)$ multiplied by $g(X) \in A\backslash\{0\}$. We conclude that $g(X) \in \mathcal{U}(A)$.

□

Theorem 3 (Gauss' Lemma)**.** *Let A be a UFD. Then, $A[X]$ is a UFD.*

Proof. We show that $A[X]$ is a UFD by using a characterization of these domains (c.f. [FG, Proposición IV.1.6]).

First we show that if $f(X)$ is irreducible in $A[X]$, then $f(X)$ is prime. If $\deg f(X) = 0$, then $f(X) \in A$ is irreducible in A, then $f(X)$ is prime in A and $(f(X))$ is prime in $A[X]$. If $\deg f(X) \geq 1$, by Lemma 3, $f(X)$ is irreducible in $K[X]$, which is an ED, hence a PID and $(f(X)) = f(X)K[X]$ is a prime ideal in $K[X]$. Then, we conclude by showing that

$$f(X)K[X] \cap A[X] = f(X)A[X]$$

hence $(f(X))$ is a prime ideal in $A[X]$ and $f(X)$ is prime in $A[X]$.

Second we show that every $f(X) \in A[X]$ can be written as a product of irreducible elements. If $f(X) \in \mathcal{U}(K[X])$, then $f(X) \in A\backslash\{0\}$ and A is a UFD, then f decomposes as a product of irreducible elements. If $f(X) \notin \mathcal{U}(K[X])$, given that $K[X]$ is a UFD, then $f(X) = g_1(X) \cdots g_r(X)$

in $K[X]$, with $a_i g_i(X) = u_i h_i(X) \in A[X]$, $a_1, \dots, a_r \in A\backslash\{0\}$, $u_1, \dots, u_r \in A\backslash\{0\}$, and $h_i(X)$ primitive in $A[X]$. As the $g_i(X)$ are irreducible, the $h_i(X)$ are irreducible, then if d is the *g.c.d.* in A of the coefficients of $f(X)$, $f(X) = df_1(X)$ with $f_1(X)$ primitive, we obtain

$$a_1 \cdots a_r d f_1(X) = u_1 \cdots u_r h_1(X) \cdots h_r(X)$$

Equalling primitive polynomials in both sides we get $f_1(X) = h_1(X) \cdots h_r(X)$. Finally, either $d \in \mathcal{U}(A)$ or $d = p_1 \cdots p_s$ irreducible elements in A, therefore

$$f(X) = p_1 \cdots p_s h_1(X) \cdots h_r(X)$$

decomposition in irreducible elements in $A[X]$, completing the proof of the Theorem. □

Corollary 2. *The rings $\mathbb{Z}[X]$, $\mathbb{Z}[X_1, \dots, X_n]$, $k[X_1, \dots, X_n]$ are UFD's.*

1.2.3 Some important examples

Example 1. *The ring of integers $\mathbb{Z}$ is an ED (with d being the absolute value), then a PID and a UFD. Apart from the zero ideal, the ideals of $\mathbb{Z}$ are the principal ideals (n), the multiples of an integer n. The prime ideals are (p), the multiples of a prime number, and these are also the maximal ideals (Proposition 6).*

Example 2. *If k is a field, the ring of polynomials in one variable $k[X]$ is an ED (with the d being the degree of a polynomial, then a PID and a UFD. The ideals of $k[X]$ are the principal ideals $(f(X))$. The prime ideals are (0) or $(f(X))$ with $f(X)$ irreducible (the latter are also the maximal ideals by Proposition 6). If k is algebraically closed (such as $k = \mathbb{C}$), then irreducible polynomials are degree 1 polynomials $f(X) = u(X - a)$, where $u \in \mathcal{U}(A)$ $a \in k$. If k is not algebraically closed (such as $k = \mathbb{R}$), there exist irreducible polynomials of degree > 1, like $f(X) = X^2 + 1 \in \mathbb{R}[X]$.*

Example 3. *The ring $\mathbb{Z}\left[\frac{1+\sqrt{-19}}{2}\right]$ is the simplest example of a PID which is not an ED, because it can be shown that there is no possible degree function.*

Example 4. ***(The arithmetic surface** $\mathbb{Z}[X]$**)** The ring $\mathbb{Z}[X]$ is a UFD but not a PID. For example, the ideal generated by 2 and X is not principal, i.e. there is no polynomial $f(X) \in \mathbb{Z}[X]$ such that $(2, X) = (f(X))$.*

The prime ideals of $\mathbb{Z}[X]$ are

- (0).
- (p), *with p a prime number.*
- $(f(X))$, *with $f(X)$ a polynomial irreducible in $\mathbb{Z}[X]$.*
- $(p, f(X))$, *with p a prime number and $f(X)$ a polynomial in $\mathbb{Z}[X]$ which is irreducible* mod p. *These are the maximal ideals.*

Let us show this. Let $\mathfrak{p} \in \mathbb{Z}[X]$ be a prime ideal. If $\mathfrak{p} = (0)$ or if $\mathfrak{p} = (g)$ with $g \in \mathbb{Z}[X]$ a prime element, then g is an irreducible element and, hence, g is either a prime number or an irreducible polynomial in $\mathbb{Z}[X]$, covering the first three cases. Assume that $\mathfrak{p} = (f_1(X), f_2(X))$ is a prime ideal which is not principal, and where $f_1(X), f_2(X)$ have no common factor in $\mathbb{Z}[X]$.

We claim that $f_1(X), f_2(X)$ also do not have a common factor in $\mathbb{Q}[X]$ where $\mathbb{Q} = \mathrm{Frac}(\mathbb{Z})$. If not, $f_1(X) = h(X)g_1(X)$, $f_2(X) = h(X)g_2(X)$, with $h(X), g_1(X), g_2(X) \in \mathbb{Q}[X]$ and $\deg h(X) \geq 1$. We extract the common denominator of these polynomials to obtain reduced expressions $h(X) = ah_0(X)$, $g_1(X) = b_1 j_1(x)$, $g_2(X) = b_2 j_2(X)$, with $a, b_1, b_2 \in K$ and $h_0(X), j_1(X), j_2(X)$ primitive polynomials in $\mathbb{Z}[X]$. By Lemma 2, $h_0(X)j_1(X)$, $h_0(X)j_2(X)$ are primitive. Then:

$$f_1(X) = h(X)g_1(X) = ah_0(X)b_1 j_1(X) = (ab_1)h_0(X)j_1(X) \in \mathbb{Z}[X]$$

$$f_2(X) = h(X)g_2(X) = ah_0(X)b_2 j_2(X) = (ab_2)h_0(X)j_2(X) \in \mathbb{Z}[X]$$

hence $ab_1, ab_2 \in \mathbb{Z}$ and, therefore, $h_0(X) \mid f_1(X), f_2(X)$, contradiction because $f_1(X)$, $f_2(X)$ have no common factor.

Now we show that $(f_1(X), f_2(X)) \cap \mathbb{Z} \neq 0$. Given that $\mathbb{Q}[X]$ is a PID and $f_1(X), f_2(X)$ have no common factor, by Bezout's identity there exist polynomials $a(X), b(X) \in \mathbb{Q}[X]$ such that $a(X)f_1(X) + b(X)f_2(X) = 1$. If $c \in \mathbb{Z}$ is the common denominator of the coeficients of $a(X)$ and $b(X)$, then we get $ca(X)f_1(X) + cb(X)f_2(X) = c \in \mathbb{Z}$, with $ca(X), cb(X) \in \mathbb{Z}[X]$.

Let us see that $(f_1(X), f_2(X)) \cap \mathbb{Z}$ is a prime ideal of $\mathbb{Z}$. On the one hand, let $r \in (f_1(X), f_2(X)) \cap \mathbb{Z}$ and let $s \in \mathbb{Z}$. Then

$$rs = (ca(X)f_1(X) + cb(X)f_2(X))s = csa(X)f_1(X) + csb(X)f_2(X) \in (f_1(X), f_2(X)) \cap \mathbb{Z}$$

then $(f_1(X), f_2(X)) \cap \mathbb{Z}$ is an ideal. On the other hand $(f_1(X), f_2(X)) \cap \mathbb{Z} = \psi^{-1}((f_1(X), f_2(X)))$, where $\psi : \mathbb{Z} \hookrightarrow \mathbb{Z}[X]$ and the preimage of a prime ideal by a ring homomorphism is a prime ideal. Then, being $\mathbb{Z}$ a PID, $(f_1(X), f_2(X)) \cap \mathbb{Z} = (p)$, where p is a prime number. Hence, p has to be one of the generators $f_1(X)$ or $f_2(X)$, otherwise $p = a(X)f_1(X) + b(X)f_2(X)$ and the right hand side has degree ≥ 1. And, for $f_2(X)$ to not have a common factor with $f_1(X) = p$, $f_2(X)$ has to be irreducible modulo p, completing the proof for the ideal $(p, f(X))$.

Note that

$$\mathbb{Z}[X] \xrightarrow{\alpha} \mathbb{F}_p[X] \xrightarrow{\beta} \mathbb{F}_p[X]/(\overline{f}(X))$$

where $\ker \beta \circ \alpha = (p, f(X))$. And $\mathbb{Z}[X]/(p, f(X)) \simeq \mathbb{F}_p[X]/(\overline{f}(X))$, which is a field (it is the quotient of a ring of polynomials with coefficients in a field, i.e. a UFD, by the ideal generated by an irreducible element, then a maximal deal). Therefore, $(p, f(X))$ is a maximal ideal.

Example 5. *(**The geometric surface** $k[X, Y]$) Similarly, $k[X, Y]$ is a UFD which is not a PID. The prime ideals of $k[X, Y]$ are*

- (0).
- *$(f(X, Y))$, with $f(X, Y)$ a polynomial irreducible in $k[X, Y]$.*
- *$(f(X), g(X, Y))$, with $f(X)$ a an irreducible polynomial in $k[X]$ and $g(X, Y)$ a polynomial in $k[X, Y]$ whose reduction $\bmod f(X)$, i.e. in $k[X, Y]/(f(X))$, is irreducible. These are the maximal ideals.*

Most of the examples of this course will be produced by means of ideals in the rings $\mathbb{Z}[X]$ and $k[X,Y]$, the arithmetic and the geometric surfaces.

Assume k is algebraically closed. The points in k^2 correspond to maximal ideals in $k[X,Y]$. Indeed, we have just seen that a maximal ideal in $k[X,Y]$ is of the form $(f(X), g(X,Y))$, with $f(X)$ a an irreducible polynomial in $k[X]$ and $g(X,Y)$ a polynomial in $k[X,Y]$ whose reduction $\bmod f(X)$ *is irreducible. This means that $f(X) = X - a$, $a \in k$ (there are the irreducible non-constant polynomials in $k[X]$). Let $g(X,Y)$ the other element of the maximal ideal. Passing to the reduction* $\bmod f(X)$ *is taking the image of the evaluation:*

$$\begin{array}{rccccc} ev_a: & k[X,Y] & \to & k[X,Y]/(X-a) & \simeq k[Y] \\ & h(X,Y) & \mapsto & h(a,Y) & \end{array}$$

if this image $ev_a(h(X,Y)) = h(a,Y)$ is irreducible as a polyonmial in $k[Y]$ then $h(a,Y) = Y - b$, $b \in k$. Therefore, we can identify each maximal ideal with $(X-a, Y-b)$ and with the point $(a,b) \in k^2$. The evaluation map

$$\begin{array}{rccccc} ev_{(a,b)}: & k[X,Y] & \to & k[X,Y]/(X-a,Y-b) & \simeq k \\ & h(X,Y) & \mapsto & h(a,b) & \end{array}$$

computes the value of each function in the point (a,b), and exhibits the maximality of $(X-a, Y-b)$ because the quotient by this ideal is the field k.

*Now, let $f(X,Y) \in k[X,Y]$ be a polynomial and consider the principal ideal $(f) \subset k[X,Y]$. Let $k[X,Y]/(f(X,Y))$ be the quotient ring whose elements are equivalence classes of polynomials $g(X,Y) + (f(X,Y))$. Let X be the subset of points in the affine plane k^2 which are solutions of the equation $f(X,Y) = 0$, i.e. $Z := \{(x,y) \in k^2 \ : \ f(x,y) = 0\}$. This is usually called an **algebraic curve** over k, or the set of k-points of the algebraic curve defined by f. If two polynomials $g(X,Y), h(X,Y) \in k[X,Y]$ have the same values over Z, i.e. $g(X,Y)|_Z = h(X,Y)|_Z$, then $(g(X,Y) - h(X,Y))|_Z$ is identically zero as a function, then $g(X,Y) - h(X,Y) \in (f(X,Y))$, therefore the elements*

$$g(X,Y) + (f(X,Y)) = h(X,Y) + (f(X,Y)) \in k[X,Y]/(f(X,Y))$$

are equal. This allows to call the quotient ring $k[X,Y]/(f(X,Y))$ the ring of (algebraic or polynomial) functions of the curve Z, this is, the elements of the ring are actually polynomial functions defined over Z. This correspondence between algebra and geometry is the core content of the course.

Let us finish by showing that there are two different types of non-domains.

Proposition 7. *Let A be a ring which is not an integral domain, then either A has nilpotents or A has more than one minimal prime.*

Proof. If $\operatorname{nilrad}(A) = 0$ then, by Proposition 4, $0 = \bigcap_{\mathfrak{p} \text{ prime}} \mathfrak{p} = \bigcap_{\mathfrak{p} \text{ prime minimal}} \mathfrak{p}$. If there is just one minimal prime, then this minimal prime is zero, and A would be a domain, contradiction. □

Example 6. *The ring $k[X,Y]/(X^2)$ is not reduced because the polynomial $f(X,Y) = X$ (modulo X^2) is a nilpotent element. It corresponds with the first type of non-domains described in Proposition 7.*

The nilradical of $k[X,Y]/(X^2)$ is the intersection of all its primes (Proposition 4). These primes are (X) and all $(X, Y-a)$, and the former is the the only minimal prime, which is the nilradical.

The elements of $k[X,Y]/(X^2)$ can be written in the form $f(Y)+Xg(Y)$, after reduced modulo X^2. This corresponds to the value of a Y-polynomial plus its first derivative, which reflects the geometry of the double Y-axis.

Example 7. *The ring $k[X,Y]/(XY)$ is not a domain because X and Y are zero-divisors. It has no nilpotents because (X) and (Y) are two different prime ideals (in fact, these are the two minimal prime ideals), intersecting in zero. It corresponds with the second type of non-domains described in Proposition 7.*

The elements of $k[X,Y]/(XY)$ can be written in the form $f(X)+g(Y)$, after reduced modulo XY. This corresponds to the value of a polynomial for each coordinate, which reflects the geometry of the union of the two axes.

1.3 Noetherian and Artinian rings

1.3.1 Noetherian rings

The condition of a ring being Noetherian reflects the algebraic counterpart to the geometric idea of finite dimension.

Definition 21. *Let $\Sigma := (\Sigma, \leq)$ be a partially ordered set. We say that Σ has the **ascending chain condition (ACC)** if every chain $x_1 \leq x_2 \leq \cdots \leq x_n \leq \cdots$ eventually stops, i.e., there exists an index k such that $x_k = x_{k+1} = x_{k+2} = \cdots$.*

For example, vector subspaces of finite dimensional vector spaces satisfy the ACC.

Exercise 11. *Prove that Σ has the ACC if and only if every non-empty subset $\Lambda \subset \Sigma$ has a maximal element.*

Definition 22. *A ring A is **Noetherian** if every ideal $I \subset A$ is finitely generated.*

Proposition 8. *The following are equivalent:*

(a) A is Noetherian.

(b) The set Σ of all ideals in A with the inclusion has the ACC.

(c) Every non-empty set of ideals Λ has a maximal element.

Proof.

(a)⇒(b) Consider the chain of ideals $I_1 \subset I_2 \subset I_3 \subset \cdots$. Let $J = \cup_i I_i$ which is an ideal and, by hypothesis, let $f_1, \ldots, f_n \in A$ such that $J = (f_1, \ldots, f_n)$. Given that each f_i belongs to any I_{j_i}, set $k = \max j_i$ and we obtain that $J = I_k$, stabilizing the chain.

(b)⇒(c) By contradiction, let $\varnothing \neq \Lambda \subset \Sigma$ be a subset with no maximal element. Then we can construct, by induction, an ascending chain of elements in Λ which does not stop.

(c)⇒(a) Let $I \subset A$ be an ideal. Let $\Lambda := \{J \subset I \ : \ J \text{ is fin. gen}\}$. We have that Λ is non-empty given that $(0) \subset \Lambda$, then by hypothesis Λ has a maximal element K. If $K \subsetneq I$, then there exists $f \in I \backslash K$ and $K \subsetneq (K, f)$, contradicting the maximality of K, then $I = K \in \Lambda$ and I is finitely generated.

□

Most of the relevant rings in algebra are Noetherian. An example of rings which are not Noetherian can be the ring of polynomials in infinite variables, $A = k[X_1, X_2, X_3, \ldots, X_n, \ldots]$.

The important Hilbert basis theorem asserts that, if A is Noetherian, there exists a finite number of generators (called 'a basis' back in time) for each ideal of its ring of polynomials $A[X]$, hence $A[X]$ is Noetherian.

Theorem 4 (Hilbert basis Theorem)**.** *If A is a Noetherian ring, then $A[X]$ is a Noetherian ring.*

Proof. Let us show that every ideal $I \subset A[X]$ is finitely generated. Define, for each n, the sets of leading coefficients of polynomials in I:

$$J_n = \{a \in A \ : \ \exists f(X) \in I \text{ such that } f(X) = aX^n + b_{n-1}X^{n-1} + \cdots + b_0\} \subset A.$$

Since I is an ideal of $A[X]$, every J_n is an ideal of A: multiply $a \in J_n$ such that there exists a polynomial $f(X)$ with leading coefficient a, by $b \in A$; the polynomial $bf(X)$ has leading coefficient $ab \in J_n$. And since $f(X) \in I$ implies $Xf(X) \in I$, we get an increasing chain of ideals

$$J_1 \subset J_2 \subset \cdots J_n \subset J_{n+1} \subset \cdots,$$

in A which is Noetherian, then the chain stops at some n. For each index $m \leq n$, the ideal J_m is finitely generated by elements $a_{m1}, a_{m2}, \ldots, a_{mr_m}$, for which there exists polynomials $f_{mi}(X)$ having a_{mi} as its leading coefficient. Let us show that the finite set $\{f_{mi}(X)\}_{m \leq n, 1 \leq i \leq r_m}$ generates the ideal I.

Let $g(X) \in I$ be a polynomial of degree l with leading coefficient c, then $c \in J_l$. If $l \geq n$, $c \in J_l = J_n$ and $c = \sum_i d_i a_{ni}$, with $d_i \in A$, then $g(X) - \sum_i d_i X^{l-n} f_{ni}(X)$ has degree less than l. If, otherwise, $l \leq n$, then $c \in J_l$ and $c = \sum_i d_i a_{li}$, with $d_i \in A$ then $g(X) - \sum_i d_i f_{li}(X)$ has degree less than l. Using induction on l we can decrease the degree to express $g(X)$ as a linear combination of finitely many elements on the desired finite set, hence I is finitely generated and $A[X]$ is Noetherian.

□

Corollary 3. *If A is Noetherian, the rings of polynomials in a finite number of variables, $A[X_1, \ldots, X_n]$ are Noetherian.*

Proof. Use induction on Hilbert's basis Theorem 4. □

Exercise 12. *Show that the nilradical of a noetherian ring is nilpotent.*

1.3.2 Artinian rings

Artinian rings are Noetherian rings with extra conditions.

Definition 23. *Let $\Sigma := (\Sigma, \leq)$ be a partially ordered set. We say that Σ has the **descending chain condition (DCC)** if every chain $\cdots \leq x_n \leq \cdots \leq x_2 \leq x_1$ eventually stops, i.e., there exists an index k such that $\cdots = x_{k+2} = x_{k+1} = x_k$.*

Definition 24. *A ring A is **Artinian** if the set Σ of all ideals in A with the inclusion has the DCC.*

Let us explore certain properties of Artin rings.

Proposition 9. *Let A be an Artin ring. Then:*

(a) Every prime ideal of A is maximal.

(b) The nilradical of A, $\operatorname{nilrad} A$, (Definition 13) equals the Jacobson radical of A, $\mathfrak{R}$, (Definition 14).

(c) A has a finite number of maximal ideals.

(d) The nilradical of A is nilpotent.

Proof. (a) Let $\mathfrak{p} \subset A$ be a prime ideal. Then $A/\mathfrak{p}$ is an integral domain which is also an Artin ring since the DCC holds by (1.3). Given $0 \neq x \in A/\mathfrak{p}$ the chain of principal ideals (x^n) stabilizes, then there exists an integer n such that $(x^n) = (x^{n+1})$ and there exist an element $y \in A/\mathfrak{p}$ such that $x^n = x^{n+1}y$ in an integral domain, then we can cancel x^n to obtain $xy = 1$ and x is a unit in $A/\mathfrak{p}$. Therefore $A/\mathfrak{p}$ is a field and $\mathfrak{p}$ is maximal.

(b) Immediate from (a), Proposition 4 and Definition 14.

(c) Let $\Sigma = \{\mathfrak{m}_1 \cap \cdots \cap \mathfrak{m}_r\}$ the set of all possible finite intersections of maximal ideals, which is a partially ordered set with the inclusion. Since A is Artinian, Σ has a minimal element $\mathfrak{m}_1 \cap \cdots \cap \mathfrak{m}_r$, hence for every other maximal ideal $\mathfrak{m}$ it is

$$\mathfrak{m} \cap \mathfrak{m}_1 \cap \cdots \cap \mathfrak{m}_r = \mathfrak{m}_1 \cap \cdots \cap \mathfrak{m}_r \ ,$$

therefore $\mathfrak{m}_1 \cap \cdots \cap \mathfrak{m}_r \subset \mathfrak{m}$. Let us see that there exists an $\mathfrak{m}_i$ with $\mathfrak{m}_i \subset \mathfrak{m}$. Suppose that, on the contrary, $\mathfrak{m}_i \not\subset \mathfrak{m}$, for every $i = 1, \ldots, r$. Then, there exists elements $x_1 \in \mathfrak{m}_1, \ldots, x_r \in \mathfrak{m}_r$ with $x_i \notin \mathfrak{m}$. But

$$x_1 \cdots x_r \in \mathfrak{m}_1 \cap \cdots \cap \mathfrak{m}_r \subset \mathfrak{m} \ ,$$

and $\mathfrak{m}$ is maximal hence prime, therefore there exists at least an $x_i \in \mathfrak{m}$, contradiction. Then, $\mathfrak{m}_i \subset \mathfrak{m}$ and both are maximal ideals, hence $\mathfrak{m}_i = \mathfrak{m}$, completing the proof.

(d) By the DCC, the chain

$$(\operatorname{nilrad} A)^n = (\operatorname{nilrad} A)^{n+1} = \cdots$$

stabilizes for n, and suppose that $(\operatorname{nilrad} A)^n \neq (0)$. Let Σ be the set of ideals $I \subset A$ such that $I \cdot (\operatorname{nilrad} A)^n \neq (0)$, which is not empty since $\operatorname{nilrad} A \in \Sigma$. Since A is Artinian, Σ has a minimal element J, which is necessarily principal $J = (a)$, such that $(a) \cdot (\operatorname{nilrad} A)^n \neq (0)$. Then,

$$(a) \cdot (\operatorname{nilrad} A)^n \cdot (\operatorname{nilrad} A)^n = (a) \cdot (\operatorname{nilrad} A)^n \neq (0) \ ,$$

hence $(a) \cdot (\operatorname{nilrad} A)^n = (a) = J$, by minimality. Then, there exists an element $b \in (\operatorname{nilrad} A)^n$ with $a = ab$, and form the chain

$$a = ab = ab^2 = ab^3 = \cdots = ab^m = \cdots \ .$$

Since $b \in (\operatorname{nilrad} A)^n \supset \operatorname{nilrad} A$ b is nilpotent, hence $a = 0$ which is a contradiction, therefore $(\operatorname{nilrad} A)^n = (0)$.

□

Next, we introduce the dimension of a ring[1].

Definition 25. *Let A be a ring. Let*

$$\mathfrak{p}_0 \subsetneq \mathfrak{p}_1 \subsetneq \mathfrak{p}_2 \subsetneq \cdots \subsetneq \mathfrak{p}_n \subsetneq A$$

be a strict increasing chain of prime ideals in A. We call its ***length*** *n. We define the* ***dimension of*** *A as the supremum of all possible lengths of chains of prime ideals in A (it can be infinite).*

Example 8. *The dimension of a field k is $\dim k = 0$ because there is only one possible prime ideal (0). In fact, every integral domain of dimension zero is a field.*

The dimension of every PID is $\dim A = 1$. Indeed, since every ideal is principal, the longest possible chain is

$$(0) \subsetneq (a) \subsetneq A$$

with a irreducible and (a) maximal (see Proposition 6). In particular, $\dim \mathbb{Z} = \dim k[X] = 1$, k field. Observe that in a 1-dimensional integral domain, every non-zero prime ideal is maximal.

Using the computation of all prime ideals in Examples 4 and 5, we see that $\dim Z[X] = \dim k[X, Y] = 2$, k a field.

Exercise 13. *Let k be a field. Prove that $\dim k[X_1, \ldots, X_n] = n$.*

The following result characterizes Artinian rings as those which are Noetherian and of dimension zero. Note that it uses material covered later in the course.

Theorem 5. *A ring A is Artinian if and only if A is Noetherian and $\dim A = 0$.*

[1] This is called the Krull dimension of a ring. For other definitions of dimension and relationships between them see [AM, Chapter 10].

Proof. Let A be an Artinian ring. By Proposition 9 (a) every prime ideal is maximal, then $\dim A = 0$. By Proposition 9 (c) let $\mathfrak{m}_1, \ldots, m_r$ the maximal ideals of A. Then

$$\mathfrak{m}_1 \cdot \mathfrak{m}_2 \cdots \mathfrak{m}_r \subset \mathfrak{m}_1 \cap \mathfrak{m}_2 \cap \cdots \mathfrak{m}_r = \mathfrak{R} = \operatorname{nilrad} A$$

by Proposition 9 (c). Hence, by Proposition 9 (d), there exists a $n \in \mathbb{N}$ such that $\mathfrak{m}_1^n \cdot \mathfrak{m}_2^n \cdots \mathfrak{m}_r^n = (\operatorname{nilrad} A)^n = (0)$. Now, consider the chain of ideals

$$A \supset \mathfrak{m}_1 \supset \mathfrak{m}_1^2 \supset \mathfrak{m}_1^n \supset \mathfrak{m}_1^n \cdot \mathfrak{m}_2 \supset \cdots \mathfrak{m}_1^n \cdot \mathfrak{m}_2^n \cdots \mathfrak{m}_r^n \, .$$

Since each quotient between a term and the following one is a vector space over a field $A/\mathfrak{m}_j$, and A is Artinian (hence DCC is satisfied) we have that ACC is satisfied for each quotient. Using recursion on short exact sequences (Proposition 12) DCC for each quotient yields DCC for A, therefore A is Noetherian.

Suppose A is a Noetherian ring of dimension zero. By Theorem 13 the ideal $(0) \subset A$ has a primary decomposition with a finite number of minimal primes, and all of these are maximal ideals $\mathfrak{m}_1, \ldots, \mathfrak{m}_r$, since $\dim A = 0$. By Proposition 4, $\operatorname{nilrad} A = \mathfrak{m}_1 \cap \ldots \cap \mathfrak{m}_r$ and using the Exercise 12, $(\operatorname{nilrad} A)^n = 0$, then $\mathfrak{m}_1^n \cdot \mathfrak{m}_2^n \cdots \mathfrak{m}_r^n = (\operatorname{nilrad} A)^n = (0)$ as in the first part of the proof. Using the similar argument as there relating the quotients in the chain of maximal ideals we obtain that noetherianity and artinianity are equivalent at this level, therefore, A is Artinian. □

A local Artin ring A has a unique maximal ideal $\mathfrak{m}$, which is also the unique prime ideal and equals the nilradical of A. Therefore, since $A = \mathcal{A} \sqcup \mathfrak{m}$, elements of A are either units or nilpotents.

Example 9. *The main examples of local Artin rings are $\mathbb{Z}/(p^n)$ or $k[X]/(f(X)^n)$ with $f(X)$ irreducible. The unique maximal ideal is (the residual class of) (p) and $(f(X))$, respectively. Note that these are not domains if $n > 1$, hence (0) is not a prime ideal.*

Every Artin ring is geometrically the sum of local Artin rings.

Theorem 6. *Every Artin ring is isomorphic (up to unique isomorphism) to a product of local Artin rings.*

Proof. See [AM, Theorem 8.7]. □

Example 10. *The rings $\mathbb{Z}/pq\mathbb{Z}$, p, q distinct primes, are Artin rings since they are Noetherian (they are quotients of $\mathbb{Z}$ which is Noetherian, see Proposition 13 (e)) and of dimension 0 (their ideals are principal (n), with n the residual class mod pq, then every prime ideal is maximal). They are not domains since $pq = 0 \in \mathbb{Z}/pq\mathbb{Z}$, i.e., there are zero-divisors. As Theorem 6 says, these rings decompose as*

$$\mathbb{Z}/pq\mathbb{Z} \simeq \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z}$$

a product of two local Artin rings. Under this isomorphism, the two maximal ideals of $\mathbb{Z}/pq\mathbb{Z}$ are

$$p\mathbb{Z}/pq\mathbb{Z} \simeq (0) \times \mathbb{Z}/q\mathbb{Z}$$

and

$$q\mathbb{Z}/pq\mathbb{Z} \simeq \mathbb{Z}/p\mathbb{Z} \times (0) \, .$$

Chapter 2

Modules

Modules can be thought as the generalization of vector spaces over a field k, when the scalars live in a ring which is not a field. This produces a much richer theory with substantial differences and patologies, which we will explore here.

2.1 General theory of modules

Definition 26. *Let A be a ring. A **module over** A or an A-**module** is the pair consisting on an abelian group M together with an external multiplication by coefficients in A,*

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

satisfying the properties

(a) $a(m+n) = am + an$

(b) $(a+b)m = am + bm$

(c) $(ab)m = a(bm)$

(d) $1_A m = m$

for $a, b \in A$, $m, n \in M$.

Definition 27. *Let M be an A-module. We say that a subset $N \subset M$ is a submodule if for every $a, b \in A$, $m, n \in N$ we have $am + bn \in N$.*

Definition 28. *A map $\psi : M \longrightarrow N$ between two A-modules is a homomorphism of modules if it is A-linear, i.e. if for every $a, b \in A$, $m, n \in M$ we have $\psi(am + bn) = a\psi(m) + b\psi(n)$.*

Let $\operatorname{End} M$ be the (non-commutative) ring of endomorphisms of M, i.e. morphisms of the abelian group M into itself where sum is defined pointwise on each element of M and non-commutative multiplication is composition of endomorphisms. An alternative way of describing

an A-module is by means of the A-linear map

$$\begin{array}{rccc} \xi_a : & M & \longrightarrow & M \\ & m & \mapsto & am \end{array}$$

where condition (a) is equivalent to ξ_a being a homomorphism of abelian groups and conditions (b), (c) and (d) are equivalent to the map $\xi : A \to \operatorname{End} M$, $a \mapsto \xi_a$ being a ring homomorphism.

Exercise 14. *Prove that ξ_a is A-linear and observe that this depends on A being a commutative ring.*

We have that $\xi(A) \subset \operatorname{End} M$. If ξ is injective, then $A \simeq \xi(A)$ and we say that M is a **faithful** A-module. Defining the **annihilator** of M as $\operatorname{Ann}(M) = \{a \in A \ : \ aM = 0\}$, M is faithful if $\operatorname{Ann}(M) = 0$.

Given an endomorphism $\phi : M \to M$ which is A-linear, the subring $\xi(A)[\phi] \subset \operatorname{End} M$ generated by the image of A by ξ, and ϕ, is commutative and makes M also an $\xi(A)[\phi]$-module (here multiplication in the ring $\xi(A)[\phi]$ is identified by composition in $\operatorname{End} M$).

Example 11. *Basic examples of A-modules are the following:*

- *The ring A itself is an A-module.*
- *Every abelian group is a $\mathbb{Z}$-module.*
- *Every ideal $I \subset A$ is an A-module and also a submodule of A.*
- *Every quotient A/I of a ring over an ideal is an A-module.*
- *If $A \subset B$ is an extension of rings, B is an A-module.*
- *Every vector space over a field k is also a k-module.*

Proposition 10. *(1) Let $\psi : M \to N$ be a homomorphism of A-modules. Then $\operatorname{Ker} \psi \subset M$ and $\operatorname{im} \psi \subset N$ are submodules of M and N, respectively.*

(2) If $N \subset M$ is a submodule, the quotient M/N has structure of A-module (with the equivalence relation $m_1 \sim m_2 \Leftrightarrow m_1 - m_2 \in N$) and there exists a surjective homomorphism of A-modules $\mu : M \to M/N$ whose kernel is N.

Proof. Exercise. □

Theorem 7 (Isomorphism theorems for modules)**.** *We have the following three isomorphism theorems for modules:*

(1) Given a homomorphism of A-modules $\psi : M \to N$, it induces an isomorphism of A modules $\overline{\psi} : M/\operatorname{Ker} \varphi \to \operatorname{im} \psi$.

(2) Given submodules $L \subset N \subset M$, we have the isomorphism of A-modules $\frac{M/L}{N/L} \to M/N$.

(3) Given two submodules $N, L \subset M$, we have the isomorphism of modules $N/N\cap L \to N+L/L$.

Proof. Exercise.

(1) Use Proposition 10.

(2) Compute the kernel of the homomorphism of modules $\alpha : M/L \to M/N$ and use (1).

(3) Compute the kernel of the homomorphism of modules $\beta : N \to N + L/L$ and use (1).

□

Definition 29. *Let M be an A-module. Given elements $m_1, \dots, m_r \in M$ we define the* ***submodule generated by*** *$m_1, \dots, m_r$ as*

$$(m_1, \dots, m_r) = \sum_i Am_i = \left\{ \sum_i a_i m_i \in M : a_i \in A \right\} \subset M$$

Given A-modules $M_1, \dots, M_r$, we define its direct sum as

$$M_1 \oplus \cdots \oplus M_r = \{(m_1, \dots, m_r) \ : \ m_i \in M_i\}.$$

In general, given a family of A-modules $\{M_\lambda\}_{\lambda\in\Lambda}$ we define its direct sum $\sum_{\lambda\in\Lambda} M_\lambda$ as the set of tuples $(m_\lambda)_{\lambda\in\Lambda}$ where only a finite number of elements $m_\lambda \neq 0$ for each tuple.

Definition 30. *We say that $(m_\lambda)_{\lambda\in\Lambda}$ is a family of generators of a module M, if the homomorphism of A-modules*

$$\begin{array}{rccc} \psi : A^{\mathrm{card}\Lambda} = & \sum_{\lambda\in\Lambda} A & \longrightarrow & M \\ & (a_\lambda)_{\lambda\in\Lambda} & \mapsto & \sum_{\lambda\in\Lambda} a_\lambda m_\lambda \end{array}$$

is surjective. If ψ is an isomorphism of modules we say that M is ***free*** *and $(m_\lambda)_{\lambda\in\Lambda}$ is a* ***basis*** *of M.*

Definition 31. *We say M is a* ***finite*** *module over A if it is generated over A by a finite number of elements $m_1, \dots, m_r \in M$.*

Example 12. *(a) Let A be a domain and let $0 \neq a \in A\backslash\mathcal{U}(A)$ an element. The ring $A[\frac{1}{a}]$ of polynomials in $\frac{1}{a}$ is an A-module generated by $a^{-1}, a^{-2}, \dots$, which is not finite in general.*

(b) The quotient of a ring by an ideal, A/I is an A-module finitely generated (generated by $1_{A/I}$) but it is not free as an A-module. This is a generalization of the cyclic group $\mathbb{Z}/n\mathbb{Z}$ being an abelian group (i.e. a $\mathbb{Z}$-module)) which is not free.

(c) Let $A = k[X, Y]$ and let $M = (X, Y)$ the A-module generated by these two polynomials. The kernel of the map $\psi : A^2 \to M$, $(f(X, Y), g(X, Y)) \mapsto f(X, Y)X + g(X, Y)Y$, is $\ker\psi = ((h(X, Y)Y, -h(X, Y)X)$, with $h(X, Y) \in A$, therefore M is not free.

(d) The A-module $M = A = k[X]$ is tautologically free. However, we can find a set of generators, for example $M = (X, 1 - X)$ which is not a basis although we cannot remove any of the elements to still generate M.

Remark 3. *The notion of finiteness for modules does match a slightly different notion of finite dimension for us, than the usual one.*

Let k be a field and let M be a k-module which is a k-vector space. If M is finite, then, there exists a finite number of vectors $m_1, \dots m_n \in M$ such that elements of M are linear combinations of these with coefficients in k. This is, for example, the situation in the finite k-algebra $k[X]/(X^3)$, which is a k-vector space of dimension 3 generated by 1, X and X^2. Geometrically, $\operatorname{Spec} k[X]/(X^3)$ *is just one point, the prime ideal (X), over* $\operatorname{Spec} k$ *also a point, and the three dimensions appear in the space of functions $a + bX + cX^2 \in k[X]/(X^3)$ over that point (0), which 'measure' the value at 0, the first and the second derivatives. This is, a finite module is a geometric spectrum of the same dimension as k but with a finite dimensional space of k-functions over it.*

Later in Definition 36 we will see that a k-algebra (which is a also k-module) is finitely generated over k if there exists elements $m_1, \dots m_n \in M$ such that elements of m can be expressed as polynomials in these with coefficients in k. This is the situation of $k[X]$ (or any ring of polynomials in a finite number of variables or quotients of it), where elements in $k[X]$ are polynomials in the single element X. Geometrically this reflects the idea of dimension for the spectra: $\operatorname{Spec} k[X]$ *is the affine line over the point* $\operatorname{Spec} k$*, a space of dimension* 1 *corresponding to one (polynomial) generator.*

2.2 The determinant trick and Nakayama's Lemma

The following result, sometimes known as the **determinant trick**, is a generalization of Cayley-Hamilton Theorem.

Proposition 11. *Let M be a finite A-module generated by $m_1, \dots, m_n \in M$, and let $\phi : M \to M$ be a homomorphism. Suppose that $I \subset A$ is an ideal satisfying $\phi(M) \subset IM$. Then, there exist elements $a_i \in I^i$, $i = 1, 2, \dots, n$ such that the relation*

$$\phi^n + a_1\phi^{n-1} + \cdots + a_{n-1}\phi + a_n = 0$$

holds in the subring $\xi(A)[\phi] \subset \operatorname{End} M$.

Proof. Given that $\phi(M) \subset IM$, for every $i = 1, \dots, n$, we have $\phi(m_i) \in IM$, therefore there exist elements $c_{ij} \in I$ such that $\phi(m_i) = \sum_j c_{ij} m_j$. This can be reformulated as $\sum_j (\delta_{ij}\phi - c_{ij}) m_j = 0$, where each $\delta_{ij}\phi - c_{ij}$ is an endomorphism in $\xi(A)[\phi]$ and δ_{ij} is Kronecker's delta. We denote by Δ the matrix whose (i, j) entries are $\delta_{ij}\phi - c_{ij}$, and by $\operatorname{adj}\Delta$ its adjoint matrix with entries d_{ij}. Pre-multiplying the previous expression by $\operatorname{adj}\Delta$ we have

$$\sum_i d_{ik} \sum_j (\delta_{ij}\phi - c_{ij}) m_j = 0$$

and, given that $(\operatorname{adj}\Delta) \cdot \Delta = \det\Delta \cdot I_n$, we arrive to $(\det\Delta) m_k = 0$, for every k. Given that m_k are generators of M, we get that $\det\Delta = 0 \in \xi(A)[\phi]$ which, expanding the determinant gives the desired result. □

Proposition 11 allows to prove several useful corollaries known as (different versions of) **Nakayama's lemma**.

Corollary 4. *Let M be a finite A-module and let $I \subset A$ be an ideal such that $IM = M$. Then, there exists an element $b \in A$ such that $b \sim 1 \mod I$ (i.e. $b - 1 \in I$) and $bM = 0$.*

Proof. Let $\phi = \mathrm{Id}_M$ be the identity in M. Since $\phi^i = \mathrm{Id}_M^i = \mathrm{Id}_M$, by Proposition 11 there exist elements $a_i \in I^i \subset I$, $i = 1, 2, \ldots, n$ such that $(1 + a_1 + a_2 + \cdots + a_n)\,\mathrm{Id}_M = 0$, from where $b := 1 + a_1 + a_2 + \cdots + a_n$ is the element we look for. □

Corollary 5. *Let $(A, \mathfrak{m})$ be a local ring, let M be a finite A-module. Then $\mathfrak{m}M = M$ implies $M = 0$.*

In general, if $I \subset \mathfrak{R}$ (the Jacobson radical, equivalently $(1 + I) \subset \mathcal{U}(A)$, see Corollary 1), then $IM = M$ implies $M = 0$.

Proof. By Corollary 4, there exists an element $b \in A$ such that $b \in 1 + I$ and $bM = 0$. Hence, $b \in \mathcal{U}(A)$ and therefore $M = 0$. □

Corollary 6. *Let $(A, \mathfrak{m})$ be a local ring, let M be an A-module and let $N \subset M$ be a submodule. Suppose that M/N is a finite module over A and that $M = N + \mathfrak{m}M$. Then, $N = M$.*

In particular, if M is finite over A and $m_1, \ldots, m_n \in M$ are elements (whose images) span the $k = A/\mathfrak{m}$-vector space $M/\mathfrak{m}M$, then $m_1, \ldots, m_n$ generate M as an A-module.

Proof. Observing that $\mathfrak{m}(M/N) = M/N$, by Corollary 5 we get $M/N = 0$ and, then $M = N$. For the second statement, let N be the submodule of M generated by $m_1, \ldots, m_n$. Using the surjective composition $N \to M \to M/\mathfrak{m}M$ we obtain $N + \mathfrak{m}M/M = M$, then $N = M$. □

Nakayama's lemma in this last versions will allow to translate several arguments about modules in commutative algebra of A to local statements for $k = A/\mathfrak{m}$-vector spaces, which are much easier to check.

Exercise 15. *Let $(A, \mathfrak{m})$ be a local ring and let M be a finite A-module. Let $m_1, \ldots, m_n \in M$ be elements and denote their images in the $k = A/\mathfrak{m}$-vector space $M/\mathfrak{m}M$, by $\overline{m_1}, \ldots, \overline{m_n}$. Prove that $\overline{m_1}, \ldots, \overline{m_n}$ is a basis of $M/\mathfrak{m}M$ if and only if $m_1, \ldots, m_n$ are a minimal set of generators of M as an A-module.*

Exercise 16. *Prove that a finitely generated ideal $I \subset A$ satisfying $I = I^2$ is generated by a single idempotent element.*

2.3 Exact sequences of modules

Definition 32. *Let L, M, N be A-modules. We say that the sequence of homomorphisms*

$$L \xrightarrow{\alpha} M \xrightarrow{\beta} N$$

*is **exact** (at M) if $\operatorname{im}\alpha = \operatorname{Ker}\beta$. Equivalently, it is exact if $\beta \circ \alpha = 0$ and every element in the kernel of β is the image of an element of L. A longer sequence of homomorphisms*

$$\cdots \to M_1 \to M_2 \to M_3 \to \cdots$$

is exact if it is exact at each term.

If 0 denotes the zero module, particular cases of exact sequences are

- $0 \to L \xrightarrow{\alpha} M$ iff α is injective
- $M \xrightarrow{\beta} N \to$ iff β is surjective
- $0 \to L \xrightarrow{\alpha} M \xrightarrow{\beta} N$ iff α gives an isomorphism $L \simeq \operatorname{Ker} \beta$
- $L \xrightarrow{\alpha} M \xrightarrow{\beta} N \to$ iff β induces an isomorphism $\operatorname{coker} \alpha := M/\operatorname{im}(L) \simeq N$

The most important case will be the exact sequence

$$0 \to L \xrightarrow{\alpha} M \xrightarrow{\beta} N \to 0,$$

called a **short exact sequence**, equivalent to say that $L \subset M$ and $N = M/L$, under the necessary identifications.

Definition 33. *A short exact sequence $0 \to L \xrightarrow{\alpha} M \xrightarrow{\beta} N \to 0$ is **split** if there exists an isomorphism $M \simeq L \oplus N$ under which we can identify $\alpha(m) = (m, 0)$ and $\beta(l, n) = n$.*

Exercise 17. *Prove that a short exact sequence $0 \to L \xrightarrow{\alpha} M \xrightarrow{\beta} N \to 0$ is split if and only if one of these two equivalent conditions happen:*

(a) There exists a section $s : N \to M$ of β, such that $\beta \circ s = \mathrm{Id}_N$.

(b) There exists a retraction $r : M \to L$ of α, such that $r \circ \alpha = \mathrm{Id}_L$.

Exercise 18. *Let $0 \to L \to M \to N \to 0$ be a short exact sequence of A-modules such that L and N are finite over A. Then, M is finite over A.*

2.4 Noetherian modules

The condition for a module to be Noetherian is similar to the one for rings.

Definition 34. *We say that an A-module M is **Noetherian** if the collection of submodules of M with the inclusion satisfies ACC (Definition 21).*

Using the same argument as in Proposition 8, it is equivalent to say that an A-module M is Noetherian if every non-empty set of submodules has a maximal element, or that every submodule is finite.

There are several properties satisfied by Noetherian modules.

Proposition 12. *Let $0 \to L \xrightarrow{\alpha} M \xrightarrow{\beta} N \to 0$ be a short exact sequence of A-modules. Then, M is Noetherian if and only if L and N are Noetherian.*

Proof. Let $0 \subset L_1 \subset L_2 \subset \cdots \subset L_n \subset \cdots$ be a chain of submodules of L. Taking their images by α, $0 \subset \alpha(L_1) \subset \alpha(L_2) \subset \cdots \subset \alpha(L_n) \subset \cdots$ is a chain of submodules of M which is Noetherian, hence the chain is stationary. Being α injective, this yields a stationary chain in L, hence L is Noetherian. The proof of N Noetherian is similar lifting a chain in N to a chain in M by means of the surjective homomorphism β.

Conversely, let $0 \subset M_1 \subset M_2 \subset \cdots \subset M_n \subset \cdots$ be a chain of submodules of M. Considering $L = \alpha(L) \subset M$, construct the chains

$$0 \subset L \cap M_1 \subset L \cap M_2 \subset \cdots \subset L \cap M_n \subset \cdots$$

of submodules of L, and

$$0 \subset \beta(M_1) \subset \beta(M_2) \subset \cdots \subset \beta(M_n) \subset \cdots$$

of submodules of N, both of which eventually stop by the Noetherian condition of L and N. Let us assume that k is a common index such that $L \cap M_k = L \cap M_{k+1}$ and $\beta(M_k) = \beta(M_{k+1})$. Then, if $m \in M_{k+1}$, $\beta(m) \in \beta(M_{k+1}) = \beta(M_k)$, and let $n \in M_k$ be an element such that $\beta(n) = \beta(m)$, then $\beta(m-n) = 0$, then $m - n \in \operatorname{Ker}\beta \cap M_{k+1}$. Given that $\ker\beta = \operatorname{im}\alpha = L \subset M$, $m - n \in L \cap M_{k+1} = L \cap M_k$, therefore $m \in M_k$, $M_k = M_{k+1}$ and M is Noetherian.

□

Proposition 13. *The following properties hold:*

(a) If M_i, $i = 1, \dots r$, are Noetherian modules, then the direct sum $\bigoplus_{i=1}^{r} M_i$ is Noetherian.

(b) If A is a Noetherian ring, then an A-module M is Noetherian if and only if it is finite over A.

(c) If A is a Noetherian ring and M is a finite A-module, then any submodule is again finite.

(d) If A is a Noetherian ring and $\varphi : A \to B$ is a ring homomorphism such that B is a finite A-module, then B is a Noetherian ring.

(e) If A is a Noetherian ring, every quotient $A[X_1, X_2, \dots, X_n]/I$, where I is an ideal, is Noetherian.

Proof. (a) Take the split short exact sequence $0 \to M_1 \to M_1 \oplus M_2 \to M_2 \to 0$ and Use Proposition 12. Then use induction.

(b) If M is a finite A-module, there exists a surjective homomorphism $A^r \xrightarrow{\beta} M \to 0$ where r is the number of generators de M as an A-module, fitting in a short exact sequence $0 \to \operatorname{Ker}\beta \to A^r \xrightarrow{\beta} M \to 0$. Since A^r is Noetherian by (a), by Proposition 12 M is Noetherian. Conversely, M Noetherian implies that M itself is a finite A-module.

(c) Using (b), M is Noetherian, then any submodule N is a finite A-module.

(d) Using (b), B is a finite A-module, and ideals of B are A-submodules of B, then by (c) submodules are generated by a finite number of elements over A, hence B is Noetherian.

(e) It follows from Hilbert basis Theorem 4 and (d).

□

Exercise 19. *Let A be a noetherian ring and let M be a finite A-module. Show that there exists an exact sequence $A^s \xrightarrow{\alpha} A^r \xrightarrow{\beta} M \to 0$ exhibiting a presentation of M by a finite number of generators and relations.*

Chapter 3

Integral dependence and normal rings

The notion of integral dependence exploits the situation when elements of a ring extension can be generated by a monic polynomial expression. The fact that this relationship is monic allows to use the lowest powers of the expression of basis of the represented element, without inverting the leading coefficient, which is not always possible in a ring. This is closely related with the notion of finiteness for modules, as we will see. Finally, normal rings will be rings which behave like UFDs regarding which are their integral elements.

3.1 Integral dependence and finiteness

Algebras are a special class of A-modules which can be thought as extension of rings to a different ring.

Definition 35. *Let A and B be rings and let $\varphi : A \to B$ be a homomorphism between them. The external product*

$$A \times B \to B\,, \quad (a,b) \mapsto \varphi(a)\cdot b$$

*endows B with a structure of A-module which is compatible with the ring operations in B. We call such ring B an **A-algebra**.*

Example 13. *Every ring A (with unit) is a $\mathbb{Z}$-algebra with the only possible homomorphism $\mathbb{Z} \to A$, $n \mapsto n\cdot 1 = 1+\ldots+1$, hence every ring A is a $\mathbb{Z}$-algebra.*

If $A = k$ is a field, $\varphi : k \to B$ is always injective, hence $k = \varphi(k)$ and a k-algebra contains canonically k as a subring.

*If we have $A \subset B$, B is an A-algebra with the inclusion which will be called an **extension ring**. In these cases we will omit the homomorphism φ and will identify A with $\varphi(A)$.*

Definition 36. *We say that an A-algebra B is **finite over** A if it is finite as an A-module. This means that there exist generators $b_1,\ldots,b_r \in B$ such that every element in B can be written as a linear combination on $b_1,\ldots,b_r$ with coefficients in $\varphi(A)$.*

*We say that an A-algebra B is **finitely generated over** A if there exist generators $b_1,\ldots,b_r \in B$ such that every element in B can be written as a polynomial on $b_1,\ldots,b_r$ with coefficients in $\varphi(A)$.*

Example 14. *If $I \subset A$ is an ideal of a ring A, the quotient homomorphism $\varphi : A \to A/I$ endows A/I with the structure of A-algebra, which is finite over A (generated by the image $\varphi(1_A)$).*

If k is a field, the rings of polynomials $k[X]$, $k[X,Y]$ are k-algebras finitely generated over k, but these are not finite over k: we need infinite monomials to produce all polynomials as linear combinations.

Given an A-algebra B, for each element $b \in B$, there can be different linear or polynomial relations for b with coefficients in A or in $\varphi(A)$: there exists a polynomial

$$f(X) = a_n X^n + a_{n-1} X^{n-1} + \cdots + a_1 X + a_0, \quad a_i \in \varphi(A)$$

such that

$$f(b) = a_n b^n + a_{n-1} b^{n-1} + \ldots + a_1 b + a_0 = 0.$$

If this relation is monic, i.e. the leading coefficient a_n of the polynomial $f(X)$ is $a_n = 1_B = \varphi(1_A)$, then the highest power b^n is a linear combination of the lowest powers $b^{n-1}, \ldots, b, 1_B$ with coefficients in $\varphi(A)$.

Definition 37. *Given an A-algebra B, we say that an element $b \in B$ is **integral over** A if there exists a monic polynomial $f(X) = X^n + a_{n-1}X^{n-1} + \cdots + a_1 X + a_0 \in \varphi(A)[X]$ such that $f(b) = 0$. We say that B is **integral over** A if every element $b \in B$ is integral over A.*

The name integral comes from those numbers that, while not being integers, behave like integers in the sense of being roots of polynomials with integer coefficients without denominators. Let us explain this with a basic example.

Let $A = \mathbb{Z}$. The element $b = \frac{2}{3} \in \mathbb{Q}\backslash\mathbb{Z}$ is root of a polynomial with integer coefficients, for example $f(X) = 3X - 2 \in \mathbb{Z}[X]$. However $b = \frac{2}{3}$ is not integral over $\mathbb{Z}$ because there is no monic polynomial in $\mathbb{Z}[X]$ having $\frac{2}{3}$ as root. In a sense, $b = \frac{2}{3}$ is not an integer by heart. And this is a general situation for any UFD, as the next exercise shows.

Exercise 20. *Let A be an UFD with field of fractions $K = \operatorname{Frac} A$. Prove that no element of $K\backslash A$ is integral over A (hint: prove first for $\mathbb{Z}$ and $\mathbb{Q}$ and then generalize).*

There are, however, integral elements outside $\mathbb{Z}$. For example, all the Gaussian integers $a + bi \in \mathbb{Z}[i]$ satisfy the monic equation $X^2 - 2aX + (a^2 - b^2) = 0$, hence they are integral over $\mathbb{Z}$. The nature and structure of integral elements over a ring is the content of this chapter.

First, let us explore the close relationship between being integral and being finite, for an A-algebra B.

Proposition 14. *Let $\varphi : A \to B$ be an A-algebra and let $b \in B$ be an element. These are equivalent:*

(a) b is integral over A.

(b) The ring $\varphi(A)[b] \subset B$ is a finite $\varphi(A)$-module.

(c) There exists an A-subalgebra $C \subset B$ such that $\varphi(A)[b] \subset C$ and C is a finite $\varphi(A)$-module.

Proof.

(a)⇒(b) By hypothesis, let $f(X) = X^n + a_{n-1}X^{n-1} + \cdots + a_1X + a_0 \in \varphi(A)[X]$ such that $f(b) = 0$, then $b^n = -a_{n-1}b^{n-1} - a_{n-2}b^{n-2} - \cdots - a_1b - a_0$. Therefore, we can also express b^{n+1} as a linear combination of $b^{n-1}, \ldots, b^2, b, 1$:

$$b^{n+1} = b \cdot b^n = b(-a_{n-1}b^{n-1} - a_{n-2}b^{n-2} - \cdots - a_1b - a_0) = -a_{n-1}b^n - a_{n-2}b^{n-1} - \cdots - a_1b^2 - a_0b =$$

$$-a_{n-1}(-a_{n-1}b^{n-1} - a_{n-2}b^{n-2} - \cdots - a_1b - a_0) - a_{n-2}b^{n-1} - \cdots - a_1b^2 - a_0b =$$

$$(a_{n-1}^2 - a_{n-2})b^{n-1} + (a_{n-1}a_{n-2} - a_{n-3})b^{n-2} + \cdots + (a_{n-1}a_2 - a_1)b^2 + (a_{n-1}a_1 - a_0)b + a_{n-1}a_0 \, .$$

By induction, all higher powers b^{n+r}, $r \geq 0$, are generated by $b^{n-1}, \ldots, b^2, b, 1$ and, therefore $\varphi(A)[b]$ is generated by $b^{n-1}, \ldots, b^2, b, 1$ as a $\varphi(A)$-module.

(b)⇒(c) Trivial, just take $C = \varphi(A)[b]$.

(c)⇒(a) Take the homomorphism of finite $\varphi(A)$-modules $\xi_b : C \to C$, $c \mapsto bc$. By Proposition 11 (taking $I = \varphi(A)$) there exist elements $a_i \in \varphi(A)$ such that $\xi_b^n + a_{n-1}\xi_b^{n-1} + \cdots + a_1\xi_b + a_0 = 0$, as an endomorphism of C. If we evaluate this expression at the unit 1_C we have that $\xi_b^i(1_C) = b^i$, therefore we obtain $b^n + a_{n-1}b^{n-1} + \cdots + a_1b + a_0 = 0$, hence b is integral.

□

Corollary 7. *Let $\varphi : A \to B$ be an A-algebra and let $b_1, b_2, \ldots, b_n \in B$ integral elements over A. Then, the ring $\varphi(A)[b_1, b_2, \ldots, b_n]$ is a finite $\varphi(A)$-module.*

Proof. Use induction in Proposition 14 (b). □

Exercise 21. *Let $A \subset B \subset C$ be extension rings i.e. B is an A-algebra and C is both an A-algebra and a B-algebra.*

(a) (finiteness is transitive) If C is a finite B-algebra and B is a finite A-algebra, then C is a finite A-algebra.

(b) (integrality is transitive) If C is integral over B and B integral over A, then C is integral over A.

(c) (finitely generated + integral = finite) If $b_1, \ldots, b_n \in B$ are integral over A then the finitely generated A-algebra $A[b_1, \ldots, b_n]$ is finite over A. In particular, $A[b_1, \ldots, b_n]$ is integral over A.

Example 15. *The concept of integral element coincides with the finiteness of the module structure since finiteness can be seen geometrically. Consider the homomorphism*

$$k[X] \to k[X, Y]/(Y^2 - X)$$

given by composition of the inclusion in $k[X, Y]$ and the quotient, which exhibits $k[X, Y]/(Y^2 - X)$ as a $k[X]$ algebra. The element $Y \in k[X, Y]/(Y^2 - X)$ is integral over $k[X]$ because the monic

polynomial $f(W) = W^2 - X \in k[X][W]$ (in the ring of polynomials in one variable with coefficients in $k[X]$) satisfies $f(Y) = 0 \in k[X,Y]/(Y^2 - X)$. Then, by Proposition 14, $k[X,Y]/(Y^2 - X)$ is generated by 1 and Y as a $k[X]$-module, hence it is a finite $k[X]$-module. In fact, using that $X = Y^2$ it is easy to see that $k[X,Y]/(Y^2 - X)$ is a rank 2 free $k[X]$-module, because its elements can be written uniquely as $g(X) + Yh(X)$, with $g(X), h(X) \in k[X]$.

Geometrically, this means that the parabola $Z := \{(x,y) \in k^2 \ : \ y^2 - x = 0\}$ maps $2:1$ to the affine line of ring of functions $k[X]$, where coordinate y can take the two square root values for each x. This is to say that, for each point $(y, x = y^2)$ in the parabola, the polynomial $f(X,Y) = g(X) + Yh(X) \in k[X,Y]/(Y^2 - X)$ takes two values in the X-axis given by the two polynomials $g(X), h(X) \in k[X]$.

Given an A-algebra B, the set of integral elements is a ring itself: if $b_1, b_2 \in B$ are integral over A, $A[b_1, b_2]$ is a finite $\varphi(A)$-module (Corollary 7) which contains $b_1 + b_2$ and $b_1 \cdot b_2$, then these latter two elements are integral over A (Proposition 14 (c)).

Exercise 22. *Given an A-algebra B, and two elements $b_1, b_2 \in B$ integral over A satisfying monic quadratic polynomials with coefficients in A, find explicit monic polynomials over A satisfied by the elements $b_1 + b_2$ and $b_1 \cdot b_2$.*

Definition 38. *Given an A-algebra B, the ring of integral elements is called the **integral closure of A in B**, denoted by $\widetilde{A}$. If $A = \widetilde{A}$, we say that A is integrally closed in B.*

*We say that an integral domain A is **normal** if it is integrally closed in its ring of fractions, i.e. $A = \widetilde{A} \subset \mathrm{Frac}(A)$. The integral closure of A in its ring of fractions $\mathrm{Frac}(A)$ is called the **normalization** of A.*

Example 16. *Observe that, if A is an UFD then A is normal (see Exercise 20).*

Exercise 23. *Show that $\widetilde{A}$ is actually a closure, this is $\widetilde{\widetilde{A}} = \widetilde{A}$, i.e. if an element $b \in B$ is integral over $\widetilde{A}$, then $b \in \widetilde{A}$.*

Example 17. *(**Cuspidal curve**) Let us see an example of a domain which is not an UFD nor a normal ring.*

Let k be an algebraically closed field and let $k[X,Y]/(Y^2 - X^3)$ be the ring of polynomial functions of the curve $Z = \{(x,y) \in k^2 \ : \ y^2 - x^3 = 0\}$. It is a domain because $Y^2 - X^3 \in k[X,Y]$ is an irreducible element in an UFD, hence the ideal $(Y^2 - X^3)$ is prime.

On the other hand, $k[X,Y]/(Y^2 - X^3)$ is not a UFD, because the element $Y^2 = X^3$, seen in the quotient, admits two different decomposition into irreducibles. Equivalently, $X, Y \in k[X,Y](Y^2 - X^3)$ are irreducible elements but they are not prime, because X divides $Y \cdot Y = Y^2$ (because $Y^2 = X^3$) but X does not divide Y.

Now, we observe that $k[X,Y]/(Y^2 - X^3) \simeq k[t^2, t^3]$. To do this, consider the homomorphism

$$\begin{array}{rccc} \phi: & k[X,Y]/(Y^2 - X^3) & \to & k[t^2,t^3] \\ & f(X,Y) & \mapsto & f(t^2,t^3) \end{array}$$

which is clearly surjective. Suppose that there exists a polynomial $f(X,Y) \in k[X,Y]/(Y^2 - X^3)$ such that $f(t^2,t^3) = 0$. We replace each monomial in $f(X,Y)$ containing Y^2 by X^3, then we can

write $f(X,Y)$ *as* $f(X,Y) = g(X) + Yh(X)$ *in* $k[X,Y]/(Y^2 - X^3)$. *Applying* ϕ *we get*

$$\phi(f(X,Y)) = \phi(g(X) + Yh(X)) = g(t^2) + t^3 h(t^2) = 0$$

which forces $g = h = 0$ *by matching the degrees. Hence,* $\ker \phi = 0$ *and we get the desired isomorphism. Note that* $t = Y/X$ *under the isomorphism* ϕ.

Next, it is easy see that the field of fractions $\operatorname{Frac} k[X,Y]/(Y^2 - X^3) \simeq \operatorname{Frac} k[t^2, t^3] = k(t)$, *i.e. the field of fractions* $\frac{f(t)}{g(t)}$, $g(t) \neq 0$, *given that* t *and* $\frac{1}{t}$ *can appear as quotients of polynomials in* $k[t^2, t^3]$.

Finally, note that $W^2 - X = 0$ *and* $W^3 - Y = 0$ *are monic polynomials in* $k[X,Y]/(Y^2 - X^3)[W]$ *(the ring of polynomials in the variable* W *with coefficients in* $k[X,Y]/(Y^2 - X^3)$*) having* $t = Y/X \in \operatorname{Frac} k[X,Y]/(Y^2 - X^3)$ *as a root. Therefore* t *is integral over* $k[X,Y]/(Y^2 - X^3)$. *However, clearly,* $t \notin k[X,Y]/(Y^2 - X^3)$. *In consequence,* $k[X,Y]/(Y^2 - X^3)$ *is not normal.*

Given that the normalization of $k[X,Y]/(Y^2 - X^3) \simeq k[t^2, t^3]$ *has to contain this element* t *and clearly* $k[t^2, t^3][t] \simeq k[t]$ *is normal (because it is a UFD), we conclude that the normalization of* $k[X,Y]/(Y^2 - X^3)$ *is* $k[t] = k[Y/X]$.

Remark 4. *Later in the course we will understand why the ring of polynomial functions of the cuspidal curve* $Z = \{(x,y) \in k^2 \ : \ y^2 - x^3 = 0\}$ *in Example 17 is not normal because of its singularity, and why its normalization* $k[t]$ *is the ring of polynomials of the affine line, which is a resolution of its singularity (a minimal non-singular curve most similar to* Z*).*

Exercise 24. *Use the arguments in Example 17 to study whether* $k[X,Y]/(Y^2 - X^2 - X^3)$, *with* k *algebraically closed, is normal or not, and compute its normalization in the latter case. This ring contains the polynomial functions of what we call the* ***nodal curve****.*

3.2 Noether normalization Lemma

The normalization lemma by Noether is a structure theorem stating that finitely generated k-algebras decompose as two extensions, one finitely generated which is a normal ring of polynomials, and another one integral over it. This normalizes a finitely generated k-algebra by expressing it as a finite module over a normal ring. Geometrically, this exhibits the spectrum of a finitely generated k-algebra as a finite covering over a normal spectrum.

Definition 39. *Let* A *be a* k*-algebra. We say that elements* $a_1, \ldots, a_n \in A$ *are* ***algebraically independent*** *over* k *if the kernel of the surjective homomorphism*

$$\begin{array}{rccc} \phi: & k[X_1, \ldots, X_n] & \to & k[a_1, \ldots, a_n] \\ & f(X_1, \ldots, X_n) & \mapsto & f(a_1, \ldots, a_n) \end{array}$$

is zero, i.e. ϕ *is an isomorphism, or, equivalently, there do not exist polynomial relations such that* $f(a_1, \ldots, a_n) = 0$.

Theorem 8 (Noether normalization lemma). *Let* k *be an infinite field and let* A *be a finitely generated* k*-algebra. Then, there exist elements* $a_1, \ldots, a_n \in A$ *algebraically independent over* k *such that* A *is integral over* $k[a_1, \ldots, a_n]$.

Proof. Let $b_1, \dots b_n \in A$ generators of A as a k-algebra. The proof goes by induction on the number n of generators.

If $n = 1$, either b_1 is algebraically independent over k, then we are done, or there exists a polynomial $f(X_1) \in k[X_1]$ such that $f(b_1) = 0$. By inverting, if necessary, the leading coefficient of f, we can assume f is monic, therefore b_1 hence A are integral over k, and we are done.

Now assume that the theorem holds for $n-1$ generators. If $b_1, \dots b_n$ are algebraically independent we are done, then suppose that there exists a polynomial $f(X_1, \dots, X_n) \in k[X_1, \dots, X_n]$ such that $f(b_1, \dots, b_n) = 0$. If d is the degree of f, we can write

$$f(X_1, \dots, X_n) = f_d(X_1, \dots, X_n) + \text{ lower order terms}$$

where f_d is the homogeneous degree d part of f. For any tuple of elements $\lambda_1, \dots, \lambda_{n-1} \in k$, we can modify the variables to have

$$f(X_1 + \lambda_1 X_n, X_2 + \lambda_2 X_n, \dots, X_{n-1} + \lambda_{n-1} X_n, X_n) =$$

$$f_d(\lambda_1, \lambda_2, \dots, \lambda_{n-1}, 1) X_n^d + \text{ other terms of lower degree in } X_n$$

The leading coefficient of this polynomial is the evaluation of $f_d(X_1, X_2, \dots, X_{n-1}, 1)$ (which is a polynomial in $k[X_1, X_2, \dots, X_{n-1}]$) at $\lambda_1, \lambda_2, \dots, \lambda_{n-1}$, which is a non-zero polynomial. Then, since k is infinite, we can find a tuple of elements $\lambda_1, \dots, \lambda_{n-1} \in k$ such that $f_d(\lambda_1, \lambda_2, \dots, \lambda_{n-1}, 1) \neq 0$ and, moreover, we can assume that $f_d(\lambda_1, \lambda_2, \dots, \lambda_{n-1}, 1) = 1$ after multiplying f by a constant.

As a consequence, choose new generators for A as a k-algebra, given by

$$b_1^* := b_1 + \lambda_1 b_n \ , \ b_2^* := b_2 + \lambda_2 b_n \ , \ \dots \ , \ b_{n-1}^* := b_{n-1} + \lambda_{n-1} b_n \ , \ b_n \ ,$$

and note that b_n is integral over $A' := k[b_1^*, b_2^*, \dots, b_{n-1}^*]$ with the monic polynomial f. Given that A' is a k-algebra finitely generated by $n-1$ elements, by induction hypothesis there exists elements $a_1, \dots, a_{n-1} \in A'$, algebraically independent over k, such that A' is integral over $k[a_1, \dots, a_{n-1}]$. By transitivity of the integral condition (Exercise 21)

$$A = k[b_1, \dots, b_{n-1}, b_n] = A[b_1^*, \dots, b_{n-1}^*, b_n] = A'[b_n]$$

is integral over $k[a_1, \dots, a_{n-1}]$, completing the proof. □

Exercise 25. *Let $k = \mathbb{F}_q$ be the finite field of q elements. Find an example of a polynomial $f(X, Y) \in k[X, Y]$ such that for every element $\lambda \in K$, the ring $k[X, Y]/(f(X, Y))$ is not finitely generated as a module over $k[X + \lambda Y]$. This shows that the proof we have given of Noether normalization lemma (Theorem 8) does not work in general for finite fields.*

Remark 5. *A more general proof for k not necessarily infinite can be found in [Re, Section 4.6].*

The geometric meaning of Noether normalization lemma is illustrated by this example.

Example 18. *Let $A = k[X, Y](XY - 1)$, which is the ring of coordinates of a hyperbola, be a finitely generated k-algebra, generated by X and Y. The second generator Y is algebraic over $k[X]$ (or algebraically dependent on X) because the polynomial $f(W) = XW - 1 \in k[X][W]$, where W*

is the variable and the coefficients live in $k[X]$, vanishes over $W = Y$. However, Y is not integral over $k[X]$: indeed any monic polynomial $W^n + f_{n-1}(X)W^{n-1} + \cdots + f_1(X)W + f_0(X) \in k[X][W]$ evaluated at $W = Y$ cannot cancel because the degree on $Y = \frac{1}{X}$ can never be zero. Geometrically this happens because the hyperbola does not project surjectively onto the X-axis (whose ring of functions in $k[X]$).

Noether normalization Theorem 8 says that we can modify the generator X by a linear combination, say to $X^* = X + \lambda Y$, such that the relation turns out to be

$$XY - 1 = 0 \Leftrightarrow (X^* - \lambda Y)Y - 1 = 0 \Leftrightarrow -\lambda Y^2 + X^*Y - 1 = 0 \, ,$$

which (after multiplying by $-1/\lambda$) is a monic polynomial in $k[X^*][W]$ having Y as a root. Then this exhibits Y as an integral element over $k[X^*]$. The geometric meaning of this is the effect of tilting the hyperbola to the axes (X^*, Y) and then projecting surjectively onto the X^* axis, i.e. to the normal affine line.

The situation is different with the ring of functions of the parabola, $k[X,Y]/(Y^2 - X)$ where Y is integral over $k[X]$ (see Example 15). Projecting onto the affine line

$$\operatorname{Spec} k[X,Y]/(Y^2 - X) \longrightarrow \operatorname{Spec} k[X]$$

is given by the homomorphism of rings

$$k[X] \longrightarrow k[X,Y]/(Y^2 - X) \, , f(X) \mapsto f(X) + (Y^2 - X)$$

The ideal $(Y^2 - a^2) = (X - a^2) \in k[X,Y]/(Y^2 - X)$ is not prime: it is a reducible polynomial corresponding to the product of two maximal ideals $(Y - a)$, $(Y + a)$, which is the union of the points $(a^2, \pm a) \in Z = \{(x,y) \in k^2 \ : \ y^2 - x = 0\}$. This ideal projects into the maximal ideal $(X - a^2) \in k[X]$, which is a point. This reflects the $2:1$ finite surjective map from the parabola to the affine line.

More generally, if k is algebraically closed and $Z = f(X_1, \ldots, X_n) = 0$ is a hypersurface (i.e. an algebraic relation between $X_1, \ldots, X_n$), there exists an affine hyperplane $H \subset k^n$ (whose ring of functions is certain $k[a_1, \ldots, a_{n-1}]$ and a linear map $\phi : k^n \to H$ such that $\phi(Z)$ maps surjectively onto H.

Exercise 26. *Let k be a field and let $A = k[X,Y,Z]/(X^2 - Y^3 - 1, XZ - 1)$. Find elements $a, b \in k$ such that A is integral over $B = k[X + aY + bZ]$ finding a finite set of generators of A as a B-module. Try to picture this geometric situation (use computer software if necessary).*

Chapter 4

Geometry of the spectrum of a ring

4.1 Weak Hilbert's Nullstellensatz

We will use Noether's normalization lemma (Theorem 8) to give a first and weaker version of the Nullstellensatz (or Hilbert's zeroes theorem) which will be further explored in the next sections.

Proposition 15. *Let A, B domains and suppose that $A \subset B$ is an integral extension of rings. Then A is a field if and only if B is a field.*

Proof. Exercise. □

Theorem 9 (Weak Nullstellensatz). *Let k, K be fields such that K is a finitely generated k-algebra. Then K is algebraic over k and $k \subset K$ is an algebraic field extension of finite degree.*

Proof. By Noether normalization Theorem 8, there exists algebraically independent elements $a_1, \dots, a_n$ such that K is integral over $k[a_1, \dots, a_n]$. By Proposition 15 the ring $k[a_1, \dots, a_n]$ must be a field, then $n = 0$ and K is already integral and finite over k. □

Corollary 8. *Let k be a field and let $k[X_1, \dots, X_n]$ be the ring of polynomials in n variables with coefficients in k. For every maximal ideal $\mathfrak{m} \in k[X_1, \dots, X_n]$, the residue field $k[X_1, \dots, X_n]/\mathfrak{m}$ is a finite algebraic field extension of k.*

Proof. This is a direct consequence of Theorem 9. □

Example 19. *Two basic examples of this fact are:*

(a) Let $f(X) = X^2+1 \in \mathbb{R}[X]$ which is an irreducible polynomial in a UFD, hence $\mathfrak{m} = (X^2+1)$ is a prime and maximal ideal and $\mathbb{R}[X]/(X^2+1)$ is a field isomorphic to $\mathbb{C}$, yielding the degree 2 extension $\mathbb{R} \subset \mathbb{C}$. This can be seen by considering the evaluation map

$$\begin{array}{rccc} ev: & \mathbb{R}[X] & \to & \mathbb{R}[X]/(X^2+1) \\ & f(X) & \mapsto & f(\sqrt{-1}) = f(i) \end{array}$$

where we identify $\sqrt{-1} = i$ with the residual class of X in $\mathbb{R}[X]/(X^2+1)$. This way, $\mathbb{R}[X]/(X^2+1) \simeq \mathbb{R}[i] \simeq \mathbb{C}$.

(b) A similar example can be constructed with the extension $\mathbb{Q}[X] \hookrightarrow \mathbb{Q}[X]/(X^3-2)$. *Then,* $\mathbb{Q} \subset \mathbb{Q}[X]/(X^3-2) \simeq \mathbb{Q}(\sqrt[3]{2})$ *is a degree* 3 *algebraic extension, which is a* $\mathbb{Q}$*-vector space of dimension* 3 *with basis* $(1, \sqrt[3]{2}, \sqrt[3]{2^2})$.

This allows, when k is an algebraically closed field, to characterize all maximal ideals.

Corollary 9. *Let* k *be an algebraically closed field and let* $k[X_1, \dots, X_n]$ *be the ring of polynomials in* n *variables with coefficients in* k. *Every maximal ideal* $\mathfrak{m} \in k[X_1, \dots, X_n]$ *is of the form* $\mathfrak{m} = (X_1 - a_1, \dots, X_n - a_n)$ *where* $a_1, \dots, a_n \in k$.

Proof. By Corollary 8, the residue field $k[X_1, \dots, X_n]/\mathfrak{m}$ is a finite algebraic extension of k, which is algebraically closed, hence $k[X_1, \dots, X_n]/\mathfrak{m} \simeq k$. Let $a_1, \dots, a_n \in k$ be the elements image of $X_1, \dots, X_n$ under the projection $\pi : k[X_1, \dots, X_n] \to k[X_1, \dots, X_n]/\mathfrak{m}$. Given that $a_i \in k \subset k[X_1, \dots, X_n]$, under π, we have also $\pi(a_i) = \pi(X_i) = a_i$, therefore $X_i - a_i \in \mathfrak{m}$, for each i. Hence, $(X_1 - a_1, \dots, X_n - a_n) \subset \mathfrak{m}$ but $(X_1 - a_1, \dots, X_n - a_n)$ is already maximal, therefore $(X_1 - a_1, \dots, X_n - a_n) = \mathfrak{m}$. □

When k is algebraically closed, the evaluation map is

$$\begin{array}{rccc} \mathrm{ev}_{(a_1,\dots,a_n)} : & k[X_1, \dots, X_n] & \to & k[X_1, \dots, X_n]/\mathfrak{m} \simeq k \\ & f(X_1, \dots, X_n) & \mapsto & f(a_1, \dots, a_n) \end{array}$$

Corollary 9 shows that, if k is algebraically closed, there is a bijective correspondence between points of the n-dimensional k-affine space $(a_1, \dots, a_n) \in k^n$ and maximal ideals $\mathfrak{m} = (X_1 - a_1, \dots, X_n - a_n) \subset k[X_1, \dots, X_n]$:

$$k^n \overset{1:1}{\longleftrightarrow} \operatorname{Specmax} k[X_1, \dots, X_n]$$

4.2 Algebraic varieties

Definition 40. *Let* k *be a field. Let* $J \subset k[X_1, \dots, X_n]$ *be an ideal. The* ***variety*** $Z \subset k^n$ *defined by* J *is*

$$Z = V(J) := \{(a_1, \dots, a_n) \in k^n \ : \ f(a_1, \dots, a_n) = 0 \ , \ \forall f(X_1, \dots, X_n) \in J\}$$

Given that $k[X_1, \dots, X_n]$ *is noetherian,* J *is finitely generated as* $J = (f_1, \dots, f_r)$, *then* Z *is the common set of zeros of the polynomials* $f_1, \dots, f_r$.

Proposition 16. *Let* k *be an algebraically closed field, let* $J \subset k[X_1, \dots, X_n]$ *be an ideal and let* $V(J)$ *be the variety defined by* J. *Every maximal ideal of* $A := k[X_1, \dots, X_n]/J$ *is of the form* $\mathfrak{m} = (x_1 - a_1, \dots, x_n - a_n)$ *where* $x_i = X_i \mod J$ *and* $(a_1, \dots, a_n) \in V(J)$.

Proof. We know that the ideals of $k[X_1, \dots, X_n]/J$ are ideals of $k[X_1, \dots, X_n]$ containing J (see 1.3). Then, maximal ideals of $k[X_1, \dots, X_n]/J$ are maximal ideals $(X_1 - a_1, \dots, X_n - a_n) \subset k[X_1, \dots, X_n]$, such that $J \subset (X_1 - a_1, \dots, X_n - a_n)$, which can be written as $(x_1 - a_1, \dots, x_n - a_n)$ where $x_i = X_i \mod J$.

Now, since $(X_1 - a_1, \dots, X_n - a_n)$ is the kernel of the evaluation $\mathrm{ev}_{(a_1,\dots,a_n)}(f(X_1, \dots, X_n)) = f(a_1, \dots, a_n)$ and $J \subset (X_1 - a_1, \dots, X_n - a_n)$, for every $g(X_1, \dots, X_n) \in J$, $g(a_1, \dots, a_n) = 0$, which is equivalent to $(a_1, \dots, a_n) \in V(J)$. □

Proposition 16 shows that, if k is algebraically closed, there is a bijective correspondence between points of variety $(a_1, \dots, a_n) \in V(J) \subset k^n$ and maximal ideals $\mathfrak{m} = (x_1 - a_1, \dots, x_n - a_n) \subset k[X_1, \dots, X_n]/J$:

$$V(J) \overset{1:1}{\longleftrightarrow} \operatorname{Specmax} k[X_1, X_2, \dots, X_n]/J$$

Remark 6. *If k is not algebraically closed, given an ideal $J \subset k[X_1, \dots, X_n]$ and a finite algebraic field extension $k \subset K$ we define a K-**valued point** of $V(J)$ as a point $(a_1, \dots, a_n) \in K^n$ such that $f(a_1, \dots, a_n) = 0$ for every $f(X_1, \dots, X_n) \in J$. The maximal ideals of $k[X_1, \dots, X_n]$ are given by*

$$\mathfrak{m} = (X_1 - a_1, \dots, X_n - a_n) \cap k[X_1, \dots, X_n]$$

For example, the variety $V(X^2 + 1) \subset \mathbb{R}$ is empty. However, it has two $\mathbb{C}$-valued points $\pm i \in \mathbb{C}$ for the degree 2 extension $\mathbb{R} \subset \mathbb{C}$, whose maximal ideals in $\mathbb{C}[X]$ are $(X - i)$, $(X + i)$, whose intersections with $\mathbb{R}[X]$ are both the maximal ideal $(X^2 + 1) \subset \mathbb{R}[X]$.

Let k be a field. We have the following operators between ideals $J \subset k[X_1, \dots, X_n]$ and subsets $Z \subset k^n$

$$\{J \subset k[X_1, \dots, X_n]\} \underset{I}{\overset{V}{\rightleftarrows}} \{X \subset k^n\} \tag{4.1}$$

where

- given $J \subset k[X_1, \dots, X_n]$,

  $$V(J) = \{(a_1, \dots, a_n) \in k^n \ : \ f(a_1, \dots, a_n) = 0 \ , \ \forall f(X_1, \dots, X_n) \in J\}$$

  is the variety of the ideal J.

- given a subset $Z \subset k^n$,

  $$I(Z) = \{f \in k[X_1, \dots, X_n] \ : \ f(a_1, \dots, a_n) = 0 \ , \ \forall (a_1, \dots, a_n) \in Z\}$$

  is the ideal of the subset X.

The exercise shows several properties of these two operators.

Exercise 27. *Check the following properties:*

(a) For every subset $Z \subset k^n$, $I(Z)$ is an ideal.

(b) Given ideals $J \subset K \subset k[X_1, \dots, X_n]$, then $k^n \supset V(J) \supset V(K)$.

(c) Given subsets $Z \subset W \subset k^n$, then $k[X_1, \dots, X_n] \supset I(Z) \supset I(W)$.

(d) For every subset $Z \subset k^n$, we have $Z \subset V(I(Z))$ and equality holds if and only if Z is a variety (i.e. $Z = V(J)$).

(e) For every ideal $J \subset k[X_1, \dots, X_n]$, we have $J \subset I(V(J))$, and equality does not hold in general.

Let us define a topology on k^n, called the **Zariski topology**.

Proposition 17. *The set of varieties $V(J) \subset k^n$ are the closed sets of a topology on k^n, called the **Zariski topology** on k^n.*

Proof. Clearly the total space $k^n = V((0))$ and the empty set $\emptyset = V(k[X_1, \dots, X_n])$ are varieties.

The (finite) union of varieties is a variety given that

$$V(J) \cup V(K) = V(J \cap K) = V(JK) \, .$$

Indeed, let $a \in V(J) \cup V(K)$ and let $f \in J \cap K$, which is an ideal. If $a \in V(J)$ then, since $f \in J$, we get $f(a) = 0$ (similarly, if $a \in V(K)$ then, since $f \in K$, we get $f(a) = 0$), hence $a \in V(J \cap K)$. This shows $V(J) \cup V(K) \subset V(J \cap K)$. Since $JK \subset J \cap K$ we have $V(J \cap K) \subset V(JK)$. Now let a be a point in $V(JK) \backslash V(J)$ and let us check that $a \in V(K)$. Let $f \in K$. Since, $a \notin V(J)$, let $g \in J$ such that $g(a) \neq 0$. Then, given that $a \in V(JK)$ and $gf \in JK$ we have $(gf)(a) = g(a)f(a) = 0$. Since $g(a) \neq 0$ therefore $f(a) = 0$ and $a \in V(K)$. This shows $V(JK) \subset V(J) \cup V(K)$ and completes the proof of $V(J) \cup V(K) = V(J \cap K) = V(JK)$. Since $J \cap K$ and JK are ideals, the union $V(J) \cup V(K)$ is a closed set.

Given a family of varieties $\{V(J_\lambda)\}_{\lambda \in \Lambda}$, the (arbitrary) intersection is a variety given that

$$\bigcap_{\lambda \in \Lambda} V(J_\lambda) = V\left(\sum_{\lambda \in \Lambda} J_\lambda \right) .$$

Indeed, let $a \in \bigcap_{\lambda \in \Lambda} V(J_\lambda)$ and let $f_{\lambda_1} + \cdots + f_{\lambda_s} \in \sum_{\lambda \in \Lambda} J_\lambda$, $f_{\lambda_l} \in J_\lambda$. Since $a \in V(J_\lambda)$, $f_{\lambda_l}(a) = 0$, then $(f_{\lambda_1} + \cdots + f_{\lambda_s})(a) = 0$ and $a \in V\left(\sum_{\lambda \in \Lambda} J_\lambda\right)$. Conversely, let $a \in V\left(\sum_{\lambda \in \Lambda} J_\lambda\right)$. Since $J_\lambda \subset \sum_{\lambda \in \Lambda} J_\lambda$ we have $V\left(\sum_{\lambda \in \Lambda} J_\lambda\right) \subset V(J_\lambda)$ for every $\lambda \in \Lambda$, completing the equality $\bigcap_{\lambda \in \Lambda} V(J_\lambda) = V\left(\sum_{\lambda \in \Lambda} J_\lambda\right)$. Since the sum $\sum_{\lambda \in \Lambda} J_\lambda$ is an ideal, the intersection $\bigcap_{\lambda \in \Lambda} V(J_\lambda)$ is a closed set. □

Let us see some features of this topology:

- Its open sets are the complements of varieties. For example, complements of the zero locus in the the plane $\mathbb{C}^2$ of a complex curve $f(X, Y) \in \mathbb{C}[X, Y]$. Note that open sets are quite big in this topology.
- It is weaker than the euclidean topology in $\mathbb{R}^n$ or $\mathbb{C}^n$, because varieties are closed in the euclidean topology (these are zeroes of polynomials, which are continuous functions), but there ar plenty of closed sets in $\mathbb{R}^n$ or $\mathbb{C}^n$ which are not varieties (for example, closed balls).
- Zariski topology is not T_2 or Hausdorff, because every two open sets have non-empty intersection.
- It is T_1 or Frechet, because singletons are varieties, which are closed sets: $\{(a_1, \dots, a_n)\} = V((X_1 - a_1, \dots, X_n - a_n))$, corresponding to maximal ideals.
- The open subsets $D(f) := k^n \backslash V((f(X_1, \dots, X_n)))$ (complements of hypersurfaces) are a basis of the Zariski topology.

Exercise 28. *Check the details of these properties.*

Definition 41. *We say that a topological space is* ***noetherian*** *if any chain of closed subsets eventually stops (this is called the* ***decreasing chain condition (DCC)****).*

The following proposition shows that the Zariski topology on k^n is noetherian, matching with the idea of its associated ring $k[X_1, \dots, X_n]$ being noetherian and noetherianity as finite dimensionality.

Proposition 18. *The Zariski topology on k^n is noetherian. In particular, any non-empty set of varieties in k^n has a minimal element.*

Proof. Given a decreasing chain of varieties

$$k^n \supset V(J_1) \supset V(J_2) \supset \cdots V(J_n) \supset \cdots$$

we obtain an increasing chain of ideals

$$I(k^n) = (0) \subset I(V(J_1)) \subset I(V(J_2)) \subset \cdots \subset I(V(J_n)) \subset \cdots k[X_1, \dots, X_n]$$

which stabilizes because $k[X_1, \dots, X_n]$ is noetherian and has the (ACC). Then, $I(V(J_n)) = I(V(J_{n+1}))) = \cdots$, hence $V(I(V(J_n))) = V(I(V(J_{n+1}))) = \cdots$. Given that $V(J_i)$ are varieties, using Exercise 27, we have that $V(J_n) = V(J_{n+1}) = \cdots$ and the decreasing chain of varieties stabilizes. □

4.3 Hilbert's Nullstellensatz

The correspondence (4.1) is not bijective. For example, over a non-algebraically closed field such as $\mathbb{R}$, the empty variety $\emptyset \subset \mathbb{R}$ corresponds to several ideals in $\mathbb{R}[X]$, $(X^2 + 1)$, $(X^2 + 2)$, $(X^2 - X - 2) \dots$. Even in an algebraically closed field such as $\mathbb{C}$, ideals (X), (X^2), $(X^3) \subset \mathbb{C}[X, Y]$ correspond to the same algebraic variety, the Y-axis. But, in this latter case, these ideals are not that different, they share the same radical. Hilbert's Nullstellensatz says that, over an algebraically closed field, the former case cannot happen and also that we can modify (4.1) to get a bijection between varieties and radical ideals.

Theorem 10 (Hilbert's Nullstellensatz). *Let k be an algebraically closed field and let $k[X_1, \dots, X_n]$ be the ring of polynomials with coefficients in k. Then:*

(a) If $J \subsetneq k[X_1, \dots, X_n]$, then $V(J) \neq \emptyset$.

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

Proof. (a) If $J \subsetneq k[X_1, \dots, X_n]$, then there exists a maximal ideal $\mathfrak{m}$ such that $J \subset \mathfrak{m} \subsetneq k[X_1, \dots, X_n]$. By Corollary 9, it is $\mathfrak{m} = (X_1 - a_1, \dots, X_n - a_n)$, where $(a_1, \dots a_n) \in k^n$, then $(a_1, \dots, a_n) \in V(J)$ and $V(J) \neq \emptyset$.

(b) We will use the so-called Rabinowitch trick. Let $f(X_1,\dots,X_n) \in I(V(J))$, i.e. a polynomial in $k[X_1,\dots,X_n]$ such that $f(a_1,\dots,a_n)=0$ for every $(a_1,\dots,a_n)\in V(J)$. Let Y be a new variable and consider the ideal $J'=(J, f(X_1,\dots,X_n)Y-1)\subset k[X_1,\dots,X_n,Y]$. Then

$$V(J')=\{(a_1,\dots,a_n,b)\in k^{n+1} \ : \ (a_1,\dots,a_n)\in V(J) \ \text{ and } \ bf(a_1,\dots,a_n)=1\},$$

which contains the points $(a_1,\dots,a_n)\in V(J)$ with $f(a_1,\dots,a_n)\neq 0$. Then, by the choice of f, we have $V(J')=\emptyset$ therefore, by (a), $J'=k[X_1,\dots,X_n,Y]$. Hence, there exists a finite number of polynomials $h_1,\dots,h_m\in J$ and polynomials $g_0,g_1,\dots,g_m\in k[X_1,\dots,X_n,Y]$ such that

$$\begin{aligned} 1 = g_1(X_1,\dots,X_n,Y)h_1(X_1,\dots,X_n)+\cdots \\ +g_m(X_1,\dots,X_n,Y)h_m(X_1,\dots,X_n)+g_0(X_1,\dots,X_n,Y)(fY-1)\end{aligned}$$

Let r be the maximum of the degrees in Y of the polynomials g_i, $i=0,\dots,m$. We multiply both sides of this equality by f^r to arrive to

$$\begin{aligned} f^r = G_1(X_1,\dots,X_n,fY)h_1(X_1,\dots,X_n)+\cdots \\ G_m(X_1,\dots,X_n,fY)h_m(X_1,\dots,X_n)+G_0(X_1,\dots,X_n,fY)(fY-1)\end{aligned}$$

where all appearances of the variable Y are as the combination fY. Being this an equality between polynomials, it remains true if we substitute $fY=1$, then

$$f^r = G_1(X_1,\dots,X_n,1)h_1(X_1,\dots,X_n)+\cdots G_m(X_1,\dots,X_n,1)h_m(X_1,\dots,X_n)$$

which means that $f^r\in J$, hence $f\in\sqrt{J}$.

Conversely, let $f\in\sqrt{J}$, then there exists an $m\in\mathbb{N}$ such that $f^m\in J$. Let $(a_1,\dots,a_n)\in V(J)$. Then $f^m(a_1,\dots,a_n)=0$, therefore $f(a_1,\dots,a_n)=0$ and $f\in I(V(J))$.

□

Theorem 10 converts (4.1) into a bijective correspondence when k is algebraically closed:

$$\{\text{radical ideals } J\subset k[X_1,\dots,X_n]\} \underset{I}{\overset{V}{\rightleftarrows}} \{\textbf{varieties } Z\subset k^n\} \tag{4.2}$$

We will extend the correspondence (4.2) with the notion of irreducible variety.

Definition 42. *A variety $Z\subset k^n$ is **irreducible** if it is non-empty and it is not the union of two proper subvarieties, i.e. if $Z=Z_1\cup Z_2$ with Z_1,Z_2 varieties, then $Z=Z_1$ or $Z=Z_2$.*

Proposition 19. *A variety $Z\subset k^n$ is irreducible if and only if $I(Z)\subset k[X_1,\dots,X_n]$ is a prime ideal.*

Proof. If the ideal $I(Z)$ is not prime let $f,g\in k[X_1,\dots,X_n]\backslash I(Z)$ be polynomials such that $fg\in I(Z)$. Consider the ideals $J_1=(I(Z),f)$, $J_2=(I(Z),g)$. Since $f,g\notin I(Z)$, there is at least one point in the variety Z over which f,g do not vanish, then $V(J_1)\subsetneq Z$ and $V(J_2)\subsetneq Z$. Also, $V(J_1)\cup V(J_2)=V(J_1\cap J_2)=V(J_1J_2)\subset Z$, by the Zariski topology properties. Let $z\in Z$ and let $h\in J_1J_2$. Since $h\in I(Z)$ or $h=fg\in J_1J_2\cap I(Z)$ it is $h(z)=0$, therefore $Z=V(J_1)\cup V(J_2)$, contradicting the fact that Z is irreducible.

We left the converse to the reader as an exercise. □

Proposition 20. *A variety $Z \subset k^n$ has a unique decomposition $Z = Z_1 \cup \cdots \cup Z_n$, up to re-ordering, such that Z_i is an irreducible variety and $Z_i \not\subset Z_j$, $i \neq j$. The Z_i are called* ***irreducible components*** *of Z.*

Proof. If Z is not irreducible then we find varieties Z_1, Z_2 such that $Z = Z_1 \cup Z_2$. Proceeding inductively like this we find a chain of subvarieties which has to stop by noetherianity of the Zariski topology (Proposition 18). After removing redundancies, we get the result. □

Remark 7. *Note that Propositions 19 and 20 do not require k being an algebraically closed field.*

Therefore, when k is algebraically closed, correspondence (4.2) can extend to

$$\begin{array}{ccc} \{\text{radical ideals } J \subset k[X_1,\ldots,X_n]\} & \underset{I}{\overset{V}{\rightleftarrows}} & \{\textbf{varieties } Z \subset k^n\} \\ \bigcup & & \bigcup \\ \{\text{prime ideals } \mathfrak{p} \subset k[X_1,\ldots,X_n]\} & \underset{I}{\overset{V}{\rightleftarrows}} & \{\textbf{irreducible varieties } Z \subset k^n\} \end{array} \tag{4.3}$$

and

$$\begin{array}{ccc} \operatorname{Spec} k[X_1,\ldots,X_n] & = & \{\textbf{irreducible varieties } Z \subset k^n\} \\ \bigcup & & \bigcup \\ \operatorname{Specmax} k[X_1,\ldots,X_n] & = & \{\textbf{points } (a_1,\ldots,a_n) \in k^n\} \end{array} \tag{4.4}$$

Using Proposition 16 and that (1.3) respects prime ideals, we can formulate the correspondence for finitely generated k-algebras $k[X_1,\ldots,X_n]/J$ where k is algebraically closed:

$$\begin{array}{ccc} \operatorname{Spec} k[X_1,\ldots,X_n]/J & = & \{\textbf{irreducible varieties } Z \subset V(J) \subset k^n\} \\ \bigcup & & \bigcup \\ \operatorname{Specmax} k[X_1,\ldots,X_n] & = & \{\textbf{points } (a_1,\ldots,a_n) \in V(J) \subset k^n\} \end{array} \tag{4.5}$$

Exercise 29. *Derive the following consequences from Nullstellensatz Theorem 10 when k is an algebraically closed field:*

(a) Let $\mathfrak{m}_a$ the maximal ideal corresponding to each point $a \in k^n$. Show that $\bigcap_{a\in k^n} \mathfrak{m}_a = 0$.

(b) If $Z = V(J)$ is a variety and $\mathfrak{m}_z \subset k[X_1,\ldots,X_n]/J$ is the maximal ideal corresponding to each point $z \in Z$, show that $\bigcap_{z\in Z} \mathfrak{m}_z = 0$.

(c) If $Z = V(\mathfrak{p})$ is an irreducible variety, $\mathfrak{p} \in \operatorname{Spec} k[X_1,\ldots,X_n]$ and $\mathfrak{m}_z \subset k[X_1,\ldots,X_n]$ is the maximal ideal corresponding to each point $z \in Z$, show that $\bigcap_{z\in Z} \mathfrak{m}_z = \mathfrak{p}$.

(d) Recall Proposition 3 where we show that $\sqrt{J} = \bigcap_{\mathfrak{p}\in\operatorname{Spec} A, J\subset\mathfrak{p}} \mathfrak{p}$ for each ideal $J \subset A$. Show that, when $A = k[X_1,\ldots,X_n]$ with k algebraically closed, we have $\sqrt{J} = \bigcap_{\mathfrak{m}\in\operatorname{Specmax} A, J\subset\mathfrak{m}} \mathfrak{m}$.

(e) A radical ideal $J \subset k[X_1,\ldots,X_n]$ is an intersection of finitely many prime ideals.

4.4 The spectrum of a ring

Let us generalize the concept of Zariski topology in $\operatorname{Spec} A$, for A a general commutative ring. Given an ideal $I \subset A$, define

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

as the set of all prime ideals containing $\mathfrak{p}$.

Proposition 21. *The sets $V(I)$ are the closed sets of a topology on $\operatorname{Spec} A$, called the **Zariski topology**.*

Proof. Clearly the total space $\operatorname{Spec} A = V((0))$ and the empty set $\emptyset = V(A)$ are closed sets.

The union of two sets of the form $V(J)$, $V(K)$, with J, K ideals of A, satisfies:

$$V(J) \cup V(K) = V(J \cap K) = V(JK)$$

hence it is a closed set. Indeed, a prime ideal $\mathfrak{p}$ such that $J \subset \mathfrak{p}$ or $K \subset \mathfrak{p}$, contains the product JK and the intersection $J \cap K$. Conversely if a prime ideal $\mathfrak{p} \notin V(J) \cup V(K)$, then $J \not\subset \mathfrak{p}$ and $K \not\subset \mathfrak{p}$, hence we can pick $f \in J \backslash \mathfrak{p}$, $g \in K \backslash \mathfrak{p}$ with $fg \in (J \cap K) \backslash \mathfrak{p}$, hence $\mathfrak{p} \notin V(J \cap K)$.

Given a family of closed sets $\{V(J_\lambda)\}_{\lambda \in \Lambda}$, the intersection satisfies

$$\bigcap_{\lambda \in \Lambda} V(J_\lambda) = V\left(\sum_{\lambda \in \Lambda} J_\lambda\right) .$$

hence it is a closed set. Indeed, let $\mathfrak{p} \in \bigcap_{\lambda \in \Lambda} V(J_\lambda)$, then $J_\lambda \subset \mathfrak{p}$ for every λ, then $\sum_{\lambda \in \Lambda} J_\lambda \subset \mathfrak{p}$. Conversely, let $\mathfrak{p}$ be a prime ideal such that $\sum_{\lambda \in \Lambda} J_\lambda \subset \mathfrak{p}$. Since $J_\lambda \subset \sum_{\lambda \in \Lambda} J_\lambda$, for every λ, $J_\lambda \subset \mathfrak{p}$ for every λ, hence the equality.

Therefore, varieties are the closed sets of a topology in $\operatorname{Spec} A$. □

Remark 8. *Note that the inclusion relation for closed subsets of the Zariski topology is the reverse inclusion relation for the ideals, i.e.*

$$J \subset K \iff V(J) \supset V(K) .$$

Definition 43. *Let A be a ring and let $f \in A$ be an element. We define the **distinguished open set** associated to f as*

$$D(f) = \{\mathfrak{p} \in \operatorname{Spec} A \ : \ f \notin \mathfrak{p}\} .$$

Observe that distinguished sets are indeed open in the Zariski topology, since its complement are $\operatorname{Spec} A \backslash D(f) = V((f))$, the closed set of all primes containing the principal ideal (f).

Exercise 30. *Prove the following properties about the distinguished open sets $D(f)$, $f \in A$.*

(a) Prove that the collection $\{D(f)\}_{f \in A}$ of distinguished open sets is a basis of the Zariski topology in $\operatorname{Spec} A$.

(b) Show that, given $f, g \in A$, $D(f) \cap D(g) = D(fg)$.

(c) *Show that if* $D(f) \subset D(g)$, $f, g \in A$, *then* $f \in \sqrt{(g)}$.

(d) *Show that,* $D(f_1) \cup D(f_2) \cup \cdots \cup D(f_n) = \operatorname{Spec} A$, $f_1, \ldots, f_n \in A$ *if and only if* $f_1, \ldots, f_n$ *generate* A *as a ring.*

(e) *Show that* $f \in \operatorname{nilrad} A$ *if and only if* $D(f) = \emptyset$.

Exercise 31. *Prove that* $\operatorname{Spec} A$ *is quasi compact*[1].

Observe that these closed sets can be written as $V(J)$ for more than one ideal J, i.e. $V(J) = V(\sqrt{J})$ (this comes from the fact that if $J \subset \mathfrak{p}$, then $\sqrt{J} \subset \mathfrak{p}$, for $\mathfrak{p}$ prime). By Proposition 3, we have that

$$\sqrt{J} = \bigcap_{J \subset \mathfrak{p}} \mathfrak{p} = \bigcap_{\mathfrak{p} \in V(J)} \mathfrak{p}$$

then each closed set can be written uniquely as $V(J)$ with J a radical ideal such that $\sqrt{J} = J$.

By analogy with varieties, given a subset $Z \subset \operatorname{Spec} A$ we define the operator I by:

$$I(Z) = \bigcap_{\mathfrak{p} \in Z} \mathfrak{p}$$

Using Definition 42 to define irreducible closed sets in the Zariski topology of $\operatorname{Spec} A$ (as sets which cannot be decomposed into two proper closed subsets), we can prove the following generalization of Proposition 19.

Exercise 32. *Prove that a closed set* $Z = V(J)$ *is irreducible if and only if* $I(Z)$ *is a prime ideal.*

Gathering all together we can generalize the previous correspondences (4.4) and (4.5) to $\operatorname{Spec} A$:

$$\begin{array}{ccc} \{\text{radical ideals } J \subset A\} & \underset{I}{\overset{V}{\rightleftarrows}} & \{\textbf{closed subsets } Z = V(J) \subset \operatorname{Spec} A\} \\ \bigcup & & \bigcup \\ \{\text{prime ideals } \mathfrak{p} \subset A\} & \underset{I}{\overset{V}{\rightleftarrows}} & \{\textbf{irreducible closed sets } Z = V(\mathfrak{p}) \subset \operatorname{Spec} A\} \end{array} \tag{4.6}$$

The closure of a point $\mathfrak{p} \in \operatorname{Spec} A$ in the Zariski topology is the smallest closed subset containing $\mathfrak{p}$.

Exercise 33. *Prove that the closure of* $\mathfrak{p} \in \operatorname{Spec} A$ *is* $V(\mathfrak{p})$. *In particular, a point* $\mathfrak{p} \in \operatorname{Spec} A$ *is closed in the Zariski topology if and only if is maximal.*

[1] In some areas (usually derived from French tradition) it is used the term quasi compact to refer to a topological space where every open cover has a finite subcover, without being necessarily Haussdorff. They call compact a topological space which is both quasi compact and Haussdorff. Since Zariski topology is never Haussdorff, algebraic geometry adopts the convention of calling quasi-compact a space where just the first condition is satisfied.

The idea of $V(\mathfrak{p})$ for a general prime ideal $\mathfrak{p}$ generalizes the following. Consider a curve $Z := \{f(X,Y) = 0\}$ defined by an irreducible element $f(X,Y) \in k[X,Y]$ yielding a point $\mathfrak{p} = (f(X,Y)) \in \operatorname{Spec} k[X,Y]$ called **the general point** of Z, which is a non-closed point in the Zariski topology. Its closure contains all points $\mathfrak{m}$ such that $\mathfrak{p} \subset \mathfrak{m} \subset k[X,Y]$, i.e. the maximal ideals. When k is algebraically closed, these are exactly the points $\mathfrak{m} = (X-a, Y-b) \in \operatorname{Specmax} k[X,Y]$ such that $f(a,b) = 0$, i.e. the k-points of the variety X. This way, the general point of the curve Z is a point in $\operatorname{Spec} k[X,Y]$ which 'contains' (topologically attached, in its closure) all the 'points' $(a,b) \in Z$.

Given an element $f \in A$ we can interpret it as a function on $\operatorname{Spec} A$ in the following way. Let $\mathfrak{p} \subset A$ be a prime ideal of A, i.e. a point of $\operatorname{Spec} A$. Then we form the composition

$$\begin{array}{ccccc} A & \twoheadrightarrow & A/\mathfrak{p} & \hookrightarrow & \operatorname{Frac}(A/\mathfrak{p}) = k(\mathfrak{p}) \\ f & \mapsto & \overline{f} = f + \mathfrak{p} & \mapsto & \dfrac{\overline{f}}{1} \end{array} \tag{4.7}$$

to the residual field at the point $\mathfrak{p}$. The image of f under this composition will be called **the value of f at the point $\mathfrak{p}$** and will be denoted $f(\mathfrak{p})$. Note that if $\mathfrak{p}$ is a maximal ideal $\mathfrak{m}$, then $A/\mathfrak{m}$ is already a field and the second map does not add any information.

When A is Noetherian, there are extra finiteness statements which simplify considerably the study of the spectrum. Let A be a Noetherian ring. Then, by the inclusion relations between closed subsets of the Zariski topology en $\operatorname{Spec} A$ and ideals in A, a chain of ideals satisfying (ACC) corresponds to a chain of closed subsets satisfying the (DCC). Hence it is immediate to see that $\operatorname{Spec} A$ is then a Noetherian topological space (See Definition 41).

Exercise 34. *Prove the generalization of Proposition 20 for a Noetherian ring A and its consequences:*

(a) A closed subset of $\operatorname{Spec} A$ *is the union of a finite number of irreducible closed subsets.*

(b) Show that a radical ideal $\sqrt{J} \subset A$ is an intersection of finitely many prime ideals.

(c) (re)-Prove that a Noetherian ring with zero-divisors either has non-zero nilpotents or has at least two minimal primes.

The connection between the simpler study of varieties and $\operatorname{Spec} A$ occurs in the so-called **geometric case** when the ring A is of the form $A = k[X_1, \ldots, X_n]/J$ with J a radical ideal and k an algebraically closed field[2]. In this case:

- A is a reduced finitely generated k-algebra.
- The Zariski topology in $\operatorname{Spec} A$ defined in Proposition 21 is the analog the Zariski topology in the variety $V(J)$ defined in Proposition 17: to be precise, the topology inherited by the subspace $\operatorname{Specmax} A \subset \operatorname{Spec} A$ coincides with the Zariski topology on the points of $V(J)$, although note that $\operatorname{Spec} A$ contains points other than maximal ideals.

[2][Re, Section 5.14] calls a ring A like this **geometric ring**.

- Hilbert's Nullstellensatz Theorem 10 and its consequences (Exercise 29) say that when evaluating an element $f \in k[X_1, \dots, X_n]/J$ over each prime $\mathfrak{p} \in \operatorname{Spec} k[X_1, \dots, X_n]/J$ (as in (4.7)) it is enough to evaluate over maximal ideals, whose residue fields are all k. This is, there is a precise relationship between $\operatorname{Spec} A$ and $\operatorname{Specmax} A$[34].

- Elements $f \in A = k[X_1, \dots, X_n]/J$ are well defined polynomial functions $f : Z = V(J) \to k$: two functions are equal $f = g \in A$ if $f - g \in J$, equivalently $(f-g)(z) = 0$ for every $z \in Z = V(J)$, which means that $f(z) = g(z)$ for every $z \in Z = V(J)$. The ring $A = k[X_1, \dots, X_n]/J$ is called the **ring of coordinates of** $Z = V(J)$, sometimes denoted $k[Z]$.

- Given two varieties $Z = V(J) \subset k^n$, $W = V(K) \subset k^m$, with $J \subset k[X_1, \dots, X_n]$, $L \subset k[Y_1, \dots, Y_m]$, a polynomial function between them $\Psi : Z \to W$ is uniquely determined by a homomorphism of k-algebras $\psi : k[W] = k[Y_1, \dots, Y_m]/L \to k[Z] = k[X_1, \dots, X_n]/J$ between the corresponding rings of coordinates. See Example 26.

Exercise 35. *Prove that a polynomial function is continuous with the Zariski topology for varieties.*

A generalization of this is the correspondence between a ring homomorphism $\psi : B \to A$ and the map

$$\begin{array}{rccc} \Psi : & \operatorname{Spec} A & \to & \operatorname{Spec} B \\ & \mathfrak{p} & \mapsto & \Psi(\mathfrak{p}) := \psi^{-1}(\mathfrak{p}) \end{array}$$

between topological spaces.

Exercise 36. *Prove that the map Ψ is continuous with the Zariski topology for* $\operatorname{Spec} A$ *and* $\operatorname{Spec} B$*.*

Remark 9. *If we relax the condition of J being a radical ideal, then the nilradical of $A = k[X_1, \dots, X_n]/J$ is not zero, i.e. A has nilpotents. By Proposition 4, if a non-zero function $f \in A$ takes the value zero when evaluated (4.7) over each prime $\mathfrak{p}$, then f is a nilpotent element. This makes the study of a non-reduced finitely generated k-algebra more difficult, since its elements are not completely determined by their evaluations. This is the further study of* ***affine schemes****.*

4.5 Examples

In this final section of the chapter we explore the features of the spectrum for the main rings of the course. We begin with the arithmetic and the geometric lines.

Example 20. *Let $A = \mathbb{Z}$. The spectrum* $\operatorname{Spec} \mathbb{Z}$ *is the set of prime ideals $p \in \mathbb{Z}$, p a prime number (which are the maximal ideals) and (0). All prime ideals $p\mathbb{Z}$ are closed points in the Zariski topology and the (0) ideal is the general point of the line* $\operatorname{Spec} \mathbb{Z}$*, whose closure contain all the primes $p\mathbb{Z}$.*

[3] In general, there is no expected relation between $\operatorname{Spec} A$ and $\operatorname{Specmax} A$.

[4] For $A = k[X_1, \dots, X_n]/J$ with k non-algebraically closed the residual fields over the maximal ideals vary (e.g. for $k = \mathbb{R}$ we get real and complex non-real points).

An element of $\mathbb{Z}$ is an integer number. For a prime number p, the composition (4.7) is

$$\mathbb{Z} \twoheadrightarrow \mathbb{Z}/p\mathbb{Z} \hookrightarrow \operatorname{Frac}(\mathbb{Z}/p\mathbb{Z}) = \mathbb{Z}/p\mathbb{Z} = \mathbb{F}_p$$

hence the value of a number $n \in \mathbb{Z}$ in the prime ideal $p\mathbb{Z}$ is just the residual class modulo p, this is $n(p\mathbb{Z}) = n \mod p$. For the zero ideal the composition (4.7) is

$$\mathbb{Z} \twoheadrightarrow \mathbb{Z}/(0) = \mathbb{Z} \hookrightarrow \operatorname{Frac}(\mathbb{Z}) = \mathbb{Q}$$

hence the value of a number $n \in \mathbb{Z}$ in the prime ideal (0) is just the same integer $\frac{n}{1}$ seen as a rational.

Note that an integer is uniquely determined by its reduction modulo every prime (which is not very useful since there are infinitely many different primes), i.e. the elements of $\mathbb{Z}$ are determined by its values over all maximal ideals.

Example 21. *Let $A = k[X]$. The spectrum $\operatorname{Spec} k[X]$ is the set of prime principal ideals $(f(X)) \subset k[X]$, with $f(X)$ an irreducible polynomial in $k[X]$, and (0). The former ones are the maximal ideals and (0) is the general point of the affine line $\operatorname{Spec} k[X]$, whose closure contain all the points corresponding to the maximal ideals.*

If k is algebraically closed (such as $\mathbb{C}$), the maximal ideals are $(X - a)$ and correspond to points $a \in \mathbb{C}$. Then the evaluation (4.7) of an element $g(X) \in k[X]$ in $\mathfrak{m} = (X - a)$ is given by

$$k[X] \twoheadrightarrow k[X]/(X - a) \simeq k \hookrightarrow \operatorname{Frac}(k[X]/(X - a)) = k$$

and corresponds to the actual evaluation $g(a)$, yielding an element of the field k.

If k is not algebraically closed (such as $\mathbb{R}$), there are maximal ideals like $(X^2 + 1)$ which do not correspond to points in k (but in a finite algebraic extension of k). For example, the evaluation (4.7) of an element $g(X) \in \mathbb{R}[X]$ in $\mathfrak{m} = (X^2 + 1)$ is given by

$$\mathbb{R}[X] \twoheadrightarrow \mathbb{R}[X]/(X^2 + 1) \simeq \mathbb{C} \hookrightarrow \operatorname{Frac}(\mathbb{R}[X]/(X^2 + 1)) = \mathbb{C}$$

If $g(X) = X^3 + 2X^2 - 1$, this evaluation has the effect of substituting $1 \leftrightarrow 1$, $X \leftrightarrow i$ and $X^2 = -1$, then we obtain that the value of the polynomial $g(X)$ at the $\mathbb{C}$-point $(X^2 + 1)$ is $-3 - i$.

Note that for k algebraically closed, the value of a function $f(X) \in k[X]$ can be completely determined by its value over each point $a \in \operatorname{Specmax} k[X]$. This is also true for k non algebraically closed, but now there are more maximal ideals giving extra values for functions in finite algebraic extensions of k.

Now we explore the geometric and the arithmetic surfaces.

Example 22. *Let $A = k[X, Y]$ with k algebraically closed. The closed points of the Zariski topology are maximal ideals $\mathfrak{m} = (X - a, Y - b)$, which correspond to points in the affine k-plane k^2. There are two kinds of non-closed points: the general point of the plane (0) (whose closure is the whole $\operatorname{Spec} k[X, Y]$) and the general points of irreducible curves $Z := \{f(X, Y) = 0\} \subset k^2$ (whose closure is the set of maximal ideals $(X - a, Y - b)$ with $f(a, b) = 0$, i.e. the points of the curve Z).*

Evaluating (4.7), a function $g(X,Y) \in k[X,Y]$ in a point $\mathfrak{m} = (X-a, Y-b)$ is just

$$k[X,Y] \twoheadrightarrow k[X,Y]/(X-a,Y-b) \simeq k \hookrightarrow \mathrm{Frac}(k[X,Y]/(X-a,Y-b)) = k$$

which corresponds to evaluating $g(a,b) \in k$. Evaluating $g(X,Y) \in k[X,Y]$ in a non-maximal point point $\mathfrak{p} = (f(X,Y))$ is just

$$k[X,Y] \twoheadrightarrow k[X,Y]/(f(X,Y)) \hookrightarrow \mathrm{Frac}(k[X,Y]/(f(X,Y))$$

and gives the value of $g(X,Y) \mod (f(X,Y))$, i.e. the residual value in the curve $Z := \{f(X,Y) = 0\}$. For example, over the general point $(Y - X^2)$ of the parabola $Z := \{Y - X^2 = 0\}$ the two functions $g(X,Y) = XY$ and $h(X,Y) = X^3$ take the same value.

Example 23. *Let $A = \mathbb{Z}[X]$ and recall (Example 4) what the prime ideals, i.e. elements of $\operatorname{Spec}\mathbb{Z}[X]$, are. Consider the function $f(X) = X^2 + 3 \in \mathbb{Z}[X]$ and let us compute the values of this function over different points of $\operatorname{Spec}\mathbb{Z}[X]$.*

For the point $(2) \in \operatorname{Spec}\mathbb{Z}[X]$, (4.7) is

$$\mathbb{Z}[X] \twoheadrightarrow \mathbb{Z}[X]/(2) \simeq \mathbb{F}_2[X] \hookrightarrow \mathrm{Frac}(\mathbb{F}_2[X])$$

Then $f(X) = X^2 + 3 \mapsto X^2 + 1 = (X+1)^2$ and $f(X)$ behaves as a square function over the line (2). If we further evaluate in the maximal point $(2, X) \in \operatorname{Spec}\mathbb{Z}[X]$, we get

$$\mathbb{Z}[X] \twoheadrightarrow \mathbb{Z}[X]/(2,X) \simeq \mathbb{F}_2 \hookrightarrow \mathrm{Frac}(\mathbb{F}_2) = \mathbb{F}_2$$

and the value is 1 (seen as an element of $\mathbb{F}_2$) while if we evaluate at $(2, X+1)$ the value is $0 \in \mathbb{F}_2$.

For the point $(5) \in \operatorname{Spec}\mathbb{Z}[X]$, (4.7) is

$$\mathbb{Z}[X] \twoheadrightarrow \mathbb{Z}[X]/(5) \simeq \mathbb{F}_5[X] \hookrightarrow \mathrm{Frac}(\mathbb{F}_5[X])$$

Then $f(X) = X^2 + 3 \mapsto X^2 + 3$ which is irreducible modulo 5. This has the consequence that the function $f(X) = X^2 + 3$ does not evaluate as zero over maximal ideals $(5, X + a)$, with $a \in \mathbb{F}_5$. Over the 'fat point' $(5, X^2 + 3)$ we have

$$\mathbb{Z}[X] \twoheadrightarrow \mathbb{Z}[X]/(5, X^2+3) \simeq \mathbb{F}_{5^2} \hookrightarrow \mathrm{Frac}(\mathbb{F}_{5^2}) = \mathbb{F}_{5^2}$$

and it obviously take the value zero, but this time it is a zero in $\mathbb{F}_{25}$.

For the point $(7) \in \operatorname{Spec}\mathbb{Z}[X]$, (4.7) is

$$\mathbb{Z}[X] \twoheadrightarrow \mathbb{Z}[X]/(7) \simeq \mathbb{F}_7[X] \hookrightarrow \mathrm{Frac}(\mathbb{F}_7[X])$$

Then $f(X) = X^2+3 \mapsto (X+2)(X+5)$ and $f(X)$ splits as a product of two linear factors over (7). In particular, over $(7, X)$, it takes the value $3 \in \mathbb{F}_7$ (by substituting $X = 0$) and over $(7, X+2)$ it takes the value 0.

The following examples are the basic cases of the two instances in Exercise 34 (c): noetherian rings with zero-divisors having either more than a minimal prime or nilpotents.

Example 24. *Let $A = k[X,Y]/(XY)$ with k algebraically closed. This k-algebra has zero-divisors: $0 \neq X \in A$, $0 \neq Y \in A$ but $XY = 0 \in A$. Observe that A does not have nilpotents since (XY) is a radical ideal.*

The spectrum $\operatorname{Spec} A$ can be identified with the Zariski closed set $V(XY) \subset \operatorname{Spec} k[X,Y]$, which is not irreducible and it is the union of two irreducible closed sets: $V(XY) = V(X) \cup V(Y)$, the union of the two axes. In particular, $V(X) = \operatorname{Spec} k[X,Y]/(X) \simeq \operatorname{Spec} k[Y]$ is the vertical axis and $V(Y) = \operatorname{Spec} k[X,Y]/(Y) \simeq \operatorname{Spec} k[X]$ is the horizontal axis.

Since A is not a domain, $(0) \subset A$ is not a prime ideal. Hence, the minimal prime ideals are, at most, principal ideals $(f(X,Y))$ with $f(X,Y) = g(X) + h(Y)$ an irreducible polynomial in A. Knowing (c.f. (4.5)) that the prime ideals of the quotient A are prime ideals $\mathfrak{p} \subset k[X,Y]$ such that $(XY) \subset \mathfrak{p}$ (which are precisely the points of $V(XY)$!), there are two minimal prime ideals which are (X) and (Y), the general points of the two irreducible components of $V(XY)$.

Example 25. *Let $A = k[X,Y]/(X^2)$ with k algebraically closed. This k-algebra has zero-divisors and is non-reduced because it has nilpotents: $0 \neq X \in A$ but $X^2 = 0 \in A$.*

Geometrically, $\operatorname{Spec} A$ can be identified with the affine line $\operatorname{Spec} k[Y]$ in the sense that there exists a correspondence of maximal ideals

$$(X, Y-b) \subset k[Y] \leftrightarrow (X, Y-b) \subset A = k[X,Y]/(X^2)$$

but the difference lays in the functions over $\operatorname{Spec} A$, which are $f(Y) + Xg(Y) \in A$, hence 'doubled', the reason why we called $\operatorname{Spec} A$ the 'double line'. Note that the affine line $\operatorname{Spec}(k[Y])$ is homeomorphic to $\operatorname{Spec} k[X,Y]/\sqrt{(X^2)}$, i.e. the the variety associated with the radical of (X^2), the difference being the functions over these two spectra.

Let us see that there are just one minimal prime in A. To begin with, A is not a domain, then $(0) \subset A$ is not a prime ideal. By (4.5), prime ideals of A are prime ideals $\mathfrak{p} \subset k[X,Y]$ such that $(X^2) \subset \mathfrak{p}$. By Example 5 the only remaining two possibilities are $\mathfrak{p} = (f(X,Y))$ principal, then $\mathfrak{p} = (X)$, the only prime containing (X^2), or the non-minimal $\mathfrak{p} = (f(X), g(X,Y))$ yielding the maximal ideals of the form $(X, Y-b)$ described before. In conclusion, A has just one minimal prime according to one irreducible component for the closed Zariski set $V(X^2)$.

The evaluation of a function $f(X,Y) \in A$ in a maximal point $(X, Y-b)$ is

$$A \twoheadrightarrow A/(X, Y-b) \simeq k \hookrightarrow \operatorname{Frac}(A/(X, Y-b)) = k$$

and it is given by evaluating at $(0,b)$, yielding $f(0,b) \in k$. This process yields the fact that the different functions $f(Y) + Xg_1(Y)$ and $f(Y) + Xg_2(Y)$ have the same evaluation $f(b)$ over $(X, Y-b)$. This shows that, in a non-reduced algebra, there are different functions whose evaluations coincide over all points (even over the non-maximal one!).

We end the chapter with an example of how a homomorphism between coordinate rings determines a morphism of varieties.

Example 26. *Let k be an algebraically closed field. Let $Z := V(Y - X^2) \subset k^2$, $W := V(X) \subset k^2$ be algebraic varieties whose coordinate rings are $k[Z] = k[X,Y]/(Y - X^2)$, $k[W] = k[X,Y]/(X) \simeq k[Y]$. We define the polynomial function*

$$\begin{array}{rccc} \psi: & k[W] = k[Y] & \to & k[Z] = k[X,Y]/(Y-X^2) \\ & f(Y) & \mapsto & f(Y) + (Y - X^2) \end{array}$$

The prime ideals of $k[Z]$ are either the general point of the parabola (the ideal $(0) \subset k[Z]$) or the maximal ideals of $k[X,Y]$ which define points in the parabola, i.e. of the form $\mathfrak{p} = (X-a, Y-a^2)$. The preimage of these ideals by ψ is

$$\psi^{-1}(\mathfrak{p}) = \psi^{-1}(X-a, Y-a^2) = (Y-a^2) =: \mathfrak{q} \, .$$

Note that

$$\psi(Y-a^2) = Y - a^2 + (Y - X^2) = X^2 - a^2 + (Y - X^2) = (X+a)(X-a) + (Y-X^2) \, ,$$

then, the preimage of the ideal $\mathfrak{p}' = (X+a, Y-a^2)$ is also

$$\psi^{-1}(\mathfrak{p}') = \psi^{-1}(X+a, Y-a^2) = (Y-a^2) = \mathfrak{q} = \psi^{-1}(\mathfrak{p}) \, .$$

We define the map between the spectra as

$$\begin{array}{rccc} \Psi: & \operatorname{Spec} k[Z] = \operatorname{Spec} k[X,Y]/(Y-X^2) & \to & \operatorname{Spec} k[W] = \operatorname{Spec} k[Y] \\ & \mathfrak{p} & \mapsto & \Psi(\mathfrak{p}) := \psi^{-1}(\mathfrak{p}) \end{array}$$

Then the two points $\mathfrak{p} = (X-a, Y-a^2)$, $\mathfrak{p}' = (X+a, Y-a^2)$ map to the same point $\Psi(\mathfrak{p}) = \Psi(\mathfrak{p}') = \mathfrak{q}$. This is the geometric meaning of folding the parabola 2-to-1 into the affine line, where the points $(\pm a, a^2)$ map to the same value a^2.

Chapter 5

Localization

The difference between a ring A and a field is that in a ring, not every element is invertible, just the units, and a ring with few units is far from behaving like a field. If A is a domain, its field of fractions is, indeed, a field, where we invert as denominators all elements in A different from zero. In this chapter we will explore the algebra and geometry produced by inverting certain elements (what we call a multiplicative set $S \subset A$) in a general situation, where A can also have zero-divisors. The ring of fractions we produce is, in general, a ring, but not necessarily a field.

5.1 Rings of fractions

Let A be a ring and let S be a multiplicative set (Definition 8). Define the following equivalence relation on the cartesian product $A \times S$

$$(a, s) \sim (b, t) \iff \text{exists } u \in S \text{ such that } u(at - bs) = 0 \tag{5.1}$$

Exercise 37. *Show that (5.1) defines an equivalence relation in $A \times S$.*

In the following we will denote by $\frac{a}{s}$ the equivalence class of the element $(a, s) \in A \times S$.

Exercise 38. *Find a ring A and a multiplicative set S for which the relation $(a, s) \sim (b, t) \iff at - bs = 0$ on $A \times S$ is not an equivalence relation.*

Definition 44. *Let A be a ring and let S be a multiplicative set. We define the **ring of fractions of A with respect to** S, denoted by $S^{-1}A$ to be the quotient of $A \times S$ by the equivalence relation (5.1),*

$$S^{-1}A = A \times S/\sim,$$

which is a ring with the operations

$$\frac{a}{s} + \frac{b}{t} = \frac{at + bs}{st}$$

$$\frac{a}{s} \cdot \frac{b}{t} = \frac{ab}{st}$$

Exercise 39. *Prove that the operations in Definition 44 satisfy the ring axioms, therefore making $S^{-1}A$ into a ring.*

If A is a domain, $S = A\backslash\{0\}$ is a multiplicative set, and $S^{-1}A = \operatorname{Frac} A$ is the field of fractions of A defined in (1.1), which contains A as a subring. In general, we will have the homomorphism of rings

$$\begin{array}{rccc} \varphi: & A & \to & S^{-1}A \\ & a & \mapsto & \frac{a}{1} \end{array}$$

which will not be necessarily injective.

The homomorphism φ satisfies that $\varphi(s)$, $s \in S$, is a unit in $S^{-1}A$, since $\frac{s}{1} \cdot \frac{1}{s} = 1_{S^{-1}A}$. Indeed, the ring of fractions is universal with respect to this property.

Proposition 22. *Let $\psi : A \to B$ a ring homomorphism and let $S \subset A$ be a multiplicative set such that $\psi(s) \in \mathcal{U}(B)$ for every $s \in S$. Then, there exists a unique homomorphism of rings $\alpha : S^{-1}A \to B$ such that $\psi = \alpha \circ \varphi$.*

Proof. Let us define the homomorphism $\alpha : S^{-1}A \to B$ as

$$\alpha\left(\frac{a}{s}\right) = \psi(a) \cdot \psi(s)^{-1} ,$$

which makes sense since $\psi(S) \subset \mathcal{U}(B)$. Let us see that the definition of α does not depend on the representative chosen in the equivalence class of the ring of fractions. Suppose that $\frac{a}{s} \sim \frac{c}{t}$, then there exists an element $u \in S$ such that $u(at - cs) = 0$. Applying ψ we have $\psi(u)\left(\psi(a)\psi(t) - \psi(c)\psi(s)\right) = 0$. Given that $\psi(S) \subset \mathcal{U}(B)$ we obtain that $\alpha\left(\frac{a}{s}\right) = \psi(a)\psi(s)^{-1} = \psi(c)\psi(t)^{-1} = \alpha\left(\frac{c}{t}\right)$ and α is well defined.

Recall that $\varphi : A \to S^{-1}A$, $\varphi(a) = \frac{a}{1}$ and suppose that the map α satisfies $\psi = \alpha \circ \varphi$. Then, $\alpha\left(\frac{a}{1}\right) = \alpha(\varphi(a)) = \psi(a)$, for every $a \in A$. Then, given an element $s \in S$, we have

$$\alpha\left(\frac{1}{s}\right) = \alpha\left(\left(\frac{s}{1}\right)^{-1}\right) = \left(\alpha\left(\frac{s}{1}\right)\right)^{-1} = \psi(s)^{-1} .$$

Therefore the homomorphism $\alpha\left(\frac{a}{s}\right) = \alpha\left(\frac{a}{1}\right)\alpha\left(\frac{1}{s}\right) = \psi(a)\psi(s)^{-1}$ is uniquely determined by ψ, hence it is unique. □

Besides the property in Proposition 22, the ring of fractions $S^{-1}A$ satisfies that

$$\ker\varphi = \{a \in A \ : \ \text{exists } s \in S \text{ such that } sa = 0\} .$$

Together with a third property, we can characterize the ring of fractions.

Proposition 23. *Let $\psi : A \to B$ a ring homomorphism and let $S \subset A$ be a multiplicative set such that*

(i) $\psi(s) \in \mathcal{U}(B)$ for every $s \in S$.

(ii) $\psi(a) = 0 \Rightarrow as = 0$ for some $s \in S$.

(iii) Every element in B is of the form $\psi(a)\psi(s)^{-1}$, $a \in A$, $s \in S$.

Then, there exists a unique isomorphism of rings $\alpha : S^{-1}A \to B$ such that $\psi = \alpha \circ \varphi$.

Proof. Using (i), let us define

$$\alpha : S^{-1}A \to B \ , \ \alpha\left(\frac{a}{s}\right) = \psi(a) \cdot \psi(s)^{-1} \ ,$$

as in Proposition 22. Let us see that α is an isomorphism. By (iii), α is surjective. Now, let $\frac{a}{s} \in S^{-1}A$ such that $\alpha\left(\frac{a}{s}\right) = \psi(a) \cdot \psi(s)^{-1} = 0$, then $\psi(a) = 0$. By (ii), there exists an element $t \in S$ such that $at = 0$, then $\frac{a}{s} \sim \frac{0}{1} \in S^{-1}A$, therefore α is injective and, hence, α is an isomorphism. □

From now on, given a ring A and a multiplicative set $S \subset A$, the map $\varphi : A \to S^{-1}A$ will denote the ring homomorphism such that $\varphi(a) = \frac{a}{1}$, for every $a \in A$.

Recall that (c.f. (1.2)), given a homomorphism of rings $\psi : A \to B$ the **extension** of an ideal $I \subset A$ is the ideal $e(I) = \psi(I)B \subset B$, and the **restriction** of an ideal $J \subset B$ is an ideal $r(J) = \psi^{-1}(J) \subset A$. If we consider $B = S^{-1}A$ and the homomorphism $\varphi : A \to S^{-1}A$, $\varphi(a) = \frac{a}{1}$, given an ideal $I \subset A$ its extension is the ideal $e(I) = \varphi(I)S^{-1}A \subset S^{-1}A$, and given an ideal $J \subset S^{-1}A$ its restriction is $r(J) = \varphi^{-1}(J) \subset A$.

Proposition 24. *Let $S \subset A$ be a multiplicative set and let $\varphi : A \to S^{-1}A$ the corresponding ring homomorphism. Then*

(a) For every ideal $J \subset S^{-1}A$, we have $e(r(J)) = J$.

(b) For every ideal $I \subset A$ we have that $r(e(I)) = \{a \in A \ : \ \text{exists } s \in S \text{ with } as \in I\}$.

(c) For every ideal $I \subset A$, $e(I) = S^{-1}A$ if and only if $I \cap S \neq \emptyset$.

(d) If $\mathfrak{p} \subset A$ is a prime ideal and $\mathfrak{p} \cap S = \emptyset$ then $e(\mathfrak{p}) = \varphi(\mathfrak{p})S^{-1}A =: S^{-1}\mathfrak{p}$ is a prime ideal of $S^{-1}A$. Then, the prime ideals of $S^{-1}A$ are in bijective correspondence with prime ideals of A which do not intersect S.

Proof. (a) Note that $e(r(J)) = e(\varphi^{-1}(J)) = JS^{-1}A = J$, because J is an ideal of $S^{-1}A$.

(b) Let $a \in r(e(I)) = \varphi^{-1}(e(I))$, then $\varphi(a) = \frac{a}{1} \in e(I) = \varphi(I)S^{-1}A$, hence $\frac{a}{1} \sim \frac{b}{t}$ with $b \in I$, $t \in S$. Then, there exists an element $u \in S$ such that $u(at - b) = 0$, hence $uat = ub \in I$ and, calling $s := ut$ we have the result. Conversely, let $a \in A$, $s \in S$ such that $as \in I$. Then $\varphi(a) = \frac{a}{1} = \frac{as}{s} \in \varphi(I)S^{-1}A = e(I)$, therefore $a \in \varphi^{-1}(e(I)) = r(e(I))$.

(c) Suppose that $e(I) = S^{-1}A$ then $\frac{1}{1} \in e(I) = \varphi(I)S^{-1}A$, hence $\frac{1}{1} \sim \frac{a}{s}$, $a \in I$, $s \in S$ and there exists $u \in S$ such that $u(a - s) = 0$. Then $ua = us \in I \cap S$. Conversely, assume that there exists an element $s \in I \cap S$, which implies that $\frac{1}{1} = \frac{s}{s} \in e(I)$, hence $e(I) = S^{-1}A$.

(d) Using (b), $r(e(\mathfrak{p})) = \{a \in A \ : \ \text{exists } s \in S \text{ with } as \in \mathfrak{p}\}$. Since $\mathfrak{p}$ is prime and $\mathfrak{p} \cap S = \emptyset$, it is $r(e(\mathfrak{p})) = \{a \in \mathfrak{p} \ : \ \text{exists } s \in S \text{ with } as \in \mathfrak{p}\} = \mathfrak{p}$, hence $r(e(\mathfrak{p})) = \varphi^{-1}(e(\mathfrak{p}))$ is a prime ideal of A. Therefore $e(\mathfrak{p}) = \varphi(\mathfrak{p})S^{-1}A = S^{-1}\mathfrak{p}$ is a prime ideal of $S^{-1}A$.

□

Exercise 40. *Let $S \subset A$ be a multiplicative set and let $\varphi : A \to S^{-1}A$ the corresponding ring homomorphism.*

(a) Prove that, given an ideal $I \subset A$, $I = r(e(I))$ if and only if

$$\text{for every } s \in S\ ,\ as \in I \Rightarrow a \in I \tag{5.2}$$

holds.

(b) Conclude that there is a bijection between ideals of $S^{-1}A$ and ideals of A satisfying (5.2).

(c) Show that if A is Noetherian then $S^{-1}A$ is Noetherian.

(d) If $\mathfrak{p} \subset A$ is a prime ideal such that $\mathfrak{p} \cap S = \emptyset$, then $\mathfrak{p}$ satisfies (5.2). Therefore, we have an inclusion

$$\begin{array}{rccc} r: & \operatorname{Spec} S^{-1}A & \hookrightarrow & \operatorname{Spec} A \\ & S^{-1}\mathfrak{p} = e(\mathfrak{p}) & \mapsto & r(S^{-1}\mathfrak{p}) = r(e(\mathfrak{p})) = \mathfrak{p} \end{array}$$

whose image is $\{\mathfrak{p} \in \operatorname{Spec} A \ :\ \mathfrak{p} \cap S = \emptyset\} \subset \operatorname{Spec} A$.

Example 27. *Let $A = \mathbb{Z}$ which is a domain. Taking $S = \mathbb{Z}\backslash\{0\}$, its ring of fractions is a field $S^{-1}\mathbb{Z} = \operatorname{Frac}\mathbb{Z} = \mathbb{Q}$. The spectrum $\operatorname{Spec}\mathbb{Q}$ contains just one point corresponding to the zero ideal, which corresponds to the zero ideal in $\mathbb{Z}$ (the unique ideal which does not intersect S). Then the inclusion $\operatorname{Spec}\mathbb{Q} \hookrightarrow \operatorname{Spec}\mathbb{Z}$ maps the point into the general point of $\operatorname{Spec}\mathbb{Z}$.*

Example 28. *A similar situation happens with $A = k[X]$ with the multiplicative set $S = k[X]\backslash\{0\}$, yielding the field of fractions $k(X) := \operatorname{Frac} k[X] = \left\{\frac{f(X)}{g(X)} \ :\ g(X) \neq 0\right\}$. The inclusion $\operatorname{Spec} k(X) \hookrightarrow \operatorname{Spec} k[X]$ maps the unique point corresponding to the zero ideal into the general point of $\operatorname{Spec} k[X]$.*

One of the most important examples of multiplicative sets is $S = \{1, f, f^2, f^3, \ldots\}$, where $f \in A$. The corresponding ring of fractions will be denoted as $A_f := S^{-1}A$ and its elements are of the form $\frac{g}{f^n}$, $g \in A$, this is, we allow the element f to be invertible. The geometric effect is that $\operatorname{Spec} A_f$ contains the primes of $\operatorname{Spec} A$ which do not intersect S, i.e. which do not intersect the principal ideal (f), i.e. which do not contain the element f.

Example 29. *Let $A = k[X]$ with k algebraically closed and let $S = \{1, X, X^2, X^3, \ldots\}$. The ring of fractions $k[X]_X = S^{-1}k[X]$ consists of fractions $\frac{f(X)}{X^n}$. Its prime ideals are in bijective correspondence with prime ideals of $k[X]$ which do not intersect S, this is, which do not intersect (X). These are precisely the (0) corresponding to the general point of the affine line and all maximal ideals $(X - a)$, $0 \neq a \in k$. Geometrically, the inclusion $\operatorname{Spec} k[X]_X \hookrightarrow \operatorname{Spec} k[X]$ is the inclusion of the open set $D(X)$, complement of the origin in the affine line, into the whole line. The effect of inverting X in the ring of fractions is recovering the geometry governed by functions which do not vanish at the zero locus of the multiplicative set, this is the origin, therefore we get the complement of the ideal of the origin (X).*

Note that this ring $k[X]_X$ can be identified with $k[X, X^{-1}]$, the ring of polynomials on the variables X and X^{-1}.

Example 30. *In general, if we take $A = k[X_1, \ldots, X_n]$ with k algebraically closed, a polynomial $f \in A$ and the multiplicative set $S = \{1, f, f^2, f^3, \ldots\}$, the spectrum of the ring of fractions $\operatorname{Spec} S^{-1}A = \operatorname{Spec} k[X_1, \ldots, X_n]_f$ can be identified with $D(f)$, the distinguished open set complement of the hypersurface $V((f))$. The functions on $\operatorname{Spec} k[X_1, \ldots, X_n]_f$ are those which do not vanish at the zero locus of f.*

Exercise 41. *Prove that $\operatorname{Spec} A_f$ is homeomorphic to $D(f)$, the distinguished open set in the Zariski topology whose complement is $V((f))$.*

Example 31. *Let $A = k[X, Y]/(XY)$ and recall that $\operatorname{Spec} A$ is the union of the X and Y axes. Let $S = \{1, X, X^2, \ldots\}$ be a multiplicative set. Observe that in the ring of fractions we get $\frac{Y}{1} \sim \frac{0}{1}$, since there exists the element $X \in S$ such that $X(Y \cdot 1 - 0 \cdot X) = 0 \in A$. Therefore we can see that the image of the homomorphism*

$$\varphi : A = k[X, Y]/(XY) \hookrightarrow S^{-1}A = (k[X, Y]/(XY))_X$$

is $\varphi(A) \simeq k[X]$.

The prime ideals of A, i.e. the points of its spectrum, are the points of the union of the X and Y axes (corresponding to maximal ideals $(X - a, Y)$ and $(X, Y - b)$), plus the two general points of both lines (corresponding to the primes (X) and (Y)). Again, the spectrum of the ring of fractions contains the prime ideals of A which do not intersect the multiplicative set S. Hence, $\operatorname{Spec} S^{-1}A = \operatorname{Spec}(k[X, Y]/(XY))_X$ is given by the maximal ideals of the form $(X - a, Y)$, $0 \neq a \in k$, plus the general point of the X axis corresponding to the prime (Y), therefore the X-axis minus the origin. Observe that this is precisely the intersection of $\operatorname{Spec}(k[X, Y]/(XY))$ (the union of the axis) with the distinguished open set $D(X)$ (the complement in the plane of the Y-axis). Finally, note the isomorphism $(k[X, Y]/(XY))_X \simeq k[X]_X$, where the fractions are the same and the points of its spectrum are also the same.

5.2 Localization

Let A be a domain and let $\mathfrak{p} \subset A$ be a prime ideal. The difference $A \backslash \mathfrak{p}$ is a multiplicative set since $1 \notin \mathfrak{p}$ and given $f, g \notin \mathfrak{p}$, $fg \notin \mathfrak{p}$. Hence, we can define the ring of fractions

$$A_{\mathfrak{p}} := (A \backslash \mathfrak{p})^{-1} A = \left\{ \frac{f}{g} \ : \ f, g \in A, g \notin \mathfrak{p} \right\},$$

which is a subring of the ring of fractions $\operatorname{Frac}(A)$.

Exercise 42. *Show that an element $\frac{f}{g} \in A_{\mathfrak{p}}$ is a unit of $A_{\mathfrak{p}}$ if and only if $f \notin \mathfrak{p}$.*

Therefore, the ring $A_{\mathfrak{p}}$ is a local ring, with maximal ideal

$$\mathfrak{m}_{\mathfrak{p}} = \left\{ \frac{f}{g} \ : \ f \in \mathfrak{p}, g \notin \mathfrak{p} \right\} \subset A_{\mathfrak{p}} \, ,$$

and it represents the geometric process of passing from $\operatorname{Spec} A$ to local information at the point $\mathfrak{p} \in \operatorname{Spec} A$.

Definition 45. *Let A be a domain and let $\mathfrak{p} \subset A$ be a prime ideal. The **localization** of A at $\mathfrak{p}$ is the local ring $(A_{\mathfrak{p}}, \mathfrak{m}_{\mathfrak{p}})$.*

The inclusion of spectra in Exercise 40 (d) is:

$$\begin{array}{rcl} \operatorname{Spec} A_{\mathfrak{p}} & \hookrightarrow & \operatorname{Spec} A \\ (A\backslash\mathfrak{p})^{-1}\mathfrak{q} & \mapsto & \mathfrak{q} \end{array} \tag{5.3}$$

such that $\mathfrak{q} \cap (A\backslash\mathfrak{p}) = \emptyset$, therefore, $\operatorname{Spec} A_{\mathfrak{p}}$ contains all primes $\mathfrak{q}$ such that $\mathfrak{q} \subset \mathfrak{p} \subset A$. This means that passing to the localization $A_{\mathfrak{p}}$ we see the geometry of all ideals $\mathfrak{q} \in \operatorname{Spec} A$ whose geometry $V(\mathfrak{q})$ contains the localization point $\mathfrak{p}$, i.e. we are looking at the Zariski neighborhood of the point $\mathfrak{p}$.

Let us explore this notion through some main examples.

Example 32. *Let $k[X]$ be the ring of polynomials in one variable with coefficients in the field k, and let $(X-a)$, $a \in k$, be the principal ideal generated by the (irreducible) polynomial $X-a$, which is a prime ideal. Localizing with respect to this ideal yields:*

$$k[X]_{(X-a)} = \left\{ \frac{f(X)}{g(X)} \ : \ f, g \in k[X] \ , \ g(X) \notin (X-a) \right\} = \left\{ \frac{f(X)}{g(X)} \ : \ g(a) \neq 0 \right\} \ ,$$

with maximal ideal $\mathfrak{m} = (X-a) \cdot k[X]_{(X-a)} =$

$$\left\{ \frac{f(X)}{g(X)} \ : \ f(X) \in (X-a) \ , \ g(X) \notin (X-a) \right\} = \left\{ \frac{f(X)}{g(X)} \ : \ f(a) = 0 \ , \ g(a) \neq 0 \right\} \ .$$

The set of units of this local ring is the complement of the maximal ideal, which are those rational functions not vanishing at a:

$$\mathcal{U}\left(k[X]_{(X-a)}\right) = \left\{ \frac{f(X)}{g(X)} \ : \ f(a) \neq 0 \ , \ g(a) \neq 0 \right\} \ .$$

The residue field of this local ring is the quotient of the ring by its maximal ideal

$$k[X]_{(X-a)} / (X-a) \cdot k[X]_{(X-a)} \simeq k \ ,$$

where each residual class can be identified with the value of the numerator at a, $f(a)$. This field k is also different from the field of fractions of $k[X]$, $\operatorname{Frac} k[X] = k(X)$, which is the field of quotients of polynomials $\frac{f(X)}{g(X)}$ where $g(X)$ is not the zero polynomial. However, all these local rings at primes $(X-a)$ yield the same residue field k.

*Polynomials in $k[X]$ can be understood as functions on the affine line $\operatorname{Spec} k[X]$. And quotients of polyomials in $k(X)$ are **rational functions** on $\operatorname{Spec} k[X]$, defined in all the affine line except by a finite number of points, i.e. defined in a Zariski open set of $k[X]$. For the prime ideal (0), which is the general point of the affine line, the localization yields $k[X]_{(0)}$, which is isomorphic to $k(X)$: localize at the whole line gives the same rational functions in the entire line.*

Now, for a prime ideal $(X-a)$, the localization yields $k[X]_{(X-a)}$ which contains rational functions which are well defined at the maximal point $X-a$ (because its denominator does not vanish). These are germs of rational functions defined locally near a point $a \in k$, hence its value is just an element of the field k, the residual field (the same field for all a).

In this example, the inclusion (5.3) is

$$\operatorname{Spec} k[X]_{(X-a)} \hookrightarrow \operatorname{Spec} k[X]$$

where the only primes in $k[X]_{(X-a)}$ are in correspondence with primes $\mathfrak{q} \subset k[X]$ such that $\mathfrak{q} \subset (X-a)$, therefore $\operatorname{Spec} k[X]_{(X-a)}$ has just two primes, the (0) and the maximal ideal $\mathfrak{m} = (X-a) \cdot k[X]_{(X-a)}$ corresponding to $(X-a)$ itself. The inclusion of $\mathfrak{m}$ collects the information of the value of a rational function at a and the general point (0) contains the information of the rest of the rational function in the surroundings of a.

Remark 10. *Mind the difference between the rings of fractions $k[X]_{X-a}$, which are fractions where we invert powers of the polynomial $X-a$ (rings of fractions of the form A_f), and $k[X]_{(X-a)}$, which are fractions where we invert elements outside the ideal $(X-a)$ (rings of fractions which are localizations of the form $A_{\mathfrak{p}}$).*

Example 33. *Let $\mathbb{Z}$ be the ring of integers and let $p \in \mathbb{Z}$ be a prime number. Let $p\mathbb{Z}$ be the ideal of multiples of p, which is a prime ideal. Localizing with respect to the prime ideal $p\mathbb{Z}$ yields the local ring denoted by $\mathbb{Z}_{(p)}$:*

$$\mathbb{Z}_{(p)} = \left\{ \frac{a}{b} \ : \ a, b \in \mathbb{Z}, b \notin p\mathbb{Z} \right\}$$

The maximal ideal of this local ring $\mathbb{Z}_{(p)}$ is

$$\mathfrak{m}(\mathbb{Z}_{(p)}) = p\mathbb{Z}_{(p)} = \left\{ \frac{a}{b} \ : \ a, b \in \mathbb{Z}, a \in p\mathbb{Z}, b \notin p\mathbb{Z} \right\}.$$

The set of units of $\mathbb{Z}_{(p)}$ is the complement

$$\mathcal{U}(\mathbb{Z}_{(p)}) = \left\{ \frac{a}{b} \ : \ a, b \in \mathbb{Z}, a \notin p\mathbb{Z}, b \notin p\mathbb{Z} \right\} .$$

The residue field of this local ring is

$$\mathbb{Z}_{(p)}/p\mathbb{Z}_{(p)} = \mathbb{F}_p \ ,$$

the finite field with p elements. Note how the finite fields $\mathbb{F}_p$ are different from the field of fractions of $\mathbb{Z}$, which is $\mathbb{Q}$.

A rational function on $\operatorname{Spec}\mathbb{Z}$ is an element of its ring of fractions, i.e. a rational number $\frac{a}{b} \in \operatorname{Frac}\mathbb{Z} = \mathbb{Q}$, which is defined at all elements of $\operatorname{Spec}\mathbb{Z}$ except by a finite number of primes (those appearing in the arithmetic decomposition of the denominator b), which is a Zariski open subset of $\operatorname{Spec}\mathbb{Z}$. Localizing at the prime (0), the general point of $\operatorname{Spec}\mathbb{Z}$, gives the same fractions in $\mathbb{Q}$.

Localizing at a prime (p) yields functions well defined at the prime p because $\mathbb{Z}_{(p)}$ contains fractions $\frac{a}{b}$ where b is not a multiple of p, hence it is not zero in $\mathbb{Z}/p\mathbb{Z}$. Functions taking the value zero at p are elements of the maximal ideal $\mathfrak{m}(\mathbb{Z}_{(p)})$, whose numerator is a multiple of p. The units in $\mathbb{Z}_{(p)}$ are functions taking a non-zero value at p. Observe that the fields $\mathbb{F}_p$, where these local functions take values, vary from one prime to another.

Example 34. *In general, if we consider the ring of polynomials $k[X_1, \ldots, X_n]$ with k algebraically closed, $\mathfrak{p} \subset k[X_1, \ldots, X_n]$ a prime ideal and $Z = V(\mathfrak{p})$ the corresponding irreducible variety in k^n, localizing at $\mathfrak{p}$ yields*

$$k[X_1, \ldots, X_n]_{\mathfrak{p}} = \left\{ \frac{f(X_1, \ldots, X_n)}{g(X_1, \ldots, X_n)} \ : \ g(X_1, \ldots, X_n) \notin \mathfrak{p} \right\} .$$

These are rational functions which do not vanish identically at the variety Z. This does not prevent functions f/g from having zeroes at some points of Z: they are actually defined on a Zariski open subset of Z. It could happen that g vanishes at certain maximal points $(X_1 - a_1, \ldots, X_n - a_n)$ but not at all points in Z. The elements in the maximal ideal $\mathfrak{p}k[X_1, \ldots, X_n]_{\mathfrak{p}}$ are those fractions whose numerator is identically zero in Z.

For example, localizing $\mathbb{C}[X, Y]$ at the prime $(Y - X^2)$ yields the ring of rational functions defined on the parabola

$$Z = \{(x, y) \in \mathbb{C}^2 \ : \ x^2 - y = 0\} .$$

Its elements are fractions $\frac{f(X,Y)}{g(X,Y)}$ whose denominator g does not belong to the principal ideal $(Y - X^2)$, i.e. where g is not a multiple of $Y - X^2$. However, $\frac{X}{X^2Y - Y^3} = \frac{X}{(X-Y)(X+Y)Y} \in \mathbb{C}[X, Y]_{(Y-X^2)}$ is not defined at the points $(0, 0), (1, 1), (-1, 1) \in Z$ (the denominator vanishes), hence it is defined in the complementary Zariski open set of these three points, which is precisely $D((X-Y)(X+Y)Y) \subset \operatorname{Spec} \mathbb{C}[X, Y]/(Y - X^2)$. Note that $\frac{X}{X^2Y - Y^3} \in \mathbb{C}[X, Y]_{(Y-X^2)}$ is a unit and it is not contained in the maximal ideal of the localization. On the other hand, the element $\frac{Y^2 - X^2Y}{X-1} = \frac{(Y-X^2)Y}{X-1} \in \mathbb{C}[X, Y]_{(Y-X^2)}$ belongs to the maximal ideal $(Y - X^2) \cdot \mathbb{C}[X, Y]_{(Y-X^2)}$, and it is a function which vanishes identically at the parabola Z.

If we consider the same parabola in the three-dimensional affine space we have

$$W = \{(x, y, z) \in \mathbb{C}^3 \ : \ x^2 - y = 0\}$$

whose ring of coordinates is $\mathbb{C}[X, Y, Z]/(Y - X^2, Z)$. Its localization is $\mathbb{C}[X, Y, Z]_{(Y-X^2,Z)}$. The rational function $Z/X \in \mathbb{C}[X, Y, Z]_{(Y-X^2,Z)}$ is well defined because the denominator X does not vanish identically at the parabola. It belongs to the maximal ideal $(Y - X^2, Z) \cdot \mathbb{C}[X, Y, Z]/(Y - X^2, Z)$ since the numerator Z belongs to the ideal $(Y - X^2, Z)$. Note that the ideal generated by the numerator, $\mathfrak{q} = (Z)$ satisfies that $\mathfrak{q} \subset \mathfrak{p} = (Y - X^2, Z)$, then it is in correspondence with a point in $\operatorname{Spec} \mathbb{C}[X, Y, Z]/(Y - X^2, Z)$: it reflects the general point of the plane $Z = 0$ which contains the parabola in which we are localizing.

5.3 Modules of fractions

Similarly, we can define modules of fractions. Let A be a ring, let S be a multiplicative set and let M be an A-module. Define the following equivalence relation on the cartesian product $M \times S$

$$(m, s) \sim (n, t) \iff \text{exists } u \in S \text{ such that } u(mt - ns) = 0 \tag{5.4}$$

and denote by $\frac{m}{s}$ the equivalence class of the element $(m, b) \in M \times S$.

Definition 46. *Let A be a ring, let S be a multiplicative set and let M be an A-module. We define the* ***module of fractions of*** *M* ***with respect to*** *S, denoted by $S^{-1}M$, to be the quotient of $M \times S$ by the equivalence relation (5.4),*

$$S^{-1}M = M \times S/\sim ,$$

which is a module with the operations

$$\frac{m}{s} + \frac{n}{t} = \frac{mt+ns}{st} , \quad \text{for } \frac{m}{s}, \frac{n}{t} \in S^{-1}M ,$$

$$\frac{a}{b} \cdot \frac{m}{s} = \frac{am}{bs} , \quad \text{for } \frac{m}{s} \in S^{-1}M \text{ and } \frac{a}{b} \in S^{-1}A .$$

Exercise 43. *Prove that $S^{-1}M$ is an $S^{-1}A$-module (hint: show that it is equivalent to the homomorphism $\xi_s : M \to M$, $m \mapsto sm$, being bijective for every $s \in S$).*

In particular, if $\mathfrak{p} \subset A$ is a prime ideal and $S = A\backslash\mathfrak{p}$ is a multiplicative set, then $S^{-1}M$ is an $S^{-1}A = A_{\mathfrak{p}}$-module. We call this the **localization of** M **at** $\mathfrak{p}$ and will be denoted by $M_{\mathfrak{p}}$.

Given a homomorphism of A-modules $\psi : M \to N$ and a multiplicative set $S \subset A$, it is induced a homomorphism of $S^{-1}A$-modules between the modules of fractions

$$\psi' : S^{-1}M \longrightarrow S^{-1}N , \quad \psi'\left(\frac{m}{s}\right) \mapsto \frac{\psi(m)}{s}$$

This says that the operation of taking fractions (with denominators in S) is functorial on modules (from A-modules to $S^{-1}A$-modules). And the next proposition says that this functor is exact.

Proposition 25. *Given an exact sequence of A-modules $L \xrightarrow{\alpha} M \xrightarrow{\beta} N$ (c.f. Definition 32), and a multiplicative set $S \subset A$, the induced sequence of $S^{-1}A$-modules $S^{-1}L \xrightarrow{\alpha'} S^{-1}M \xrightarrow{\beta'} S^{-1}N$ is exact.*

Proof. Let $\frac{m}{s} \in S^{-1}M$. Then $\beta'\left(\frac{m}{s}\right) = 0 \in S^{-1}N$ if and only if there exists an element $u \in S$ such that $u\beta(m) = \beta(um) = 0 \in N$. Since $\operatorname{im}\alpha = \ker\beta$, this is equivalent to the existence of elements $u \in S$, $l \in L$ such that $um = \alpha(l)$, therefore $\frac{m}{s} = \alpha'\left(\frac{l}{us}\right)$, hence $\frac{m}{s} \in \operatorname{im}\alpha'$. □

Corollary 10. *Given an exact sequence of A-modules $L \xrightarrow{\alpha} M \xrightarrow{\beta} N$ and a prime ideal $\mathfrak{p} \subset A$, the induced sequence $L_{\mathfrak{p}} \xrightarrow{\alpha'} M_{\mathfrak{p}} \xrightarrow{\beta'} N_{\mathfrak{p}}$ between the localized modules is exact.*

Proof. Follows immediate from Proposition 25 by taking $S = A\backslash\mathfrak{p}$. □

Exercise 44. *(a) Let M, N be A-modules. Let $S \subset A$ be a multiplicative set. Then*

$$S^{-1}(M+N) = S^{-1}M + S^{-1}N .$$

In particular,

$$S^{-1}(M \oplus N) = S^{-1}M \oplus S^{-1}N .$$

(b) *Let M, N be A-modules. Let $S \subset A$ be a multiplicative set. Then*

$$S^{-1}(M \cap N) = S^{-1}M \cap S^{-1}N \ .$$

(c) *Let M be an A-module and let $N \subset M$ be a submodule. Let $S \subset A$ be a multiplicative set. Then*

$$S^{-1}\left(\frac{M}{N}\right) \simeq \frac{S^{-1}M}{S^{-1}N}$$

Given a ring A, a multiplicative set $S \subset A$ and an ideal I, we have the quotient map

$$\begin{array}{rccc} \pi: & A & \to & A/I \\ & S & \mapsto & \pi(S) \end{array}$$

where note that $\pi(S)$ is a multiplicative set of the quotient A/I. Then, we can obtain the ring of fractions $(\pi(S))^{-1}(A/I)$. On the other hand, consider the ring of fractions $S^{-1}A$ and the ring homomorphism $\varphi : A \to S^{-1}A$. Hence, $S^{-1}I := e(I) = \varphi(I)S^{-1}A$ is the extended ideal in $S^{-1}A$. Then, we are allowed to take the quotient $S^{-1}A/S^{-1}I$.

Proposition 26. *There is an isomorphism $(\pi(S))^{-1}(A/I) \simeq S^{-1}A/S^{-1}I$.*

Proof. If we see the quotient $\pi(A) = A/I$ as an A-module, the ring of fractions $(\pi(S))^{-1}(A/I)$ is precisely the module of fractions $S^{-1}(A/I)$. Using Exercise 44 (c), we have the isomorphisms

$$(\pi(S))^{-1}(A/I) = S^{-1}(A/I) \simeq S^{-1}A/S^{-1}I$$

which can be shown to also be a ring homomorphism. □

In particular, if we are localizing at a prime ideal, the commutation of these two processes has a precise meaning.

Corollary 11. *If $\mathfrak{p} \subset A$ is a prime ideal, the residue field of the localization $A_\mathfrak{p}/\mathfrak{p}A_\mathfrak{p}$ (coming from taking fractions and then quotient) equals the field of fractions $k(\mathfrak{p}) = \operatorname{Frac}(A/\mathfrak{p})$ (coming from taking the quotient and then fractions).*

Proof. Follows from Proposition 26. □

Let us summarize the content of this chapter. Let $\mathfrak{p} \subset A$ be a prime ideal.

- $A/\mathfrak{p}$ is a ring containing the polynomial functions on $\mathfrak{p}$. This is a domain whose field of fractions $\operatorname{Frac}(A/\mathfrak{p})$ is the residue field $k(\mathfrak{p})$ of the point $\mathfrak{p}$. Its ideals are in bijective correspondence with primes $\mathfrak{q} \subset A$ such that $\mathfrak{p} \subset \mathfrak{q} \subset A$, hence $A/\mathfrak{p}$ contains *all the geometry inside the point* $\mathfrak{p}$, which is $V(\mathfrak{p}) \subset \operatorname{Spec} A$.

- $A_\mathfrak{p}$ is a local ring containing the fractions of polynomials whose denominator does not vanish at $\mathfrak{p}$, hence regular functions defined at (a neighborhood of) $\mathfrak{p}$. Its residue field $A_\mathfrak{p}/\mathfrak{p}A_\mathfrak{p}$ (taking the quotient by the unique maximal ideal) contains the evaluation of these regular functions at the point $\mathfrak{p}$, and coincides with $k(\mathfrak{p}) = \operatorname{Frac}(A/\mathfrak{p})$, by Corollary 11. Its ideals, by (5.3), are in bijective correspondence with primes $\mathfrak{q} \subset A$ such that $\mathfrak{q} \subset \mathfrak{p} \subset A$, hence $A_\mathfrak{p}$ contains *all the geometry surrounding the point* $\mathfrak{p}$, which is $\operatorname{Spec} A_\mathfrak{p} \subset \operatorname{Spec} A$.

In the particular case where $\mathfrak{p} = (f)$ is a principal ideal, $f \in A$:

- A_f is a ring contains the fractions of polynomials whose denominator vanishes at $\mathfrak{p}$, hence regular functions defined at $D(f) = \operatorname{Spec} A \backslash V(\mathfrak{p}) = \operatorname{Spec} A \backslash V((f))$. It is not necessarily a domain, hence we do not talk about its ring of fractions.

Example 35. *Observe that the localization $A_\mathfrak{p}$ is a local ring, hence* $\operatorname{Spec} A_\mathfrak{p}$ *just contains one maximal ideal. However,* $\operatorname{Spec} A_\mathfrak{p}$ *can contain lots of prime ideals. For example, the localization of $k[X,Y]$ at the maximal ideal of the origin, $k[X,Y]_{(X,Y)}$ is a local ring whose maximal ideal is (X,Y), whose elements are fractions of polynomials of the form $\frac{f(X,Y)}{g(X,Y)}$ such that $g(0,0) \neq 0$. These fractions, at the origin, take values in the residue field k. Prime ideals of $k[X,Y]_{(X,Y)}$ correspond to irreducible curves (i.e. prime principal ideals $(h(X,Y)) \subset k[X,Y]$) passing through the origin. The prime ideals $(Y - X^2)$ and $(Y^2 - X^3)$ are different, but they take the same value at the origin, $0 \in k$: indeed, they are both contained in the maximal ideal (X,Y).*

Exercise 45. *In light of the isomorphism between the residue field $A_\mathfrak{p}/\mathfrak{p}A_\mathfrak{p} \simeq \operatorname{Frac}(A/\mathfrak{p}) = k(\mathfrak{p})$, try to understand the details of the map (4.7) in the Examples of Section 4.5.*

We end the chapter by discussing the meaning in algebraic geometry of a property being local. We say that a property P of a ring A or of an A-module M is **local** if:

$$A \text{ or } M \text{ has } P \iff A_\mathfrak{p} \text{ or } M_\mathfrak{p} \text{ has } P \text{ for every } \mathfrak{p} \in \operatorname{Spec} A\ .$$

The following results show the locality of certain properties.

Proposition 27. *Being zero is a local property of A-modules M, i.e., $M = 0$ if and only if $M_\mathfrak{p} = 0$ for every $\mathfrak{p} \in \operatorname{Spec} A$.*

Proof. It is clear than, if $M = 0$, then $M_\mathfrak{p} = 0$ and $M_\mathfrak{m} = 0$ for every prime $\mathfrak{p}$ or maximal ideal $\mathfrak{m}$. Suppose that $M_\mathfrak{m} = 0$ for every maximal ideal $\mathfrak{m} \subset A$ but $M \neq 0$. Let $0 \neq m \in M$. Consider the ideal $\operatorname{Ann}(m) = \{a \in A \ : \ am = 0\}$ (see Definition 48 of the annihilator), which is different from the total ring A (because $M \neq 0$). Then, by Proposition 2, there exists a maximal ideal $\mathfrak{m} \subset A$ such that $\operatorname{Ann}(m) \subset \mathfrak{m}$. Since $M_\mathfrak{m} = 0$, the fraction $\frac{m}{1} = \frac{0}{1}$, hence there exists $u \notin \mathfrak{m}$ with $u(m \cdot 1 - 0 \cdot 1) = 0$, i.e. $um = 0$, i.e. $u \in \operatorname{Ann}(m)$, which is a contradiction since $\operatorname{Ann}(m) \subset \mathfrak{m}$. □

Proposition 28. *Being injective (resp. surjective) is a local property of homomorphisms of A-modules, i.e., $\psi : M \to N$ is injective (resp. surjective) if and only if $\psi' : M_\mathfrak{p} \to N_\mathfrak{p}$ is injective (resp. surjective) for every $\mathfrak{p} \in \operatorname{Spec} A$.*

Proof. Exercise. As in Proposition 27, use that the locality can be checked just at maximal ideals. □

Exercise 46. *Let $\mathfrak{p} \subset \mathfrak{q} \subset A$ be prime ideals. Prove that the localization $A_\mathfrak{p}$ is isomorphic to $(A_\mathfrak{q})_\mathfrak{p}$, the localization of $A_\mathfrak{q}$ at the prime ideal $\mathfrak{p}A_\mathfrak{q}$.*

Chapter 6

Primary decomposition

In every UFD, an element decomposes uniquely (up to rearranging and units) as a product of irreducible elements. When the ring is also a PID, as it is the case of $\mathbb{Z}$, this decomposition can be translated into ideals. For example, the arithmetic decomposition $300 = 2^2 \cdot 3 \cdot 5^2$ yields

$$300\mathbb{Z} = (2\mathbb{Z})^2 \cap (3\mathbb{Z}) \cap (5\mathbb{Z})^2$$

which exhibits every principal ideal as a unique intersection of powers of prime ideals.

In $k[X_1, \dots, X_n]$ the situation is more complicated. A variety V corresponding to a radical ideal $I(V)$ (4.2) can be expressed as a union of irreducible varieties (Definition 42) $V = \cup V_i$ which corresponds to prime ideals $I(V_i) = \mathfrak{p}_i$, such that $I(V) = \cap_i \mathfrak{p}_i$. These prime ideals $\mathfrak{p}_i$ are the minimal primes which contain $I(V)$, but this description does not account for powers of ideals as it happens with $\mathbb{Z}$. Nor we are allowed, in principle, to describe a non-radical ideal as an intersection of primes.

As we know, the algebra of an ideal $I \subset A$ is related to the geometry of $\operatorname{Spec} A/I$. For example, $\operatorname{Spec} \mathbb{Z}/300\mathbb{Z}$ contains three points, the prime ideals $2\mathbb{Z}, 3\mathbb{Z}$ and $5\mathbb{Z}$ (these will be their associated primes and the support of the $\mathbb{Z}$-module $\mathbb{Z}/300\mathbb{Z}$), and the prime 2 appears in the arithmetic decomposition of 300 because of the very same reason: 2 is a zero divisor of $\mathbb{Z}/300\mathbb{Z}$. There are other non-prime elements of the ring $\mathbb{Z}$ which annihilate the module $\mathbb{Z}/300\mathbb{Z}$, for example the element 4.

This chapter is devoted to find, when possible, good descriptions of an ideal as an intersection of ideals (called primary ideals) which resemble the notion of arithmetic decomposition in $\mathbb{Z}$.

6.1 Support of a module and associated primes

Most of the modules we are interested in are quotients A/I of a ring over an ideal. However, the notions in this section can be formulated for modules in general.

Definition 47. *Let M be an A-module. The **support** of M is*

$$\operatorname{Supp} M = \{\mathfrak{p} \in \operatorname{Spec} A \ : \ M_{\mathfrak{p}} \neq 0\} \subset \operatorname{Spec} A \ ,$$

i.e. the set of primes whose localizations $M_{\mathfrak{p}} = (A \backslash \mathfrak{p})^{-1} M$ are different from zero.

Definition 48. *Let M be an A-module and let $m \in M$ be an element. The* ***annihilator*** *of m is*

$$\operatorname{Ann} m = \{a \in A \ : \ am = 0\} \ ,$$

which is an ideal of A. An element $a \in A$ is a zero divisor of M if there exists an $0 \neq m \in M$ with $a \in \operatorname{Ann} m$. The ***annihilator*** *of the module M is*

$$\operatorname{Ann} M = \{f \in A \ : \ fM = 0\} \ .$$

Let us explore several properties of the support and annihilator of a module.

Proposition 29. *Let M be an A-module.*

(a) If M is generated by a single element m then $\operatorname{Supp} M = V(\operatorname{Ann} m)$. In particular, the quotient ring A/I is generated by 1 and $I = \operatorname{Ann} 1$, therefore $\operatorname{Supp} A/I = V(I)$.

(b) If $M = \sum_{i \in I} M_i$, then $\operatorname{Supp} M = \cup_{i \in I} \operatorname{Supp} M_i$.

(c) Given an exact sequence $0 \to L \to M \to N \to 0$, $\operatorname{Supp} M = \operatorname{Supp} L \cup \operatorname{Supp} N$.

(d) If M is finite over A, then $\operatorname{Supp} M = V(\operatorname{Ann} M)$ is a closed subset of $\operatorname{Spec} A$.

(e) If M is finite over A and if $\mathfrak{p} \in \operatorname{Supp} M$, then $V(\mathfrak{p}) \subset \operatorname{Supp} M$.

Proof. (a) Assume M is generated by a single element $m \in M$, therefore, $M = Am$. By contradiction, let $\mathfrak{p} \notin \operatorname{Supp} M$, then the localization $M_{\mathfrak{p}} = 0$. Therefore, all elements of the form $\frac{am}{1}$ with $a \in A$ are zero in the localization $M_{\mathfrak{p}}$, in particular, $\frac{m}{1} = 0$. This is equivalent to the existence of an element $u \notin \mathfrak{p}$ such that $um = 0$, which is equivalent to $(A \backslash \mathfrak{p}) \cap \operatorname{Ann} m \neq \emptyset$ which happens if and only if $\operatorname{Ann} m \not\subset \mathfrak{p}$, i.e. $\mathfrak{p} \notin V(\operatorname{Ann} m)$. Therefore, $\operatorname{Supp} M = V(\operatorname{Ann} m)$.

(b) By Exercise 44 (a), $M_{\mathfrak{p}} = \sum_{i \in I} (M_i)_{\mathfrak{p}}$, then it is immediate that those supporting primes $\mathfrak{p} \in \operatorname{Spec} A$ for which $M_{\mathfrak{p}} \neq 0$ are those primes for which there exists (at least) an $i \in I$ with $(M_i)_{\mathfrak{p}} \neq 0$.

(c) It follows from the exactness of localization (Corollary 10).

(d) Let $m_1, \ldots, m_s$ be generators of M as an A-module. By Definition 29, $M = Am_1 + \cdots + Am_s$, where each Am_i is an A-module generated by a single element. Combining (a) and (b) we have

$$\operatorname{Supp} M = V(\operatorname{Ann} m_1) \cup \cdots \cup V(\operatorname{Ann} m_s) = V(\operatorname{Ann} m_1 \cap \cdots \cap \operatorname{Ann} m_s) \ ,$$

by the properties of the Zariski topology. Let us see that $V(\operatorname{Ann} m_1 \cap \cdots \cap \operatorname{Ann} m_s) = V(\operatorname{Ann} M)$.

Let $\mathfrak{p}$ be a prime ideal which contains $\operatorname{Ann} m_1 \cap \cdots \cap \operatorname{Ann} m_s$ and let $a_i \in A$, $i = 1, \ldots, s$ be elements such that $a_i \in \operatorname{Ann} m_i$. Then the product $a_1 \cdots a_s \in \operatorname{Ann} m_1 \cap \cdots \cap \operatorname{Ann} m_s \subset \mathfrak{p}$ and, then, there exists (at least) an index j such that $a_j \in \mathfrak{p}$, hence $\operatorname{Ann} m_j \subset \mathfrak{p}$. Since $\operatorname{Ann} M \subset \operatorname{Ann} m_j$, $\operatorname{Ann} M \subset \mathfrak{p}$ and $\mathfrak{p} \in V(\operatorname{Ann} M)$. Conversely, let $\mathfrak{p} \subset A$ be a prime

ideal such that $\operatorname{Ann} M \subset \mathfrak{p}$ and let $a \in \operatorname{Ann} m_1 \cap \cdots \cap \operatorname{Ann} m_s$. Then, $a \in \operatorname{Ann} M = \operatorname{Ann}(Am_1 + \cdots Am_s) \subset \mathfrak{p}$, hence $\operatorname{Ann} m_1 \cap \cdots \cap \operatorname{Ann} m_s \subset \mathfrak{p}$ and $\mathfrak{p} \in V(\operatorname{Ann} m_1 \cap \cdots \cap \operatorname{Ann} m_s)$. We conclude that $\operatorname{Supp} M = V(\operatorname{Ann} m_1 \cap \cdots \cap \operatorname{Ann} m_s) = V(\operatorname{Ann} M)$.

(e) Since $\operatorname{Supp} M$ is a closed Zariski subset by (d) and $V(\mathfrak{p})$ is the Zariski closure of the point $\mathfrak{p}$ by Exercise 33, we get the result.

□

Exercise 47. *Show that the support of a ring A is its spectrum,* $\operatorname{Supp} A = \operatorname{Spec} A$.

Example 36. *Let M be a $\mathbb{Z}$-module which is a finitely generated abelian group and, by the classification of these objects, it is isomorphic to*

$$M = \mathbb{Z}^r \oplus \mathbb{Z}/p_1^{n_1}\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/p_s^{n_s}\mathbb{Z} \tag{6.1}$$

where $p_1, \ldots, p_s$ are prime numbers (not necessarily distinct).

The prime ideals of $\operatorname{Spec} \mathbb{Z}$ *are* (0) *and the principal ideals $p\mathbb{Z}$, with p a prime number. If there is a free module part, i.e. $r \neq 0$, localizing at (0) yields $\mathbb{Q}^r$, the rings of fractions of the free module part and localizing with respect to any prime $p\mathbb{Z}$ yields non-zero localizations (they contain, at least, modules isomorphic to $\mathbb{Z}_{(p)}$).*

If M is a torsion module, i.e. $r = 0$, localizing at primes which do not appear in (6.1) yields zero but localizing at the primes appearing in (6.1) give non-zero local modules (show this as an exercise, use Exercise 44 (c) when localization commutes with quotients).

As a consequence, given (6.1), $\operatorname{Supp} M = \operatorname{Spec} \mathbb{Z}$ *if there is a free part $r \neq 0$, or* $\operatorname{Supp} M = \{p_1\mathbb{Z}, \ldots, p_s\mathbb{Z}\}$ *if M is torsion.*

Observe that there are annihilators of elements which are not prime, $\operatorname{Ann} p_i^{n_i}$*, but the varieties associated to these ideals are the same as the associated to the primes themselves,* $V(\operatorname{Ann} p_i^{n_i}) = V(\operatorname{Ann} p_i)$*. Also observe that once the ideal (0) is a supporting prime of M, all the variety $V(0) = \operatorname{Spec} \mathbb{Z}$ belongs to the support (this is the case when $r \neq 0$).*

Proposition 29 says that we can understand an A-module M by means of its support $\operatorname{Supp} M$ which contains the information of those non-zero localizations $M_{\mathfrak{p}}$. The elements $m \in M$ yield elements $m_{\mathfrak{p}} = \frac{m}{1}$ in each $A_{\mathfrak{p}}$-module $M_{\mathfrak{p}}$ called the **stalk** of M at $\mathfrak{p}$. This support is a Zariski closed set which is the union of the supports of several annihilators $\operatorname{Ann} m_i$. If the module is finite over A (which happens if M is noetherian, of if M is finite over A noetherian) this is a finite union. This way, we can understand the support of a module by understanding a finite number of components related to certain zero-divisors. These special zero-divisors are the associated primes.

Definition 49. *Let M be an A-module. A prime ideal $\mathfrak{p} \subset A$ is an* ***associated prime*** *of M if it is the annihilator ideal of an element $m \in M$, i.e. there exists $m \in M$ such that $\mathfrak{p} = \operatorname{Ann} m$. The set of associated primes of M will be denoted by* $\operatorname{Ass} M$.

Exercise 48. *Show that $\mathfrak{p} \in \operatorname{Ass} M$ if and only if M contains a submodule isomorphic to $A/\mathfrak{p}$ (hint: the submodule is Am, with $\mathfrak{p} = \operatorname{Ann} m$).*

Example 37. *Not all annihilators* $\operatorname{Ann} m$ *are prime: in the* $\mathbb{Z}$*-module* $\mathbb{Z}/60\mathbb{Z}$*, the ideal* $10\mathbb{Z} \subset \mathbb{Z}$ *is the annihilator of the element* $6 \in \mathbb{Z}/60\mathbb{Z}$*:*

$$\operatorname{Ann} 6 = \{n \in \mathbb{Z} \ : \ 6n = 0 \in \mathbb{Z}/60\mathbb{Z}\} = 10\mathbb{Z}$$

The associated primes of $\mathbb{Z}/60\mathbb{Z}$ *are* $(2) = 2\mathbb{Z} = \operatorname{Ann} 30$*,* $(3) = 3\mathbb{Z} = \operatorname{Ann} 10$ *and* $(5) = 5\mathbb{Z} = \operatorname{Ann} 6$*, the only prime numbers which can be annihilator ideals of elements in* $\mathbb{Z}/60\mathbb{Z}$*. Therefore* $\operatorname{Ass} \mathbb{Z}/60\mathbb{Z} = \{(2) = 2\mathbb{Z}, (3) = 3\mathbb{Z}, (5) = 5\mathbb{Z}\}$.

Let us now explore several properties of the associated primes of a module.

Proposition 30. *Let* M *be an* A*-module.*

(a) If $\mathfrak{p} = \operatorname{Ann} m$*,* $m \in M$*, is an associated prime of* M*, then for every* $0 \neq n \in Am$ *we have* $\operatorname{Ann} n = \mathfrak{p}$.

(b) For every $\mathfrak{p} \in \operatorname{Spec} A$*,* $\operatorname{Ass}(A/\mathfrak{p}) = \{\mathfrak{p}\}$.

(c) Any maximal element of the set of annihilator ideals $\{\operatorname{Ann} m \ : \ 0 \neq m \in M\}$ *is an associated prime belonging to* $\operatorname{Ass} M$.

(d) Given an exact sequence $0 \to L \to M \to N \to 0$*,* $\operatorname{Ass} M \subset \operatorname{Ass} L \cup \operatorname{Ass} N$.

Proof.

(a) By the Exercise 48, M contains the submodule Am isomorphic to $A/\mathfrak{p}$, which is an integral domain. Then, any non-zero element $n \in A/\mathfrak{p} = Am$ has the same annihilator, $\operatorname{Ann} n = \mathfrak{p}$.

(b) Since $A/\mathfrak{p}$ is generated by 1 as an A-module we have $\mathfrak{p} = \operatorname{Ann} 1 \subset M$. By (a), any other annihilator $\operatorname{Ann} n$, with $n \in A \cdot 1 = A/\mathfrak{p}$, is $\operatorname{Ann} n = \mathfrak{p}$.

(c) Let $\mathfrak{p} = \operatorname{Ann} m$ be maximal among all annihilator ideals and let us show that $\mathfrak{p}$ is a prime ideal. Let $f, g \in A$ such that $fg \in \mathfrak{p} = \operatorname{Ann} m$, then $fgm = 0$. Suppose that $gm = 0$, then $g \in \operatorname{Ann} m = \mathfrak{p}$. Suppose that $gm \neq 0$. Then $\operatorname{Ann} m \subset \operatorname{Ann} gm$ and, by maximality of $\operatorname{Ann} m$ we have $\mathfrak{p} = \operatorname{Ann} m = \operatorname{Ann} gm$, then $f \in \mathfrak{p}$.

(d) Let $\mathfrak{p} \in \operatorname{Ass} M$ and recall that M contains the submodule Am isomorphic to $A/\mathfrak{p}$. If $(A/\mathfrak{p}) \cap L = 0$, then $A/\mathfrak{p}$ maps isomorphically to a submodule of N, therefore $\mathfrak{p} \in \operatorname{Ass} N$. Otherwise $(A/\mathfrak{p}) \cap L \neq 0$; choose $0 \neq l \in A/\mathfrak{p} \cap L$, then by (a) $\operatorname{Ann} l = \mathfrak{p}$, hence $\mathfrak{p} \in \operatorname{Ass} L$. □

Remark 11. *Observe that Proposition 30 (d) for associated primes does nor need to give an equality as in Proposition 29 (c) for supports. Indeed, take a ring* A *and* $\mathfrak{p} \subset A$ *a prime ideal. The exact sequence* $0 \to \mathfrak{p} \to A \to A/\mathfrak{p} \to 0$ *gives (Exercise 47)*

$$\operatorname{Spec} A = \operatorname{Supp} A = \operatorname{Supp} \mathfrak{p} \cup \operatorname{Supp} A/\mathfrak{p}$$

which, if $\mathfrak{p} = (f)$ *is principal with* f *prime, can be written as*

$$\operatorname{Spec} A = \operatorname{Supp} A = \operatorname{Supp}(f) \cup \operatorname{Supp} A/(f) = V((f)) \cup D(f) \ ,$$

the support is the union of the variety defined by f and the distinguished complementary Zariski open set $D(f)$. However, if A is a domain, it has no associated primes other than zero, because it has no zero-divisors, but

$$\operatorname{Ass} A = (0) \subsetneq \operatorname{Ass} \mathfrak{p} \cup \operatorname{Ass} A/\mathfrak{p} = (0) \cup \{\mathfrak{p}\} .$$

Let us see that all associated primes are supporting primes.

Proposition 31. *Let M be an A-module. Then $\operatorname{Ass} M \subset \operatorname{Supp} M$.*

Proof. Let $\mathfrak{p} \in \operatorname{Ass} M$, then $A/\mathfrak{p} \subset M$. Localizing at $\mathfrak{p}$ (i.e. at the zero ideal of $A/\mathfrak{p}$) we get $0 \neq k(\mathfrak{p}) = \operatorname{Frac}(A/\mathfrak{p}) = (A/\mathfrak{p})_{\mathfrak{p}} \subset M_{\mathfrak{p}}$, then $\mathfrak{p} \in \operatorname{Supp} M$. □

Corollary 12. *If $\mathfrak{p}$ is an associated prime of an A-module M, then the irreducible closed Zariski set $V(\mathfrak{p})$ is contained in the support of M.*

Proof. Let $\mathfrak{q} \in V(\mathfrak{p})$ a prime ideal such that $\mathfrak{p} \subset \mathfrak{q}$. Then, by as similar argument as in the Exercise 46, $M_{\mathfrak{p}} = (M_{\mathfrak{q}})_{\mathfrak{p}} \neq 0$, then the module $M_{\mathfrak{q}}$ of the latter localization cannot be zero (otherwise the localization $(M_{\mathfrak{q}})_{\mathfrak{p}} = 0$), then $M_{\mathfrak{q}} \neq 0$ and $\mathfrak{q} \in \operatorname{Supp} M$. □

Let us end the section with stronger results for the case when A is a noetherian ring.

Proposition 32. *Let A be a noetherian ring and let $0 \neq M$ be an A-module.*

(a) M has, at least, one associate prime.

(b) The set of zero-divisors of M is the union of the associated primes.

Proof. (a) The set of annihilator ideals $\operatorname{Ann} m$, with $m \in M$, is non-empty. Since A is noetherian, this set has a maximal element, which is a prime ideal by Proposition 30 (c), hence $\operatorname{Ass} M \neq \emptyset$.

(b) Every zero-divisor of M is an element $a \in A$ such that $a \in \operatorname{Ann} m$, with $m \in M$. And $\operatorname{Ann} m$ is contained in a maximal element which is an associated prime by (a).

□

Theorem 11. *Let A be a noetherian ring and let M be an A-module. Every irreducible component $V(\mathfrak{p}) \subset \operatorname{Supp} M$ (i.e. minimal prime in $\operatorname{Supp} M$) yields an associated prime $\mathfrak{p} \in \operatorname{Ass} M$.*

Proof. Let $\mathfrak{p}$ be a prime ideal which is minimal among those in $\operatorname{Supp} M$. This means that the localization $M_{\mathfrak{p}} \neq 0$ but for every smaller prime $\mathfrak{q} \subsetneq \mathfrak{p}$ we have $M_{\mathfrak{q}} = 0$.

Consider the $A_{\mathfrak{p}}$-module $M_{\mathfrak{p}} \neq 0$. By Proposition 32 (a), $\operatorname{Ass} M_{\mathfrak{p}} \neq \emptyset$. It is clear that the maximal ideal $\mathfrak{p}A_{\mathfrak{p}}$ of the local ring $A_{\mathfrak{p}}$ is an associated prime of $M_{\mathfrak{p}}$, let us see that there are not any more. Let $\mathfrak{q}' \subset A_{\mathfrak{p}}$ be a prime ideal, which is of the form $\mathfrak{q}' = \mathfrak{q}A_{\mathfrak{p}}$ with $\mathfrak{q} \cap (A \backslash \mathfrak{p}) = \emptyset$, then $\mathfrak{q} \subset \mathfrak{p}$ (see Exercise 40). Then, the localization $(M_{\mathfrak{p}})_{\mathfrak{q}'} = M_{\mathfrak{q}} = 0$ unless $\mathfrak{q}' = \mathfrak{p}A_{\mathfrak{p}}$. Hence, $\operatorname{Supp} M_{\mathfrak{p}} = \{\mathfrak{p}A_{\mathfrak{p}}\}$. Since $\emptyset \neq \operatorname{Ass} M_{\mathfrak{p}} \subset \operatorname{Supp} M_{\mathfrak{p}} = \{\mathfrak{p}A_{\mathfrak{p}}\}$ we arrive at $\operatorname{Ass} M_{\mathfrak{p}} = \{\mathfrak{p}A_{\mathfrak{p}}\}$. This has so far solved the question locally: the general point of the component $V(\mathfrak{p})$ gives the unique associated prime of the local module $M_{\mathfrak{p}}$.

Now, since $\mathfrak{p}A_\mathfrak{p}$ is an associated prime of $M_\mathfrak{p}$, let $0 \neq \frac{m}{s} \in M_\mathfrak{p}$ such that $\operatorname{Ann} \frac{m}{s} = \mathfrak{p}A_\mathfrak{p}$, where $m \in M$ and $s \in A\backslash\mathfrak{p}$. We claim that $\operatorname{Ann} tm \subset \mathfrak{p}$ for every $t \in A\backslash\mathfrak{p}$. Indeed, if $u \in A\backslash\mathfrak{p}$ were to make $utm = 0$, then m goes to a non-zero element under the map $M \to M_\mathfrak{p}$, and t, u go to units, hence a contradiction.

The end of the proof is to show that we can find a $t \in A\backslash\mathfrak{p}$ such that $\operatorname{Ann} tm = \mathfrak{p}$, therefore $\mathfrak{p} \in \operatorname{Ass} M$. Since $\operatorname{Ann} \frac{m}{s} = \mathfrak{p}A_\mathfrak{p}$, every $f \in \mathfrak{p}$ produces $\frac{f}{1} \cdot \frac{m}{s} = 0$, which means that there exists an element $t \in A\backslash\mathfrak{p}$ with $tfm = 0$. Since A is noetherian, $\mathfrak{p}$ is finitely generated, then there exist $f_1, \ldots, f_k \in A$ such that $\mathfrak{p} = (f_1, \ldots, f_k)$, and choose elements $t_i \in A\backslash\mathfrak{p}$ with this condition, i.e. $t_i f_i m = 0$. Defining $t := t_1 \cdots t_k$, the annihilator ideal $\operatorname{Ann} tm$ contains all generators f_i, then it contains $\mathfrak{p}$ and $\operatorname{Ann} tm = \mathfrak{p}$. Therefore, $\mathfrak{p} \in \operatorname{Ass} M$. □

Corollary 13. *Let A be a noetherian ring and let M be a finite A-module. The support of M is a finite union of its irreducible components $V(\mathfrak{p}_i)$, where $\mathfrak{p}_i \in \operatorname{Ass} M$ and these $\mathfrak{p}_i$ are the minimal associated primes which contain $\operatorname{Ann} M$.*

Proof. By Proposition 29 (d) we have that $\operatorname{Supp} M = V(\operatorname{Ann} M)$ and by Exercise 34 (a) $V(\operatorname{Ann} M)$ consists of a finite number of irreducible closed subsets $V(\mathfrak{p}_i)$ where each $\mathfrak{p}_i$ is a minimal prime containing $\operatorname{Ann} M$. By Theorem 11, these primes $\mathfrak{p}_i$ belong to $\operatorname{Ass} M$. □

Moreover, we can decompose a module inductively by extracting the associated prime components recursively.

Proposition 33. *Let A be a noetherian ring and let M be a finite A-module. Then there exists a chain of submodules*

$$0 = M_0 \subset M_1 \subset \cdots \subset M_n = M$$

such that $M_1/M_{i-1} \simeq A/\mathfrak{p}_i$, where $\mathfrak{p}_i \in \operatorname{Spec} A$, $i = 1, \ldots, n$. Therefore $\operatorname{Ass} M \subset \{\mathfrak{p}_1, \ldots, \mathfrak{p}_n\}$ and there are a finite number of associated primes in M.

Proof. By Proposition 32 there exists, at least, one associated prime $\mathfrak{p}_1$. Then, there exists a submodule $M_1 \simeq A/\mathfrak{p}_1 \subset M$. By induction, assume that we have a chain $0 = M_0 \subset M_1 \subset \cdots \subset M_i \subset M$ and $M/M_i \neq 0$, then there exists another associated prime $\mathfrak{p}_{i+1}$ and a sumbodule $N \simeq A/\mathfrak{p}_{i+1} \subset M/M_i$, whose inverse image by $\pi : M \to M/M_i$, $M_{i+1} := \pi^{-1}(N)$ yields a enlarged chain $0 = M_0 \subset M_1 \subset \cdots \subset M_i \subset M_{i+1} \subset M$ which has to stop eventually, because M is noetherian. □

Example 38. *Let $A = k[X, Y]$ and let $I = (X^2Y)$ be an ideal. The A-module $A/I = k[X, Y]/(X^2Y)$ contains polynomials of the form $f(X) + g(Y) + Xh(Y)$ and geometrically represents functions over the union of the axis X and Y, where Y is doubled. The annihilator of the module A/I is clearly the ideal $(X^2Y) \subset k[X, Y]$ which is the intersection of the annihilators $(X) = \operatorname{Ann} XY$, $(X^2) = \operatorname{Ann} Y$, $(Y) = \operatorname{Ann} X^2$ and $(XY) = \operatorname{Ann} X$. The support of the module A/I is the union of the supports of these annihilators: $\operatorname{Supp}(X)$ and $\operatorname{Supp}(X^2)$ are the vertical axis, $\operatorname{Supp}(Y)$ is the horizontal axis and $\operatorname{Supp}(XY)$ is union of the axes. Observe that $\operatorname{Spec}(X) = \operatorname{Supp}(X) = \operatorname{Spec}(X^2) = \operatorname{Supp}(X^2)$, hence $\operatorname{Supp} A/I$ is the union of the axes (and nothing more!). However, we can express the support as the union of just two varieties of annihilators, those which are minimal primes, i.e. $\operatorname{Supp} A/I = V((X)) \cup V((Y))$.*

6.2 Primary ideals

Let us explore the generalization of a power of a prime ideal, which are the primary ideals.

Definition 50. *An ideal $\mathfrak{q} \subset A$ is a **primary ideal** if $\mathfrak{q} \neq A$ and given elements $f, g \in A$ such that $fg \in \mathfrak{q}$, then either $f \in \mathfrak{q}$ or there exists $n \in \mathbb{N}$ such that $g^n \in \mathfrak{q}$.*

Exercise 49. *Show that an ideal $\mathfrak{q} \subset A$ is primary if $A/\mathfrak{q} \neq 0$ and every zero-divisor in $A/\mathfrak{q}$ is nilpotent.*

Given an ideal $I \subset A$, the radical $\sqrt{I}$ is not always a prime ideal. For example the radical of $I = (X^2Y^3) \subset k[X,Y]$ is $\sqrt{(X^2Y^3)} = (XY)$. However, the radical of a primary ideal is a prime ideal.

Proposition 34. *Let $\mathfrak{q} \subset A$ be a primary ideal. Then, its radical $\sqrt{\mathfrak{q}}$ is a prime ideal.*

Proof. Let $fg \in \sqrt{\mathfrak{q}}$ and suppose that $f \notin \sqrt{\mathfrak{q}}$. Since $\mathfrak{q} \subset \sqrt{\mathfrak{q}}$ we have $f \notin \mathfrak{q}$ and, since $\mathfrak{q}$ is primary, there exists an $n \in \mathbb{N}$ such that $g^n \in \mathfrak{q}$, therefore $g \in \sqrt{\mathfrak{q}}$. □

Definition 51. *We will say that a primary ideal $\mathfrak{q}$ is $\mathfrak{p}$-**primary** if its radical $\sqrt{\mathfrak{q}}$ is equal to the prime ideal $\mathfrak{p}$.*

Example 39. *The primary ideals in $\mathbb{Z}$ are the powers of a prime ideal. Indeed, let $\mathfrak{q} = (p^n) \subset \mathbb{Z}$ be an ideal with p a prime number and $n \in \mathbb{N}$. Then, if $a, b \in \mathbb{Z}$ with $ab \in (p^n)$, then it is clear that at least one of then, say a, has a power such that $a^m \in (p^n)$. Observe that $\sqrt{\mathfrak{q}} = \sqrt{(p^n)} = (p)$ and $\mathfrak{q} = (p^n)$ is (p)-primary.*

Reciprocally, if $(n) \subset \mathbb{Z}$ is an ideal such that n has two different primes p, q in its arithmetic decomposition, then p and q are zero-divisors in $\mathbb{Z}/n\mathbb{Z}$ but they are not nilpotents (Exercise 49), then (n) is not a primary ideal.

Exercise 50. *Show that the previous example just requires the ring to be a PID. This is, let A be a PID, then its primary ideals are of the form $\mathfrak{q} = \mathfrak{p}^n$, powers of prime ideals $\mathfrak{p}$.*

Exercise 51. *Prove that, if $\mathfrak{p} \subset A$ is a prime ideal, then $\sqrt{\mathfrak{p}^n} = \mathfrak{p}$, $n \in \mathbb{N}$. Find a counterexample to this equality if $I \subset A$ is a non-prime ideal.*

In general, being a primary ideal and being a power of a prime ideal are different concepts.

Example 40. *Let $A = k[X,Y]$ and let $\mathfrak{q} = (X^2, Y)$ be an ideal. Then, $\mathfrak{q}$ is $\mathfrak{p}$-primary with $\mathfrak{p} = (X,Y)$. Indeed, the quotient $A/\mathfrak{q} = k[X,Y]/(X^2,Y) \simeq k[X]/(X^2)$, which is not zero and whose zero-divisors are the multiples of X, which are all nilpotents. It is also clear that $\sqrt{\mathfrak{q}} = \sqrt{(X^2,Y)} = (X,Y)$. However, $\mathfrak{q}$ is not a power of any prime ideal of A.*

Example 41. *Let $A = k[W] = k[X,Y,Z]/(XZ - Y^2)$ be the coordinate ring of the affine cone $W = \{(x,y,z) \in k^3 \ : \ xz - y^2 = 0\}$. Let $\overline{X}, \overline{Y}, \overline{Z}$ be the images of X, Y, Z on A and consider the ideal $\mathfrak{p} = (\overline{X}, \overline{Y}) \subset A$, which is prime because $A/\mathfrak{p} \simeq k[Z]$, which is an integral domain. Let $\mathfrak{p}^2$ the square power of $\mathfrak{p}$ and let us see that $\mathfrak{p}^2$ is not primary: $\overline{XZ} = \overline{Y}^2 \in \mathfrak{p}^2$ but $\overline{X} \notin \mathfrak{p}^2$ and $\overline{Z} \notin \sqrt{\mathfrak{p}^2} = \mathfrak{p}$.*

What is true is that a primary ideal, whose radical is finitely generated, contains a power of its radical.

Proposition 35. *Let $\mathfrak{q}$ be a $\mathfrak{p}$-primary ideal with $\mathfrak{p}$ finitely generated. Then there exists an $m \in \mathbb{N}$ such that $\mathfrak{p}^m \subset \mathfrak{q} \subset \mathfrak{p}$.*

Proof. Let $\mathfrak{p} = \sqrt{\mathfrak{q}} = (f_1, \dots, f_s)$ be finitely generated. Then, there exist integers $n_1, \dots, n_s \in \mathbb{N}$ such that $f_i^{n_i} \in \mathfrak{q}$. Let $m := (\sum_{i=1}^s (n_i - 1)) + 1$ and observe that $\mathfrak{p}^m$ is generated by all the products $\prod_{i=1}^s f_i^{r_i}$ with $\sum_{i=1}^s r_i = m$. Then, from the definition of m we see that there exists, at least, an index i such that $r_i \geq n_i$, therefore $\prod_{i=1}^s f_i^{r_i} \in \mathfrak{q}$ for every $i = 1, \dots, s$, hence $\mathfrak{p}^m \subset \mathfrak{q}$. □

Remark 12. *Proposition 35 is more general for noetherian rings: in fact, every ideal (not-necessarily primary) contains a power of its radical [AM, Proposition 7.14].*

For maximal ideals it is true that their powers are primary ideals.

Proposition 36. *Let $I \subset A$ be an ideal such that its radical $\sqrt{I} = \mathfrak{m}$ is a maximal ideal. Then, I is $\mathfrak{m}$-primary. In particular, the powers $\mathfrak{m}^n$ of a maximal ideal $\mathfrak{m}$ are $\mathfrak{m}$-primary.*

Proof. Let $f \in A \backslash I$ and form the set $J := \{g \in A \ : \ fg \in I\}$, which is an ideal such that $I \subset J \subsetneq A$ (otherwise J contains a unit and $f \in I$). Therefore, there exists a maximal ideal K such that $I \subset J \subset K \subsetneq A$. By Proposition 3, $\sqrt{I}$ is the intersection of all the prime ideals containing I. Since $\sqrt{I} = \mathfrak{m}$ is maximal , there is only one maximal ideal containing I, hence $K = \mathfrak{m}$. Therefore, for $fg \in I$, then $g \in J$, we have $g \in J \subset K = \mathfrak{m} = \sqrt{I}$, hence $g^n \in I$ and I is $\mathfrak{m}$-primary. □

The idea of primary decomposition is the abstraction of the Fundamental Theorem of arithmetics in the PID $\mathbb{Z}$, stating that an integer can be factored as a product of powers of primes in a unique way, up to units. This is, given $n \in \mathbb{Z}$, there exists distinct prime numbers $p_1, \dots, p_s \in \mathbb{Z}$ such that $n = up_1^{n_1} \cdots p_s^{n_s}$, where $u = \pm 1$ is a unit. In terms of ideals, this means that there exists a primary decomposition

$$(n) = (p_1)^{n_1} \cap \cdots \cap (p_s)^{n_s}$$

where $(p_i)^{n_i}$ are distinct (p_i)-primary ideals (see Exercise 50) and (n) is not contained in an intersection of less than these primary ideals.

Definition 52. *Let A be a ring and let $I \subset A$ be an ideal. A **(minimal) primary decomposition** of I is*

$$I = \mathfrak{q}_1 \cap \cdots \cap \mathfrak{q}_s$$

where each $\mathfrak{q}_i$ is $\mathfrak{p}_i$-primary with $\mathfrak{p}_i \neq \mathfrak{p}_j$, $i \neq j$, and such that the decomposition is minimal, i.e. for every i, $I \subsetneq \cap_{i \neq j} \mathfrak{q}_j$.

Observe that once there exists a primary decomposition there exists a minimal one as in Definition 52: we can make any primary decomposition into a minimal one by eliminating redundant primary ideals:

Exercise 52. *Let $\mathfrak{q}_1$, $\mathfrak{q}_2$ be $\mathfrak{p}$-primary ideals. Then $\mathfrak{q}_1 \cap \mathfrak{q}_2$ is $\mathfrak{p}$-primary.*

A primary decomposition, when it exists, is not necessarily unique.

Example 42. *Let $I = (X^2, XY) \subset k[X,Y]$ be an ideal. The elements of $k[X,Y]/I$ are polynomials of the form $a + bX + c_1Y + \cdots + c_nY^n$. On the one hand, I admits the primary decomposition $I = (X) \cap (X,Y)^2$. Observe that (X) is prime, then (X)-primary, and (X,Y) is maximal, then by Proposition 36 its square $(X,Y)^2$ is (X,Y)-primary. On the other hand, see that I also admits the different primary decomposition $I = (X) \cap (X^2, Y)$, where we can easily see that (X^2,Y) is (X,Y)-primary.*

Indeed, we have any primary decomposition of the form $I = (X) \cap (X^2, Y - \lambda X)$, with $\lambda \in k$. We can consider the isomorphism $k[X,Y] \simeq k[X, Y-\lambda X]$ and, then, $k[X,Y-\lambda X]/(X^2, Y-\lambda X) \simeq k[X]/(X^2)$, which is a non-zero ring where every zero-divisor is nilpotent (Exercise 49). The radical of this ideal is also (X,Y): note that $(X^2, Y-\lambda X) = (X,Y)^2 + (Y - \lambda X)$ and use that $\sqrt{I+J} = \sqrt{\sqrt{I} + \sqrt{J}}$ (exercise) to conclude

$$\sqrt{(X^2, Y-\lambda X)} = \sqrt{(X,Y)^2 + (Y-\lambda X)} = \sqrt{\sqrt{(X,Y)^2} + \sqrt{Y - \lambda X}} =$$

$$\sqrt{(X,Y) + (Y - \lambda X)} = \sqrt{(X,Y)} = (X,Y)\ .$$

*All of these decompositions exhibit $k[X,Y]/I$ as the ring of coordinates of the vertical line extra information in the origin (the coefficient b in the polynomial functions of $k[X,Y]/I$), but they encode differently this extra information. The minimal primes (radicals of the primary ideals) in all decompositions, i.e. the prime (X), is common (see Corollary 13). These are the **maximal components** of the module: in this case the vertical line is the maximal component coming from* $\operatorname{Spec} k[X,Y]/I$.

*However, the other primary ideals are different, yielding **embedded components** as is the case of the origin here. The primary ideals represent the extra information on polynomials as different forms of extra vanishing at the origin. However, note that the prime (maximal) ideal (X,Y) associated to the different primary decompositions is always the same.*

This represent the situation that we will encounter for the primary decomposition of an ideal in a noetherian ring: there always exists a primary decomposition (Theorem 13) although it is not unique; however, the associated primes radicals of the primary ideals are unique (Theorem 14) and the maximal components coming from minimal primes are unique (Theorem 15).

6.3 Existence and uniqueness of primary decompositions

We conclude the chapter with a study of the cases where we can assure that there exists a primary decomposition, and which information coming from different decompositions remains the same.

First, let us see that, in the noetherian case, there is only one associated prime for quotients by a primary ideal.

Theorem 12. *Let A be a noetherian ring. An ideal $\mathfrak{q} \subset A$ is $\mathfrak{p}$-primary ideal if and only if* $\operatorname{Ass}(A/\mathfrak{q}) = \{\mathfrak{p}\}$.

Proof. Let $\mathfrak{q} \subset A$ be a $\mathfrak{p}$-primary ideal. Since $A/\mathfrak{q}$ is a noetherian module, by Proposition 32 (a) we have $\operatorname{Ass}(A/\mathfrak{q}) \neq \emptyset$. Let I be an associated prime of $A/\mathfrak{q}$ and let us show that $I = \mathfrak{p}$. There exists an element $m \in A/\mathfrak{q}$ such that $\mathfrak{q} \subset I = \operatorname{Ann} m$. Since the elements of $\operatorname{Ann} m$ are zero-divisors of $A/\mathfrak{q}$, these are nilpotent (Exercise 49), then $\mathfrak{q} \subset I = \operatorname{Ann} m \subset \sqrt{\mathfrak{q}} = \mathfrak{p}$. Then, $\sqrt{I} = \sqrt{\mathfrak{q}} = \mathfrak{p}$. But $I = \operatorname{Ann} m$ is already a prime ideal, therefore a radical ideal, hence $I = \sqrt{I} = \mathfrak{p}$.

Conversely, assume that $\operatorname{Ass}(A/\mathfrak{q}) = \{\mathfrak{p}\}$ and let us show that $\mathfrak{q}$ is $\mathfrak{p}$-primary. We first show that for every non-trivial submodule $0 \neq M \subset A/\mathfrak{q}$, it is $\sqrt{\operatorname{Ann} M} = \mathfrak{p}$. Observe that $\operatorname{Ass}(A/\mathfrak{q}) = \{\mathfrak{p}\}$ implies $\operatorname{Ass} M = \{\mathfrak{p}\}$ (note that $A/\mathfrak{q}$ is generated by 1 as an A module and then, any submodule M is generated by one element and use Proposition 30 (a)). Now, since $\sqrt{\operatorname{Ann} M}$ is the intersection of all prime ideals containing $\operatorname{Ann} M$ (Proposition 3), taking the intersection over the minimal primes, which are the primes of $\operatorname{Supp} M$ and which are in $\operatorname{Ass} M$ (see Theorem 11), then $\sqrt{\operatorname{Ann} M} = \mathfrak{p}$. Applying this to $M = A/\mathfrak{q}$ itself we obtain that $\mathfrak{q} = \operatorname{Ann} A/\mathfrak{q}$ and $\sqrt{\mathfrak{q}} = \mathfrak{p}$.

Now, let $f, g \in A$ be elements such that $fg \in \mathfrak{q}$ but $f \notin \mathfrak{q}$. Denote $\overline{f} \in A/\mathfrak{q}$ the image of f in the quotient $A/\mathfrak{q}$. We have that $g \in \operatorname{Ann} \overline{f}$, which is an ideal, then $g \in \operatorname{Ann} \overline{f} \subset \sqrt{\operatorname{Ann} \overline{f}} = \mathfrak{p} = \sqrt{\mathfrak{q}}$ (where we have applied the part before with $M = \operatorname{Ann} \overline{f}$). Therefore, $g \in \sqrt{q}$, and there exists an $n \in \mathbb{N}$ with $g^n \in \mathfrak{q}$, then $\mathfrak{q}$ is $\mathfrak{p}$-primary. □

Example 43. *Let $A = k[X, Y]$ and consider the primary ideal $\mathfrak{q} = (X^n, Y^m)$, $n, m \in \mathbb{N}$, whose radical is $\mathfrak{p} = \sqrt{(X^n, Y^m)} = (X, Y)$. The quotient $A/\mathfrak{q} = k[X, Y]/(X^n, Y^m)$ contains (as representatives of the equivalence classes) polynomials of the form $f(X, Y) = \sum_{i,j} a_{ij} X^i Y^j$, $0 \leq i \leq n, 0 \leq j \leq m$. There are several annihilator ideals of elements of $A/\mathfrak{q}$, for example, (X^2, Y^3) annihilates the element $X^{n-2}Y^{m-3}$. However, there is just one annihilator which is prime, $(X, Y) = \operatorname{Ann} X^{n-1}Y^{m-1}$.*

Note that the support $\operatorname{Supp} A/\mathfrak{q}$ is just one point, the maximal ideal $\mathfrak{p} = (X, Y)$ corresponding to the origin in k^2, then we have just one associated prime (X, Y) as in Theorem 12.

Let us prove Emmy Noether's most important result in algebra: in a Noetherian ring, every ideal has a primary decomposition. The theorem is a consequence of two lemmas regarding the notion of indecomposable ideal.

Definition 53. *An ideal $I \subset A$ is **indecomposable** if it cannot be written as an intersection of two strictly bigger ideals, i.e. if $I = J \cap K$, then either $I = J$ or $I = K$.*

Exercise 53. *Show that a prime ideal is indecomposable.*

Lemma 4. *Let A be a Noetherian ring. Every ideal $I \subset A$ can be expressed as a finite intersection of indecomposable ideals.*

Proof. Consider the set Σ of ideals of A which cannot be expressed as a finite intersection of indecomposable ideals, and assume it is non-empty. Since A is Noetherian, this set Σ has a maximal element K, which is necessarily a decomposable ideal (otherwise $K \notin \Sigma$), hence $K = I \cap J$ with $K \subsetneq I$, $K \subsetneq J$. Then, by maximality of K, these two ideals I and J are, in fact, finite intersections of indecomposable ideals, and so is K, which is a contradiction. Then Σ is empty and every ideal of A can be expressed as a finite intersection of indecomposable ideals. □

Lemma 5. *Let A be a Noetherian ring. Every proper indecomposable ideal is a primary ideal.*

Proof. By the correspondence (1.3) between ideals through quotients it is equivalent that $I \subset A$ is indecomposable (resp. primary) to $(0) \subset A/I$ is indecomposable (resp. primary), then we will show that, in a Noetherian ring A, if (0) is indecomposable, then (0) is primary.

Let $f, g \in A$ such that $fg = 0$. Then $g \in \operatorname{Ann} f$ and consider the chain

$$\operatorname{Ann} f \subset \operatorname{Ann} f^2 \subset \cdots \subset \operatorname{Ann} f^n \subset \cdots$$

which stabilizes because A is Noetherian, then $\operatorname{Ann} f^n = \operatorname{Ann} f^{n+1}$, for some $n \in \mathbb{N}$. Let us show that $(f^n) \cap (g) = (0)$. Let $a \in (f^n) \cap (g)$, then there exists an element $b \in A$ with $a = bg$, hence $af = bgf = 0$. Also, there exists an element $c \in A$ with $a = cf^n$, then $0 = af = cf^{n+1}$, hence $c \in \operatorname{Ann} f^{n+1} = \operatorname{Ann} f^n$, therefore $0 = cf^n = a$. Finally, if (0) is indecomposable, either $f^n = 0$ or $g = 0$, hence (0) is primary. □

Theorem 13 (**Existence of primary decomposition for noetherian rings**). *Let A be a noetherian ring. Every proper ideal I has a primary decomposition.*

Proof. It is a consequence of Lemma 4 and Lemma 5. □

Remark 13. *Observe that the notions of decomposable ideal and primary ideal are different. The ideal $(X, Y) \subset k[X, Y]$ is obviously primary (it is prime and maximal) but it is decomposable: $(X, Y) = (X^2, Y) \cap (X, Y^2)$. Noether's Theorem 13 proves that every ideal in a Noetherian ring has a primary decomposition by showing that is has a finite indecomposable decomposition and these indecomposable ideals are, indeed, primary ideals.*

As we have seen in Example 42 primary decompositions are not unique. However, in the noetherian case, the associated primes of the quotient ring are equal and uniquely determined by the ideal in the different primary decompositions.

Theorem 14 (**1st uniqueness theorem**). *Let A be a noetherian ring, let $I \subset A$ be an ideal and let $I = \mathfrak{q}_1 \cap \cdots \cap \mathfrak{q}_s$ be a minimal primary decomposition where each $\mathfrak{q}_i$ is $\mathfrak{p}_i$-primary. Then,*

$$\operatorname{Ass}(A/I) = \{\mathfrak{p}_1, \ldots, \mathfrak{p}_s\}$$

and the associated primes of the quotient are uniquely determined by I.

Proof. Let $I = \mathfrak{q}_1 \cap \cdots \cap \mathfrak{q}_s$ be a minimal primary decomposition and consider the inclusion map

$$A/I \hookrightarrow \bigoplus_{i=1}^{s} A/\mathfrak{q}_i \tag{6.2}$$

Then, every associated prime of A/I is an associated prime of some $A/\mathfrak{q}_i$, hence $\operatorname{Ass}(A/I) \subset \bigcup_{i=1}^{s} \operatorname{Ass}(A/\mathfrak{q}_i) = \{\mathfrak{p}_1, \ldots, \mathfrak{p}_s\}$, since each $\mathfrak{q}_i$ is $\mathfrak{p}_i$-primary (Theorem 12). Since the primary decomposition is minimal, for every $j = 1, \ldots, s$, the ideal $\cap_{i \neq j} \mathfrak{q}_i / I \subset A/I$ is non-empty, therefore by (6.2) we have $\cap_{i \neq j} \mathfrak{q}_i / I \hookrightarrow A/\mathfrak{q}_j$, the inclusion being zero in the other summands. Again by Theorem 12 we have that $\operatorname{Ass}(A/\mathfrak{q}_j) = \{\mathfrak{p}_j\}$, hence, A/I contains the non-zero submodule $\cap_{i \neq j} \mathfrak{q}_i / I$ with $\operatorname{Ass}(\cap_{i \neq j} \mathfrak{q}_i / I) \subset \{\mathfrak{p}_j\}$. But, $(\cap_{i \neq j} \mathfrak{q}_i / I)$ is a noetherian A-module, then it has at least one associated prime by Proposition 30 (a). Therefore, $(\cap_{i \neq j} \mathfrak{q}_i / I)$ contains a submodule isomorphic to $A/\mathfrak{p}_i$ (Exercise 48) and so does A/I, then $\mathfrak{p}_j \in \operatorname{Ass}(A/I)$, completing the proof. □

Example 44. *The decompositions in Example 42 yield the same two associated primes in* $A/I = k[X,Y]/(X^2, XY)$*, which are* $\mathfrak{p}_1 = (X)$*,* $\mathfrak{p}_2 = (X,Y)$*. Observe that the primary ideals* $(X,Y)^2$*,* (X^2, Y) *and* $(X^2, Y - \lambda X)$*,* $\lambda \in k$*, have the same prime radical* (X,Y)*.*

Example 45. *Recall from Example 41 the ring* $A = k[W] = k[X,Y,Z]/(XZ - Y^2)$ *which is the coordinate ring of the cone* $W = \{(x,y,z) \in k^3 \ : \ xz - y^2 = 0\}$*. Let* $\mathfrak{p} = (\overline{X}, \overline{Y}) \subset k[X,Y,Z]/(XZ - Y^2)$ *be the ideal of functions defined on the cone* W *which vanish along the line* $L = \{X = Y = 0\}$*, i.e. vanishing at the apex* $(0,0,0)$ *of the cone* W*.*

Consider the ideal $\mathfrak{p}^2$*, which is not primary (Example 41) but has a primary decomposition by Theorem 13. One of these primary decompositions can be:*

$$\mathfrak{p}^2 = (\overline{X}^2, \overline{XY}, \overline{Y}^2) = (\overline{X}) \cdot (\overline{X}, \overline{Y}, \overline{Z}) = (\overline{X}) \cap (\overline{X}, \overline{Y}, \overline{Z})^2$$

where $\mathfrak{q}_1 = (\overline{X})$ *is* $\mathfrak{p}_1 = (\overline{X})$*-primary (it is, in fact, already prime) and* $\mathfrak{q}_2 = (\overline{X}, \overline{Y}, \overline{Z})^2$ *is* $\mathfrak{p}_2 = (\overline{X}, \overline{Y}, \overline{Z})$*-primary (it is a power of a maximal ideal, Proposition 36). By Theorem 14 the associated primes of* $A/\mathfrak{p}^2$ *are precisely* $\mathfrak{p}_1 = (\overline{X})$ *and* $\mathfrak{p}_2 = (\overline{X}, \overline{Y}, \overline{Z})$*, where* $(\overline{X})$ *is the maximal component of the module* $\mathfrak{p}^2$ *and* $(\overline{X}, \overline{Y}, \overline{Z})^2$ *is an extra embedded component imposing an extra vanishing condition. Note that*

$$A/\mathfrak{p}^2 \simeq k[X,Y,Z]/(XZ - Y^2, X^2, XY, Y^2) = k[X,Y,Z]/(XZ, X^2, XY, Y^2)\ ,$$

as a $k[W]$*-module, then the associated primes are annihilators of certain elements, for example* $\mathfrak{p}_1 = (\overline{X}) = \operatorname{Ann}(\overline{Y} + \overline{Z})$ *and* $\mathfrak{p}_2 = (\overline{X}, \overline{Y}, \overline{Z}) = \operatorname{Ann} \overline{X}$*.*

We end the chapter by stating a second uniqueness theorem regarding the minimal primary component. Recall from Proposition 24 (d) that, for each multiplicative set S and each prime ideal $\mathfrak{p} \subset A$ disjoint with S, $e(\mathfrak{p}) = S^{-1}\mathfrak{p}$ is a prime ideal of $S^{-1}A$.

Exercise 54. *Let* S *be a multiplicative set of* A *and let* $\varphi : A \to S^{-1}A$ *be the corresponding ring homomorphism. Let* $\mathfrak{q}$ *be a* $\mathfrak{p}$*-primary ideal such that* $S \cap \mathfrak{p} = \emptyset$*. Show that* $S^{-1}\mathfrak{q}$ *is* $S^{-1}\mathfrak{p}$*-primary and* $\varphi^{-1}(S^{-1}\mathfrak{q}) = \mathfrak{q}$*.*

Proposition 37. *Let* S *be a multiplicative set of* A*, let* $I \subset A$ *be an ideal and let* $I = \mathfrak{q}_1 \cap \cdots \cap \mathfrak{q}_s$ *be a minimal primary decomposition where each* $\mathfrak{q}_i$ *is* $\mathfrak{p}_i$*-primary. Assume that* $S \cap \mathfrak{p}_i = \emptyset$ *for* $i = 1, \ldots, m$ *and* $S \cap \mathfrak{p}_i \neq \emptyset$ *for* $i = m+1, \ldots, s$*. Then,* $S^{-1}I = S^{-1}\mathfrak{q}_1 \cap \cdots \cap S^{-1}\mathfrak{q}_m$ *and* $\varphi^{-1}(S^{-1}I) = \mathfrak{q}_1 \cap \cdots \cap \mathfrak{q}_m$*.*

Proof. It is a consequence of Exercise 44 (b) and Exercise 54. □

Definition 54. *Let* $I = \mathfrak{q}_1 \cap \cdots \cap \mathfrak{q}_s$ *be a minimal primary decomposition where each* $\mathfrak{q}_i$ *is* $\mathfrak{p}_i$*-primary. We say that a subset of the prime ideals* $\Xi \subset \{\mathfrak{p}_1, \ldots, \mathfrak{p}_s\}$ *is* ***isolated*** *if for every* i, j *such that* $\mathfrak{p}_j \in \Xi$ *and* $\mathfrak{p}_i \subset \mathfrak{p}_j$*, we have* $\mathfrak{p}_i \in \Xi$*.*

Theorem 15 (2nd uniqueness theorem). *Let* $I \subset A$ *be an ideal and let* $I = \mathfrak{q}_1 \cap \cdots \cap \mathfrak{q}_s$ *be a minimal primary decomposition where each* $\mathfrak{q}_i$ *is* $\mathfrak{p}_i$*-primary. If* $\Xi \subset \{\mathfrak{p}_1, \ldots, \mathfrak{p}_s\}$ *is isolated then the intersection* $\bigcap_{i:\mathfrak{p}_i \in \Xi} \mathfrak{q}_i$ *is independent of the primary decomposition. In particular, if* $\mathfrak{p}_1$ *is the minimal prime among* $\mathfrak{p}_1, \ldots, \mathfrak{p}_s$*, then the isolated primary component corresponding to* $\mathfrak{q}_1$ *is uniquely determined by* I*.*

Proof. Let Ξ be a subset of isolated primes where $\mathfrak{p}_1, \ldots, \mathfrak{p}_m \in \Xi$ are the minimal primes of this isolated set. For each $i = 1, \ldots, m$ apply Proposition 37 with $S = A \backslash \mathfrak{p}_i$ to conclude that $\varphi^{-1}(S^{-1}I) = \mathfrak{q}_i$, hence the intersection $\bigcap_{i:\mathfrak{p}_i \in \Xi} \mathfrak{q}_i$ is independent of the primary decomposition. In particular, if $m = 1$, i.e. there is just one minimal prime $\mathfrak{p}_1$, the isolated primary component corresponding to $\mathfrak{q}_1$ is also independent of the primary decomposition and uniquely determined by I. □

Example 46. *Notice that, in Example 42, for the ideal $I = (X^2, XY) \subset k[X, Y]$ admitting $I = (X) \cap (X, Y)^2 = (X) \cap (X^2, Y) = (X) \cap (X^2, Y - \lambda X)$, $\lambda \in k$, different primary decompositions, the primary component of the minimal prime (X) is the same in all the decompositions, as prescribed by Theorem 15.*

Chapter 7

Discrete valuation rings

Every ideal I in a Noetherian ring admits a primary decomposition (Theorem 13) $I = \mathfrak{q}_1 \cap \cdots \cap \mathfrak{q}_s$ where $\mathfrak{q}_i$ are primary ideals, in principle different, but the list of associated primes $\mathfrak{p}_i = \sqrt{\mathfrak{q}_i}$ being unique (Theorem 14). In general, these primary ideals are not powers of its associated primes, i.e. $\mathfrak{q}_i \neq \mathfrak{p}_i^{n_i}$. If we restrict to rings of dimension 1 (Definition 25), all maximal ideals are principal ideals, and powers of maximal ideals are always primary ideals (Proposition 36). Combining both assumptions we can see that in a Noetherian domain of dimension 1 where primary ideals are powers of primes, primary decomposition of ideals is, indeed a factorization theorem for ideals and $I = \mathfrak{q}_1 \cdots \mathfrak{q}_s$. In particular, Dedekind domains are rings where this happens.

The fact that all maximal ideals are principal means that the local geometry of the ring at a maximal point can be understood by means of the vanishing order of functions at a certain power of the generator of the ideal: this vanishing order will be the discrete valuation of the local ring. And, under certain additional conditions (normality) these local rings will be the discrete valuation rings (DVRs). Its study is deeply linked to the idea of singularity, as we will see.

7.1 Characterization of a DVR

We begin with the definition of a discrete valuation ring.

Definition 55. *Let K be a field. A **discrete valuation** of K is a surjective map*

$$v : K\backslash\{0\} \longrightarrow \mathbb{Z}$$

satisfying the following conditions, for every $f, g \in K\backslash\{0\}$:

(i) $v(fg) = v(f) + v(g)$

(ii) $v(f+g) \geq \min\{v(f), v(g))\}$,

Condition (i) states that v is a group homomorphism between the multiplicative group $K\backslash\{0\}$ and the additive group $\mathbb{Z}$. Let us adopt the convention $v(0) = \infty$. Then,

$$A = \{f \in K \ : \ v(f) \geq 0\}$$

*is a ring (exercise) called the **discrete valuation ring (DVR)** of the discrete valuation v.*

Observe that a DVR is an integral domain, since it is a subring of a field. Let us see the main properties of a DVR.

Proposition 38. *Let A be a discrete valuation ring and let $v : K\backslash\{0\} \longrightarrow \mathbb{Z}$ its discrete valuation.*

(a) $v(1) = 0$ *and* $v(f^{-1}) = -v(f)$.

(b) $v(f) = 0$ *if and only if* $f \in \mathcal{U}(A)$.

(c) If $v(f) = v(g)$, $f, g \in A$, *then the principal ideals* $(f) = (g)$ *in* A *are equal.*

(d) A *is a local ring whose maximal is* $\mathfrak{m} = \{f \in K \ : \ v(f) > 0\}$.

(e) The non-zero ideals of A *are* $\{f \in A \ : \ v(f) \geq n\}$.

(f) The maximal ideal is principal $\mathfrak{m} = (t)$ *with* $v(t) = 1$. *Therefore, the non-zero ideals of* A *are* $\mathfrak{m}^n = (t^n)$ *and* A *is a PID, hence also a UFD, hence also a normal ring.*

(g) The only non-zero prime ideal is maximal, hence $\dim A = 1$.

(h) A *is Noetherian.*

Proof. (a) Immediate from Definition 55 (i).

(b) Immediate from (a) since $A = \{f \in K \ : \ v(f) \geq 0\}$.

(c) Observe that $v(fg^{-1}) = v(f) - v(g) = 0$, then $fg^{-1} \in \mathcal{U}(A)$ by (b) and, then, $(f) = (g)$.

(d) By Corollary 1, A is local if the non-units, i.e. $\{f \in K \ : \ v(f) > 0\}$ are an ideal. Let $f \in A$ such that $v(f) > 0$ and let $g \in A$. Then $v(fg) = v(f) + v(g) > 0$, hence $fg \in \{f \in K \ : \ v(f) > 0\}$, and this is the maximal ideal $\mathfrak{m}$ of the local ring A.

(e) Let $I \subset A$ be a non-zero ideal and let $f \in I$ whose valuation $v(f) = n$ is the lowest possible among elements of I, then $I \subset \{f \in A \ : \ v(f) \geq n\}$. Observe that, $v(fg) \geq n$, for every $g \in A$, then $\{f \in A \ : \ v(f) \geq n\} \subset I$. Then, the non-zero ideals of A are of the form $\{f \in A \ : \ v(f) \geq n\}$.

(f) Since v is surjective, let $t \in A$ such that $v(t) = 1$. By (e), the principal ideal (t) has to be of the form $\{f \in A \ : \ v(f) \geq n\}$, for some $n \in \mathbb{N}$. Since $t \in (t)$ with $v(t) = 1$, we conclude that $(t) = \{f \in A \ : \ v(f) \geq 1\} = \mathfrak{m}$. Observe that $v(t^n) = nv(t) = n$, then $(t^n) = \{f \in A \ : \ v(f) \geq n\} = \mathfrak{m}^n$.

(g) Observe that ideals $(t^n) = \mathfrak{m}^n$ are never prime for $n > 1$, then the maximal $(t) = \mathfrak{m}$ is prime. From the Definition 25 of dimension, the longest chain of prime ideals in a domain where the only non-zero prime is maximal is: $\mathfrak{p}_0 = (0) \subsetneq \mathfrak{p}_1 = \mathfrak{m} \subsetneq A$, then $\dim A = 1$.

(h) The only ascending chain we can construct is

$$\cdots \subset \mathfrak{m}^n = (t^n) \subset \cdots \subset \mathfrak{m}^2 = (t^2) \subset \mathfrak{m} = (t)$$

which is stationary, then A is Noetherian.

□

From Proposition 38 we conclude that a DVR is a Noetherian integral domain of dimension 1 whose prime ideals are (0) and $\mathfrak{m}$, i.e. $\operatorname{Spec} A = \{(0), \mathfrak{m}\}$ and every other ideal is of the form $\mathfrak{m}^n$. Equivalently, we can say that a DVR is a PID with just one non-zero maximal ideal. Any generator t of the maximal ideal $\mathfrak{m} = (t)$ is called a **uniformizer parameter** of the DVR.

Exercise 55. *Show that the valuation function makes a DVR into an Euclidean domain (Definition 18). Therefore, from Proposition 38, Theorem 2 and Exercise 16, we can complete the list of classes of domains and rings as:*

$$DVR \Rightarrow ED \Rightarrow PID \Rightarrow UFD \Rightarrow normal\,.$$

Example 47. *Consider the field $\mathbb{Q}$ and choose a prime number p. Each rational number $q \in \mathbb{Q}$ can be written in a unique way as $p^n \frac{a}{b}$, where $n \in \mathbb{Z}$ and $a, b \in \mathbb{Z}$ with $b \neq 0$ and a, b coprime with p. Define the **p-adic valuation** as*

$$v_p : \mathbb{Q}\backslash\{0\} \longrightarrow \mathbb{Z}\ ,\ v_p(q) = n\ ,$$

*which is a discrete valuation of the field $\mathbb{Q}$. The **p-adic value** of each fraction $q \in \mathbb{Q}$ is the maximum number of times that the prime p divides the numerator and/or denominator. The set of rationals such that the p-adic valuation is non-negative is $\{q \in \mathbb{Q} \ :\ v_p(q) \geq 0\}$, which is equal to the localization $\mathbb{Z}_{(p)}$ of $\mathbb{Z}$ at the prime ideal (p) and which will be called, from now on, the **ring of p-adic integers**. Indeed, the elements of $\mathbb{Z}_{(p)}$ are (equivalent to) fractions $\frac{a}{b}$ where $b \in \mathbb{Z}\backslash(p)$, therefore the p-adic valuation equals the number of times we can extract p just from the numerator, which is non-negative. Understanding the integers m as functions over $\operatorname{Spec}\mathbb{Z}$, the p-adic valuations for the different primes p tell us the vanishing order of m at each prime (p).*

The maximal ideal of this local ring is $p\mathbb{Z}_{(p)}$ which are the fractions with valuation at least 1, i.e.

$$\mathfrak{m} = p\mathbb{Z}_{(p)} = \{q \in \mathbb{Q} \ :\ v_p(q) > 0\}\ .$$

A uniformizer parameter, i.e. a generator of $\mathfrak{m}$ is, whichever fraction of the form $p\frac{a}{b}$, where a, b are coprime with p: for example p (or $\frac{3p}{5}$ if $p > 5$, etc). The non-zero ideals of $\mathbb{Z}_{(p)}$ are

$$\mathfrak{m}^n = p^n\mathbb{Z}_{(p)} = \left\{p^n\frac{a}{b} \ :\ a, b \text{ coprime with } p\right\} = \{q \in \mathbb{Q} \ :\ v_p(q) \geq n\}.$$

The units of $\mathbb{Z}_{(p)}$ are the elements of valuation zero, i.e. fractions $\frac{a}{b}$ with a, b coprime with p: indeed, there exists $\frac{b}{a} \in \mathbb{Z}_{(p)}$ such that $\frac{a}{b} \cdot \frac{b}{a} = 1$. Note that $\frac{p}{b}$ is not a unit since $\frac{b}{p} \notin \mathbb{Z}_{(p)}$ because $p \notin \mathbb{Z}\backslash(p)$.

Example 48. *Consider the ring of rational functions with coefficients in a field k*

$$k(X) = \left\{ \frac{g(X)}{h(X)} \ : \ g(X), h(X) \in k[X] \ , \ h(X) \neq 0 \right\} = \operatorname{Frac} k[X] \ ,$$

which is the field of fractions of the ring of polynomials $k[X]$. Let $f(X) \in k[X]$ be an irreducible polynomial, then $(f(X))$ is a prime and maximal ideal. Similarly to Example 47, every fraction in $k(X)$ can be written as $f(X)^n \frac{g(X)}{h(X)}$ with $n \in \mathbb{Z}$, and this defines a discrete valuation (with respect to f):

$$v_f : k(X)\backslash\{0\} \longrightarrow \mathbb{Z} \ , \ v_f \left(f(X)^n \frac{g(X)}{h(X)} \right) = n \ ,$$

whose DVR is the local ring $k[X]_{(f)}$. If k is algebraically closed, then an irreducible polynomial is of the form $f(X) = X - a$ with $a \in k$, and the valuation of a rational function $\frac{g(X)}{h(X)}$ at $f(X) = X - a$ expresses the vanishing order of $\frac{g(X)}{h(X)}$ at $X = a$, as a zero or pole.

The maximal ideal of $k[X]_{(f)}$ is $f(X) \cdot k[X]_{(f)}$ which are the rational functions with valuation greater or equal than 1, i.e.

$$\mathfrak{m} = f(X) \cdot k[X]_{(f)} = \left\{ \frac{g(X)}{h(X)} \in k(X) \ : \ v_f \left(\frac{g(X)}{h(X)} \right) > 0 \right\} \ .$$

A uniformizer parameter generating $\mathfrak{m}$ is given by a rational function of the form $f(X) \frac{g(X)}{h(X)}$, where $g(X), h(X)$ are not multiples of $f(X)$: for example $f(X)$ itself. The non-zero ideals of $k[X]_{(f)}$ are

$$\mathfrak{m}^n = f(X)^n \cdot k[X]_{(f)} = \left\{ f(X)^n \frac{g(X)}{h(X)} \ : \ g(X), h(X) \text{ coprime with } f(X) \right\} =$$

$$\left\{ \frac{g(X)}{h(X)} \in k(X) \ : \ v_f \left(\frac{g(X)}{h(X)} \right) \geq n \right\} .$$

Again, the units of $k[X]_{(f)}$ are the elements of valuation zero, i.e. rational functions $\frac{g(X)}{h(X)}$ with $g(X), h(X)$ coprime with $f(X)$.

The following result says that a local domain which is Noetherian, normal (Definition 38) and 1-dimensional is a DVR, hence these properties characterize DVRs.

Theorem 16. *A ring A is a DVR if and only if A is a Noetherian normal local integral domain of dimension 1.*

Proof. If A is a DVR, by Proposition 38 we can collect all the desired properties.

Conversely, let A be a Noetherian normal local integral domain of dimension 1. Since A is a local domain, (0) and the only maximal $\mathfrak{m}$ are prime ideals. If there were another prime ideal $\mathfrak{p} \subset A$, it would be contained in a maximal ideal, then we would get $(0) \subsetneq \mathfrak{p} \subsetneq \mathfrak{m} \subsetneq A$, contradicting that $\dim A = 1$. Then, $\operatorname{Spec} A = \{(0), \mathfrak{m}\}$.

The main step is to show that the maximal ideal $\mathfrak{m}$ is principal. First, we see that $\mathfrak{m}^2 \subsetneq \mathfrak{m}$. Otherwise, treating $\mathfrak{m}$ as an A-module, we would have $\mathfrak{m} \cdot \mathfrak{m} = \mathfrak{m}$ with A local, hence $\mathfrak{m} = 0$ by Nakayama Lemma (Corollary 5). Then, let $t \in \mathfrak{m} \backslash \mathfrak{m}^2$ and let us show that $\mathfrak{m} = (t)$.

Consider the A-module $\mathfrak{m}/(t)$ and suppose that it is non-zero. Since A is Noetherian, by Proposition 32 (a) there exists one associated prime of $\mathfrak{m}/(t)$, i.e. there exists $\mathfrak{p} \in \operatorname{Spec} A = \{(0), \mathfrak{m}\}$ such that there exists an element $0 \neq n \in \mathfrak{m}/(t)$ with $\mathfrak{p} = \operatorname{Ann} n = \{a \in A \ : \ an = 0 \in \mathfrak{m}/(t)\}$. Since the element t is in all the possible annihilators $\operatorname{Ann} n$, the only candidate to be an associated prime is the maximal ideal $\mathfrak{m}$ itself, then $\mathfrak{m} = \operatorname{Ann} n = \{a \in A \ : \ an = 0 \in \mathfrak{m}/(t)\}$ with $0 \neq n \in \mathfrak{m}/(t)$. In particular, $\mathfrak{m}n \subset (t)$.

Since A is a domain, let $\operatorname{Frac} A$ be its field of fractions, and consider the element $\frac{n}{t} \in \operatorname{Frac} A$. Given that $\mathfrak{m}n \subset (t)$, the ideal $\left(\frac{n}{t}\right) \cdot \mathfrak{m} \subset A$. Suppose that $\left(\frac{n}{t}\right) \cdot \mathfrak{m} = A$. Then, there exists an element $l \in \mathfrak{m}$ such that $\frac{nl}{t} = 1$, which means $t = nl \in \mathfrak{m}^2$, contradicting the choice of t. Then $\left(\frac{n}{t}\right) \cdot \mathfrak{m} \subsetneq A$, hence $\left(\frac{n}{t}\right) \cdot \mathfrak{m} \subset \mathfrak{m}$.

Let us see that $\frac{n}{t}$ is integral over A. This follows from the determinant trick (Proposition 11) in the form of Proposition 14 (c)⇒(a): we have $\varphi : A \to \operatorname{Frac} A$, the element $\frac{n}{t} \in \operatorname{Frac} A$ and $\mathfrak{m} \subset \operatorname{Frac} A$ is a finite A-module (it is an ideal of the Noetherian ring A) containing $\left(\frac{n}{t}\right) \cdot \mathfrak{m}$. Therefore $\frac{n}{t}$ is integral over A. Since A is normal, $\frac{n}{t} \in A$, hence $n \in (t)$ and $n = 0$ as an element in $\mathfrak{m}/(t)$, which is a contradiction. Therefore, the A-module $\mathfrak{m}/(t)$ is zero and $\mathfrak{m} = (t)$ is a principal ideal.

The local ring A decomposes as $A = \mathfrak{m} \sqcup \mathcal{U}(A) = (t) \sqcup \mathcal{U}(A)$ and we have the chain of ideals

$$\mathfrak{m} = (t) \supsetneq \mathfrak{m}^2 = (t^2) \supsetneq \mathfrak{m}^3 = (t^3) \supsetneq \cdots \supsetneq \mathfrak{m}^n = (t^n) \supsetneq \cdots \ .$$

The inclusions are strict because, otherwise, $t^n \in (t^{n+1})$, then

$$t^n = at^{n+1} \ , \ a \in A \iff t^n(at - 1) = 0 \ ,$$

and t would be either a zero-divisor in a domain, or a unit in a maximal ideal, both a contradiction. Also, the intersection $\bigcap_{n=1}^{\infty}(t^n)$ is zero. Otherwise, there exists an element $0 \neq a \in \bigcap_{n=1}^{\infty}(t^n)$, hence $a = b_1 t = b_2 t^3 = b_3 t^3 = \cdots$, with $0 \neq b_n \in A$; we get the ascending chain

$$(a) \subsetneq (b_1) \subsetneq (b_2) \subsetneq (b_3) \subsetneq \cdots (b_n) \subsetneq \cdots$$

which is also strict, if not, $(b_n) = (b_{n+1})$ and there exists $c \in A$ with $b_{n+1} = cb_n$, then

$$a = b_n t^n = b_{n+1} t^{n+1} = cb_n t^{n+1} \ .$$

As before, this implies $t^n b_n (tc - 1) = 0$, which is not possible. Since A is Noetherian, a non-stationary infinite ascending chain is a contradiction, then $a = 0$ and $\bigcap_{n=1}^{\infty}(t^n) = (0)$.

Therefore, for every $a \in A$, either $a \in \mathcal{U}(A)$ or there exists a well-defined minimum $n \in \mathbb{N}$ such that $a \in (t^n) \backslash (t^{n+1})$, then necessarily $a = ut^n$, with $u \in \mathcal{U}(A)$. We set $v(a) := n$ the previous integer, and define

$$v : \operatorname{Frac} A \backslash \{0\} \longrightarrow \mathbb{Z} \ , \ v\left(\frac{a}{b}\right) = v(a) - v(b)$$

plus the convention $v(0) = \infty$.

The function v is a discrete valuation. It is obviously surjective. Given elements $a = ut^n$, $c = wt^m$, $u, w \in \mathcal{U}(A)$, it is clear that $v(ac) = v(a) + v(c)$, then given $\frac{a}{b}, \frac{c}{d} \in \operatorname{Frac} A$,

$$v\left(\frac{a}{b} \cdot \frac{c}{d}\right) = v\left(\frac{ac}{bd}\right) = v(ac) - v(bd) = v(a) + v(c) - v(b) - v(d) = v\left(\frac{a}{b}\right) + v\left(\frac{c}{d}\right) .$$

For the second property note that given elements $a = ut^n$, $c = wt^m$, $a + c \neq 0$, with $n \geq m$ and $u, w \in \mathcal{U}(A)$:

$$v(a + c) = v(ut^n + wt^m) = v(t^m(ut^{n-m} + w)) = m = \min\{v(a), v(c)\} ,$$

then

$$v\left(\frac{a}{b} + \frac{c}{d}\right) = v\left(\frac{ad + cb}{bd}\right) = v(ad + cb) - v(bd) = \min\{v(ad), v(cb)\} - v(bd) =$$

$$\min\{v(a)+v(d), v(c)+v(b)\}-v(b)-v(d) = \min\{v(a)-v(b), v(c)-v(d)\} = \min\left\{v\left(\frac{a}{b}\right), v\left(\frac{c}{d}\right)\right\} ,$$

unless $\frac{a}{b} + \frac{c}{d} = 0$ where we get the required inequality with $v(0) = \infty$.

Finally, it is clear by its very definition that the elements with non-negative valuation v are those of A, therefore, A is a discrete valuation ring. □

Exercise 56. *Assume that A is a Noetherian local integral domain. Prove that the maximal ideal $\mathfrak{m}$ is principal if and only if $\mathfrak{m}/\mathfrak{m}^2$ is a 1-dimensional vector space over the residual field $k = A/\mathfrak{m}$*[1].

Exercise 57. *Prove that a Noetherian local ring (not necessarily an integral domain) where the maximal ideal is principal $\mathfrak{m} = (t)$ is either a DVR or an Artinian local ring with $t^n = 0$ for some n (see Theorem 5).*

7.2 General valuation rings

In this section let us consider general valuation rings.

Definition 56. *Let A be an integral domain and let $K := \operatorname{Frac} A$ be its field of fractions. We say that A is a **valuation ring** of K if for every $0 \neq x \in K$, it is either $x \in A$ or $x^{-1} \in A$ (or both).*

Example 49. *Observe that $A = \mathbb{Z}$ is not a valuation ring of its field of fractions $K = \operatorname{Frac} \mathbb{Z} = \mathbb{Q}$ since neither $x = \frac{3}{5}$ nor $x^{-1} = \frac{5}{3}$ are integers.*

We can rephrase this definition in terms of a function called valuation, as in the case of DVRs, where a valuation ring turns out to be the set of elements with non-negative valuations.

Let A be an integral domain and let $K := \operatorname{Frac} A$ its field of fractions. Denote by $K\backslash\{0\}$ its multiplicative group. Let $\mathcal{U}(A)$ be the subgroup of units of A and take the group quotient

[1] Indeed, under the hypothesis of A being a Noetherian local integral domain, these two properties are equivalent to A being normal and A being a DVR, see [AM, Proposition 9.2].

$\Gamma := K\backslash\{0\}/\mathcal{U}(A)$. We denote the elements of Γ by $[x]$, with representatives $x \in K\backslash\{0\}$. We will use the additive notation for the abelian group Γ. Define a partial order in Γ by

$$[x] \geq 0 \Leftrightarrow x \in A \quad \text{equivalent to} \quad [x] \geq [y] \Leftrightarrow \frac{x}{y} \in A\,.$$

Define the map $v : K\backslash\{0\} \to \Gamma = K\backslash\{0\}/\mathcal{U}(A)$, $x \mapsto v(x) := [x]$ the canonical quotient group homomorphism.

Proposition 39. *With the previous notations, A is a valuation ring of K if and only if Γ is a totally ordered group (with the order compatible with the group operation) and v satisfies*

(a) $v(xy) = v(x) + v(y)$ *(i.e. v is a group homomorphism)*

(b) $v(x+y) \geq \min\{v(x), v(y)\}$

We call the map v a ***valuation*** *of $K\backslash\{0\}$ with* ***value group*** *Γ. Conversely, any group homomorphism $v : K\backslash\{0\} \to \Gamma$ satisfying (a) and (b) with Γ totally ordered determines a* ***valuation ring*** *$A := \{a \in K\backslash\{0\} \ : \ v(a) = [a] \geq 0\} \cup \{0\}$.*

Proof. The relation $\geq$ defines a total order in Γ if for every $[x], [y] \in \Gamma$, it is exactly one of $[x] > [y]$, $[x] = [y]$ or $[x] < [y]$. By definition of $\geq$ this is equivalent to $\frac{x}{y} \in A$, $\frac{y}{x} \in A$ or $\frac{x}{y}, \frac{y}{x} \in A$ (which means $\frac{x}{y} \in \mathcal{U}(A)$), which is equivalent to A being a valuation ring of K. Proving that $\geq$ is compatible with the group operation in Γ, i.e. $[x] \geq [y] \Leftrightarrow [x] + [z] \geq [y] + [z]$, for every $[z] \in \Gamma$ is left as an exercise.

Note that, by the definition of Γ as an additive group, condition (a) derives from the definition of homomorphism:

$$v(xy) = [xy] = [x] + [y] = v(x) + v(y)\,.$$

Condition (b) is equivalent to

$$v(x+y) \geq \min\{v(x), v(y)\} \Leftrightarrow v(x+y) \geq v(x) \ \text{ or } \ v(x+y) \geq v(y) \Leftrightarrow$$

$$\frac{x+y}{x} = 1 + \frac{y}{x} \in A \ \text{ or } \ \frac{x+y}{y} = 1 + \frac{x}{y} \in A \Leftrightarrow \frac{y}{x} \in A \ \text{ or } \ \frac{x}{y} \in A\,.$$

which is equivalent to Γ being a totally ordered set as we have seen. □

Example 50. *Given $A = \mathbb{Z}$ and its field of fractions $K = \operatorname{Frac}\mathbb{Z} = \mathbb{Q}$, consider the additive group $\Gamma := \mathbb{Q}\backslash\{0\}/\mathcal{U}(\mathbb{Z}) = \mathbb{Q}\backslash\{0\}/\{\pm 1\} = \mathbb{Q}_{>0}$. The partial order is $\left[\frac{a}{b}\right] \geq \left[\frac{c}{d}\right] \Leftrightarrow \frac{a/b}{c/d} = \frac{ad}{bc} \in \mathbb{Z}$. Note that this is not a total order since the elements $\frac{3}{5}$ and $\frac{5}{3}$ are not comparable because neither $\frac{25}{9}$ nor $\frac{9}{25}$ are integers. Therefore, again, $\mathbb{Z}$ is not a valuation ring of $\mathbb{Q}$.*

Let us discuss the main properties of general valuation rings. Compare with those of Proposition 38.

Proposition 40. *Let A be a valuation ring of its field of fractions $K = \operatorname{Frac} A$.*

(a) The units are $\mathcal{U}(A) := \{a \in K\backslash\{0\} \ : \ v(a) = 0\}$. Also, $v(x^{-1}) = -v(x)$.

(b) *A is a local ring whose maximal ideal is* $\mathfrak{m} := \{a \in K \backslash \{0\} \ : \ v(a) > 0\} \cup \{0\}$.

(c) *Every finitely generated ideal $I \subset A$ is principal.*

(d) *A is normal.*

Proof. (a) It is equivalent $v(a) = 0$ to $v(a) \geq 0$ and $v(a) \leq 0$, which is equivalent to $a \in A$ and $a^{-1} \in A$, which means $a \in \mathcal{U}(A)$. For the second, use the property (a) of the homomorphism valuation.

(b) The proof is the same as in Proposition 38 (d).

(c) Suppose that $I = (x_1, x_2, \ldots, x_n) \subset A$, $x_i \neq 0$, $i = 1, \ldots, n$. Then, given the field element $\frac{x_1}{x_2}$ it is either $\frac{x_1}{x_2} \in A$ or $\frac{x_2}{x_1} \in A$. Suppose $\frac{x_1}{x_2} \in A$, then $x_1 = x_2 \cdot \frac{x_1}{x_2} \in (x_2, \ldots, x_n)$, then $I = (x_2, \ldots, x_n)$. By induction, I is principal.

(d) Let $y \in K$ be an integral element over A. Then, there exists elements $a_0, a_1, \ldots, a_{n-1} \in A$ such that $y^n + a_{n-1}y^{n-1} + \cdots + a_2y^2 + a_1y + a_0 = 0$. Since A is a valuation ring we have that $y \in A$ or $y^{-1} \in A$ (or both). If $y \in A$ we are done, and if $y^{-1} \in A$ we can multiply the previous integral expression by $(y^{-1})^{n-1} = y^{1-n}$ to get

$$y + a_{n-1} + a_{n-2}y^{-1} + \cdots + a_2y^{3-n} + a_1y^{2-n} + a_0y^{1-n} = 0 \Leftrightarrow y =$$

$$-a_{n-1} - a_{n-2}y^{-1} - \cdots - a_2y^{3-n} - a_1y^{2-n} - a_0y^{1-n} \in A$$

and we are also done.

□

Valuation rings are not necessarily discrete valuation rings. Indeed, this condition is equivalent to being Noetherian.

Theorem 17. *Let A be a valuation ring. Then, A is Noetherian if and only if A is a DVR.*

Proof. Let A be a valuation ring, then it is a normal local integral domain (Proposition 40 (b, d). Suppose that A is Noetherian, then its maximal ideal $\mathfrak{m}$ is finitely generated, then it is principal $\mathfrak{m} = (t)$, by Proposition 40 (b). Along the lines of the proof of Theorem 16, every element $x \in A$ can be uniquely written as $a = ut^n$, $u \in \mathcal{U}(A)$, then every non-zero ideal is of the form $(t^n) = \mathfrak{m}^n$ and there is no other prime ideals between (0) and $\mathfrak{m}$, hence A is a DVR. Conversely, a DVR is Noetherian, by Proposition 38 (h). □

Example 51. *Let us see an example of a general valuation ring which is not a DVR, i.e. which is not Noetherian.*

Let A be a DVR with maximal $\mathfrak{m} = (t)$, t the uniformizer parameter. Construct the ring

$$A_\infty := A[t] \cup A[t^{1/2}] \cup A[t^{1/3}] \cup \cdots \cup A[t^{1/n}] \cup \cdots = \bigcup_{n=1}^{\infty} A[t^{1/n}]$$

resulting from adjoining all the n^{th}-roots of t. The ring A_∞ is a domain (we do not add zero-divisors in the construction) whose ring of fractions $K = \operatorname{Frac} A_\infty$ contains quotients of expressions involving n^{th}-roots of t, i.e. is infinitely generated by all possible fractional powers of t, $t^{a/b}$, as an A-module, hence A_∞ is not Noetherian. Defining the valuation

$$v : K\backslash\{0\} \to \Gamma = \mathbb{Q}$$

where $v(f/g) = v(f) - v(g)$ and, for $f \in A_\infty$, $v(f)$ is the highest fractional exponent of t in f (i.e. for example $v\left(\frac{(t^{1/2})^3+t^{1/5}}{t^{1/3}+(t^{1/4})^7}\right) = \frac{3}{2} - \frac{7}{4} = -\frac{1}{4}$) it is easy to see that A_∞ is a valuation ring (Exercise, use Proposition 39) which is not a DVR.

7.3 Normal Noetherian rings

Let us characterize Noetherian integral domains which are normal.

Definition 57. *Let A be an integral domain and let $K = \operatorname{Frac} A$ be its field of fractions. For every element $x \in K$ we define its **ideal of denominators** of x as*

$$D(x) = \{a \in A \ : \ ax \in A\} = \{a \in A \ : \ x = \frac{b}{a} \text{ with } b \in A\} \cup \{0\} \ .$$

The ideal of denominators $D(x)$ is an ideal of A.

Example 52. *The ideal of denominators of a rational number in $\mathbb{Q} = \operatorname{Frac} \mathbb{Z}$ is the principal ideal generated by its denominator, after reducing the fraction. For example,*

$$D\left(\frac{4}{30}\right) = \left\{n \in \mathbb{Z} \ : \ n\frac{4}{30} \in \mathbb{Z}\right\} = 15\mathbb{Z} \ .$$

Lemma 6. *Let A be an integral domain and let $K = \operatorname{Frac} A$ be its field of fractions. Then,*

$$A = \bigcap_{\mathfrak{p} \in \operatorname{Spec} A} A_\mathfrak{p} = \bigcap_{\mathfrak{m} \in \operatorname{Specmax} A} A_\mathfrak{m}$$

where the intersections take place in K.

Proof. Let $x \in K$. It is equivalent $x \notin A$ to $D(x) \neq A$, which is also equivalent to the existence of a maximal ideal $\mathfrak{m} \subsetneq A$ such that $D(x) \subset \mathfrak{m}$. And this is equivalent to $x \notin A_\mathfrak{m}$. Therefore A is the intersection of all its maximal ideals. □

Let us see that normality is a local condition for integral domains.

Proposition 41. *Let A be an integral domain and let $K = \operatorname{Frac} A$ be its field of fractions. Then, the following are equivalent:*

(a) A is normal.

(b) $A_{\mathfrak{p}}$ *is normal for every* $\mathfrak{p} \in \operatorname{Spec} A$.

(a) $A_{\mathfrak{m}}$ *is normal for every* $\mathfrak{m} \in \operatorname{Specmax} A$.

Proof.

(i)⇒(ii) Let $x \in k(\mathfrak{p}) = A_{\mathfrak{p}}/\mathfrak{p}A_{\mathfrak{p}} \subset K$ be an integral element over $A_{\mathfrak{p}}$. Then, there exist elements $\frac{b_0}{c_0}, \dots, \frac{b_{n-1}}{c_{n-1}} \in A_{\mathfrak{p}}$, with $b_i \in A$, $c_i \in A\backslash\mathfrak{p}$, such that

$$x^n + \frac{b_{n-1}}{c_{n-1}}x^{n-1} + \cdots + \frac{b_1}{c_1}x + \frac{b_0}{c_0} = 0\,.$$

By clearing denominators in this expression, we multiply by $(c_0c_1\cdots c_{n-1})^n$ and get an integral dependence relation for the element $c_0c_1\cdots c_{n-1}x$ over A. Since A is normal, $c_0c_1\cdots c_{n-1}x \in A$ and, since every $c_i \in A\backslash\mathfrak{p}$, $c_0c_1\cdots c_{n-1} \in A\backslash\mathfrak{p}$, hence $x = \frac{c_0c_1\cdots c_{n-1}x}{c_0c_1\cdots c_{n-1}} \in A_{\mathfrak{p}}$. Therefore $A_{\mathfrak{p}}$ is normal.

(ii)⇒(iii) Trivial.

(iii)⇒(i) Let $x \in K$ be an integral element over A, then there exist elements $a_0, \dots, a_n \in A$ such that

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

Since, for each i, $a_i = \frac{a_i}{1}$ and $1 \notin \mathfrak{m}$ for every $\mathfrak{m} \in \operatorname{Specmax} A$, this is also an integral relation for x over $A_{\mathfrak{m}}$ for each maximal. By hypothesis $A_{\mathfrak{m}}$ is normal, hence, $x \in A_{\mathfrak{m}}$ for every $\mathfrak{m} \in \operatorname{Specmax} A$. By Lemma 6, $x \in \bigcap_{\mathfrak{m}\in\operatorname{Specmax} A} A_{\mathfrak{m}} = A$.

□

Remark 14. *Observe that Proposition 41 implies that if A is a normal integral domain, all its fraction rings $S^{-1}A$ are normal, for every multiplicative set S.*

Let us see now that localizing normal Noetherian integral domains into minimal primes yield DVRs.

Proposition 42. *Let A be a normal Noetherian integral domain.*

(a) Suppose that $0 \neq I = (x) \subset A$ is a principal ideal and $\mathfrak{p} \in \operatorname{Ass} A/I$. Then $\mathfrak{p}$ is a minimal non-zero prime ideal.

(b) If $\mathfrak{p} \subset A$ is a minimal non-zero prime ideal, then $A_{\mathfrak{p}}$ is a DVR.

Proof. (a) Consider the local ring $(A_{\mathfrak{p}}, \mathfrak{m} := \mathfrak{p}A_{\mathfrak{p}})$ and let $J := IA_{\mathfrak{p}} = xA_{\mathfrak{p}}$ be an ideal of $A_{\mathfrak{p}}$. By Proposition 26, taking $S = A\backslash\mathfrak{p}$, we have $A_{\mathfrak{p}}/J = A_p/IA_{\mathfrak{p}} = S^{-1}(A/I)$. Since, by hypothesis, $\mathfrak{p} \in \operatorname{Ass} A/I$, then by Proposition 37, $\mathfrak{m} \in \operatorname{Ass}(A_{\mathfrak{p}}/J)$. We will prove that $\mathfrak{m}$ is a minimal non-zero prime of $A_{\mathfrak{p}}$ and, by Exercise 40, we will conclude that $\mathfrak{p}$ is a minimal non-zero prime of A.

Let $\mathfrak{m} \in \operatorname{Ass}(A_\mathfrak{p}/I) = \operatorname{Ass}(A_\mathfrak{p}/(x))$, then there exists an element $y \in A_\mathfrak{p} \backslash (x)$ such that $\mathfrak{m}y \subset (x)$, hence the element $\frac{y}{x} \in \operatorname{Frac} A_\mathfrak{p} = A_\mathfrak{p}/pA_\mathfrak{p}$ verifies $\mathfrak{m}\frac{y}{x} \subset A_\mathfrak{p}$. Let us see that $\mathfrak{m} = \left(\frac{x}{y}\right)$.

Since $\mathfrak{m}\frac{y}{x} \subset A_\mathfrak{p}$ is an ideal in a local ring, either $\mathfrak{m}\frac{y}{x} = \mathfrak{m}$ or $\mathfrak{m}\frac{y}{x} = A_\mathfrak{p}$. In the first case, using the same arguments as in Theorem 16, we get that $\frac{y}{x}$ is integral over $A_\mathfrak{p}$, which is normal (A is normal and normality is local), then $\frac{y}{x} \in A_\mathfrak{p}$, contradiction. In the second case, $1 \in \mathfrak{m}\frac{y}{x}$, then there exists an element $t \in \mathfrak{m}$ with $1 = t\frac{y}{x}$ and, for any other $a \in \mathfrak{m}$, $a\frac{y}{x} = \frac{a}{t} \in A_\mathfrak{p}$, therefore $a \in \left(\frac{x}{y}\right)$. Finally, since $\mathfrak{m} = \left(\frac{x}{y}\right)$ is principal, Theorem 16 implies that $A_\mathfrak{p}$ is a DVR and, hence, $\mathfrak{m} = \mathfrak{p}A_\mathfrak{p}$ is a minimal non-zero prime ideal.

(b) By Proposition 41, the local ring $A_\mathfrak{p}$ is normal. By Exercise 40 (c), $A_\mathfrak{p}$ is Noetherian and by the same Exercise 40 (d) and minimality of $\mathfrak{p}$, we have $\operatorname{Spec} A_\mathfrak{p} = \{(0), \mathfrak{p}A_\mathfrak{p}\}$. Then $A_\mathfrak{p}$ is a Noetherian normal local domain of dimension 1 which, by Theorem 16, is a DVR.

□

Theorem 18. *A normal Noetherian integral domain A is the intersection of the DVRs $A_\mathfrak{p}$, where $\mathfrak{p}$ are the minimal primes.*

Proof. By Lemma 6 A is the intersection of all localizations at primes, which is contained in the intersection of just the localization at minimal primes. Then we need to prove that an element contained in all localizations $A_\mathfrak{p}$ with $\mathfrak{p}$ a minimal prime, is indeed in A. Equivalently we will show that, given an element $x \in K$ such that $x \notin A$ there exists a minimal prime $\mathfrak{p}$ such that $x \notin A_\mathfrak{p}$.

Let us write $x = \frac{b}{c}$. The ideal of denominators of x is

$$D(x) = \left\{ a \in A \ : \ ax = a\frac{b}{c} \in A \right\} = \{a \in A \ : \ ab \in (c)\} = \operatorname{Ann}(\overline{b})$$

where $\overline{b} \in A/(c)$ is the residual class of b modulo the ideal (c). If $x \notin A$, then $0 \neq \overline{b} \in A/(c)$.

Let us see that there exists a prime ideal $\mathfrak{p} \in \operatorname{Ass}(A/(c))$ such that $D(x) \subset \mathfrak{p}$. First, $D(x) = \operatorname{Ann} \overline{b}$, with $0 \neq \overline{b} \in A/(c)$, then the set of annihilator ideals is non-empty. Since A is Noetherian, by Proposition 8 (c) there exists a maximal annihilator ideal containing $D(x)$, and by Proposition 30 (c), this annihilator is an associated prime in $\operatorname{Ass}(A/(c))$. By Proposition 42 (a), this prime ideal $\mathfrak{p} \in \operatorname{Ass}(A/(c))$ is a minimal non-zero prime. Since $D(x) \subset \mathfrak{p}$, then $x \notin A_\mathfrak{p}$, completing the proof. □

Let us understand the geometric meaning of Proposition 42 and Theorem 18. Let k be an algebraically closed field and let $Z = V(\mathfrak{p}) \subset k^n$ be an irreducible variety with $\mathfrak{p} \subset k[X_1, \ldots, X_n]$ a prime ideal of the ring of polynomials in several variables. Let $A = k[Z] = k[X_1, \ldots, X_n]/\mathfrak{p}$ be the coordinate ring of the variety Z. Let $\mathfrak{q} \subset A$ be a minimal prime (i.e. a prime ideal which does not contain another prime ideal different from zero). Then, necessarily $Y := V(\mathfrak{q}) \subset Z$ is an irreducible subvariety of Z of codimension 1, i.e. Y is a hypersurface of Z.

Assume that Z is normal, i.e. its ring of coordinates $A = k[Z]$ is a normal ring. Observe that it is also a Noetherian integral domain. Then, the local ring

$$A_\mathfrak{q} = k[Z]_\mathfrak{q} = \left\{ \frac{f}{g} \ : \ f, g \in k[Z] \ , \ g \neq 0 \text{ on } Y \right\}$$

is a DVR by Proposition 42 (b) and measures the vanishing order of the rational function $\frac{f}{g}$ along the hypersurface Y.

Now let $f \in A = k[Z]$ be a polynomial function on Z. Then $(f) \subset k[Z]$ is a principal ideal and $V((f)) \subset Z$ is a subvariety determined by the points $z \in Z$ such that $f(z) = 0$. Let $W \subset V((f))$ be an irreducible component of $V((f))$, then $W = V(\mathfrak{q}')$ with $\mathfrak{q}' \in \operatorname{Ass} A/(f)$ (by Theorem 11). By Proposition 42 (a) this $\mathfrak{q}'$ is a minimal non-zero prime ideal of $A = k[Z]$, hence W is, itself, a hypersurface of Z. This means that a polynomial function on a normal variety has zeros along hypersurfaces and not along lower dimensional varieties.

Finally, Theorem 18 says that if Z is a normal variety with ring of coordinates $k[Z]$, a rational function $\frac{f}{g} \in \operatorname{Frac} k[Z]$, is either in $k[Z]$ (it has no poles) or it has poles along a hypersurface of Z. Otherwise there would exists a non-minimal prime $\mathfrak{q} \subset k[Z]$ such that $g \in \mathfrak{q}$, then $\frac{f}{g} \notin k[Z]_{\mathfrak{q}}$, but for each minimal prime $\mathfrak{p} \subsetneq \mathfrak{q}$ we have $g \notin \mathfrak{p}$, then $0 \neq \frac{f}{g} \in A_{\mathfrak{p}}$. Hence, by Theorem 18,

$$\frac{f}{g} \in \bigcap_{(0)\neq\mathfrak{p}\subset k[Z] \text{ minimal}} k[Z]_{\mathfrak{p}} = k[Z] \, .$$

This way, the set of rational functions with no poles along any hypersurface of Z is precisely the ring $k[Z]$.

Example 53. *Let $W = V(XZ - Y^2) \subset k^3$ be the affine cone of Example 45 with coordinate ring $k[W] = k[X, Y, Z]/(XZ - Y^2)$. Observe that it is not a UFD since $XZ = Y^2$ are two different factorizations of the same element.*

Let us see that the cone is normal. This is an example of the implication UFD $\Rightarrow$ normal not being an equivalence. Let $k[W] = k[X, Y, Z]/(XZ - Y^2)$ be the ring of coordinates of the cone X and let $k(W) := \operatorname{Frac} k[W]$ be its field of rational functions. Since $Y^2 = XZ$, their elements can be written as $f(X, Z) + g(X, Z)Y \in k[W]$ and $\frac{f(X,Z)}{h(X,Z)} + \frac{g(X,Z)}{i(X,Z)}Y \in k(W)$. This shows that Y is integral over $k[X, Z]$ and, hence, $k[W]$ is a finite module over $k[X, Z]$ (Proposition 14). Assume that an element $\frac{f(X,Z)}{h(X,Z)} + \frac{g(X,Z)}{i(X,Z)}Y \in k(W)$ is integral over the ring $k[W]$; then, by transitivity of integrality (Exercise 21), it is integral over $k[X, Z]$. In this case, the polynomial in T

$$T^2 - 2\frac{f}{h}T + \frac{f^2}{h^2} - \frac{g^2}{i^2}XZ \in k[X, Z][T]$$

vanishes at $T = \frac{f}{h} + \frac{g}{i}Y$, then it should have its coefficients in the ring $k[X, Z]$. Then, $\frac{f}{h} \in k[X, Z]$, hence h is a unit. Now $\frac{f^2}{h^2} - \frac{g^2}{i^2}XZ \in k[X, Z]$, hence $\frac{g^2}{i^2}XZ \in k[X, Z]$. Since XZ is the product of two irreducible elements with no common factor in the UFD $k[X, Z]$, i is necessarily a unit and $\frac{f}{h} + \frac{g}{i}Y \in k[W]$, therefore $k[W]$ is normal.

The only singularity of the cone is the apex point $(0, 0, 0)$, corresponding to the maximal ideal (X, Y, Z) (which is a non-minimal prime). The localization at this singular point is not a UFD (the same two distinct factorizations $XZ = Y^2$ hold locally), hence the local ring $k[W]_{(X,Y,Z)}$ is not a DVR. But this is not in contradiction with Theorem 18 since a point in a surface is a codimension 2 subvariety: the cone is normal and is smooth in codimension 1!

The rational function $\frac{1}{X+Z}$ has poles in the cone W when $X = -Z$, this is when $Y^2 + Z^2 = 0$. Do not get confused thinking that this denominator $X + Z = 0$ is the real plane intersecting the

cone in just the singular point! Over the complex numbers, the solutions of $Y^2 + Z^2 = 0$ *are two lines, exactly a codimension* 1 *subvariety given by minimal primes of* $k[W]$*, as prescribed by Proposition 42 and Theorem 18.*

Example 54. *This example is taken from Enrique Arrondo's notes [Ar, Exercise 7.12 and Example 7.14] and you can check the details there.*

Let k *be an algebraically closed field. Consider the ideal*

$$I = (TZ - XY, X^3 - T^2Y, Y^3 - XZ^2, X^2Z - TY^2) \subset k[X, Y, Z, T]$$

and the quotient ring $k[X, Y, Z, T]/I$ *which is the ring of coordinates of the variety* $W = V(I)$*. Then it can be shown that:*

(a) W *is a surface, i.e. the ring* $k[W]$ *has dimension* 2*.*

(b) $k[W]$ *is not integrally closed in its field of fractions, i.e.* $k[W]$ *is not normal, by showing that the element* $\frac{X^2}{T} \in k(W)$ *is not integral over* $k[W]$*.*

(c) The rational function $\frac{X^2}{T} \in k(W)$ *has a single pole at the origin* $(0, 0, 0, 0) \in k^4$*, i.e. at the maximal ideal* (X, Y, Z, T)*, which is a non-minimal prime of* $k[W]$*.*

Therefore, this is an example of a non-normal ring of coordinates corresponding to a surface, having a rational function with poles along a subvariety of codimension 2*.*

Since in dimension 1 there are no space for codimension 2 issues, a consequence of Theorem 18 is that normality of algebraic curves is equivalent to smoothness.

Theorem 19. *Let* k *be an algebraically closed field and let* $f(X, Y) \in k[X, Y]$*. Let* $Z = \{(x, y) \in k^2 \ : \ f(x, y) = 0\}$ *be an irreducible plane curve, i.e.* $Z = V((f))$*. We have that* Z *is a non-singular curve if and only if its ring of coordinates* $k[Z] = k[X, Y]/(f)$ *is normal.*

Proof. Observe that, in an irreducible curve $Z = V((f))$, non-zero primes coincide with maximal ideals which are minimal non-zero primes, and those are of the form $\mathfrak{m} = (X - a, Y - b) + (f) \subset k[Z] = k[X, Y]/(f)$, where $f(a, b) = 0$.

Suppose that $k[Z]$ is normal. Then, by Proposition 41, it is equivalent to $k[Z]_{\mathfrak{m}}$ being normal, for every maximal ideal $\mathfrak{m} = (X - a, Y - b) + (f)$. Being $k[Z]_{\mathfrak{m}}$ a Noetherian local domain of dimension 1, by Theorem 16 it is equivalent to $k[Z]_{\mathfrak{m}}$ being a DVR or the maximal ideal $\mathfrak{m}$ being a principal ideal. And, using Exercise 56 (and Nakayama Corollary 6) this is equivalent to $\dim \mathfrak{m}/\mathfrak{m}^2 = 1$, where the module $\mathfrak{m}/\mathfrak{m}^2$ is a vector space over $k \simeq k[Z]/\mathfrak{m}$.

Note that $k[Z]_{\mathfrak{m}} = (k[X, Y]/(f))_{(X-a,Y-b)+(f)} \simeq \left(k[X, Y]_{(X-a,Y-b)}\right)/(f)$ (c.f. Proposition 26), then the vector space $\mathfrak{m}/\mathfrak{m}^2$ is generated by two elements, $X - a + (f)$ and $Y - b + (f)$. We will show that Z is non-singular at (a, b) if and only if there is a linear relation between the two generators $X - a + (f)$ and $Y - b + (f)$.

Suppose that $f(X, Y) = \alpha(X - a) + \beta(Y - b) + g(X - a, Y - b)$, where $g(X - a, Y - a) \in (X - a, Y - b)^2$. We have that f is non-singular at (a, b) if and only if $\alpha(X - a) + \beta(Y - b) \neq 0$.

Then, we assume that $\beta \neq 0$ and we will prove that $X - a + (f)$ generates $\mathfrak{m}/\mathfrak{m}^2$ by showing that $Y - b + (f)$ belongs to the ideal generated by $X - a + (f)$, i.e.

$$Y - b \in (X - a, f(X, Y)) \cdot k[X, Y]_{(X-a,Y-b)} \, .$$

Note that we can rewrite f as

$$f(X, Y) = \beta(Y - b)f_1(Y - b) + (X - a)f_2(X - a, Y - b) \, ,$$

where $f_1(Y - b) = 1 + \cdots$, hence it is a unit in $k[X, Y]_{(X-a,Y-b)}$. Then,

$$(X - a, f(X, Y)) \cdot k[X, Y]_{(X-a,Y-b)} =$$

$$\big(X - a, \beta(Y - b)f_1(Y - b) + (X - a)f_2(X - a, Y - b)\big) \cdot k[X, Y]_{(X-a,Y-b)} =$$

$$\big(X - a, \beta(Y - b)f_1(Y - b)\big) \cdot k[X, Y]_{(X-a,Y-b)} =$$

$$(X - a, Y - b) \cdot k[X, Y]_{(X-a,Y-b)} \, ,$$

hence $Y - b \in (X - a, f(X, Y)) \cdot k[X, Y]_{(X-a,Y-b)}$ and the vector space $\mathfrak{m}/\mathfrak{m}^2$ is generated by $X - a + (f)$, therefore, $\dim \mathfrak{m}/\mathfrak{m}^2 = 1$. □

Example 55. *Recall the cuspidal curve Z from Example 17, whose ring of coordinates is $k[Z] = k[X, Y]/(Y^2 - X^3)$. We already saw in the Example 17 that this ring is not normal. Indeed, all localizations are normal except for the localization at the singular point $(0, 0)$. The rational function $\frac{Y}{X} \in k(Z) = \operatorname{Frac} k[Z]$ satisfies $\left(\frac{Y}{X}\right)^2 - X = 0$, then it is an integral element over the ring $k[Z]$. However, this rational function does not belong to the localized ring $k[Z]_{(X,Y)}$, since the denominator X belongs to the prime (X, Y). This shows that this $Y/X = \sqrt{X}$ is an extra rational function vanishing at the origin, yielding an additional generator of the maximal ideal $(X, Y) \cdot k[Z]_{(X,Y)}$, and making this maximal ideal not principal.*

Note that, for a non-singular point (a, b), the equation of the curve Z can be written as $f(X, Y) = l(X - a, Y - b) + g(X - a, Y - b)$ with linear part $l \neq 0$ and $g \in (X - a, Y - b)^2$. For example, at the non-singular point $(1, 1)$ we get:

$$f(X, Y) = Y^2 - X^3 = -3(X - 1) + 2(Y - 1) - (X + 2)(X - 1)^2 + (Y - 1)^2 \, ,$$

where $l(X, Y) = -3(X - 1) + 2(Y - 1) \neq 0$ and $g(X, Y) = -(X + 2)(X - 1)^2 + (Y - 1)^2 \in (X - 1, Y - 1)^2$. However, for the point $(a, b) = (0, 0)$, it is clear from the equation $f(X, Y) = Y^2 - X^3$ that $l = 0$ and the curve Z is singular, coinciding with the localization at (X, Y) not being normal, as prescribed by Theorem 19.

Let us finish the section generalizing the idea of a 1-dimensional ring where all the localizations are DVRs: Dedekind domains.

Definition 58. *A **Dedekind domain** is a normal Noetherian integral domain of dimension* 1.

Observe that a Dedekind domain is not necessarily local. For example, the coordinate ring $k[Z]$ of a non-singular algebraic curve, k algebraically closed, is a Dedekind domain (Theorem 19). The ring of integers of a number field is the other main example of a Dedekind domain ([AM, Theorem 9.5]).

Dedekind domains are the rings where the arithmetic property of a number factoring as a finite product of primes holds at the level of ideals.

Proposition 43. *Let A be a Dedekind domain. Every ideal $I \subset A$ has a unique factorization as a product of a finite number of prime ideals.*

Proof. Let A be a Dedekind domain and let $\mathfrak{p} \subset A$ be a non-zero prime ideal. Since $\dim A = 1$, $\mathfrak{p}$ is a minimal prime and also a maximal ideal. By Proposition 42 (b), all localizations $A_{\mathfrak{p}}$ are DVRs. For every ideal $I \subset A$, its localization $e(I) \subset A_{\mathfrak{p}}$ is of the form $(t_{\mathfrak{p}}^{n_{\mathfrak{p}}})$, where $t_{\mathfrak{p}}$ is a uniformizer parameter in $A_{\mathfrak{p}}$, $n_{\mathfrak{p}} \geq 0$. By Noetherianity (Corollary 13), there exists a finite number of associated primes in $\operatorname{Ass} A/I$ and these are the prime ideals such that $n_{\mathfrak{p}} \neq 0$. Therefore

$$I = \mathfrak{p}_1^{n_{\mathfrak{p}_1}} \cap \cdots \cap \mathfrak{p}_s^{n_{\mathfrak{p}_s}} = \mathfrak{p}_1^{n_{\mathfrak{p}_1}} \cdots \mathfrak{p}_s^{n_{\mathfrak{p}_s}} .$$

□

7.4 Completion of a DVR

We use Cauchy sequences of rational numbers to define real numbers as infinite decimal expansions where two expansions are equivalent if their limits are equal. We call the real numbers a complete space because every Cauchy sequence has a limit, i.e. every Cauchy sequence has a real number in its equivalence class. In general we call completion of a metric space to the space of equivalence classes of Cauchy sequences.

Here we will show the analogue in commutative algebra where we will complete a DVR by measuring the vanishing order of a function at the maximal point, i.e. the lowest power of the uniformizer parameter in every element. An extended treatment of completions of rings along other ideals (I-adic completions) can be found in [AM, Chapter 9].

Definition 59. *Let A be a DVR with maximal ideal $\mathfrak{m} = (t)$, t being the uniformizer parameter. We say that a sequence of elements $a_0, a_1, \ldots, a_n, \ldots \in A$ is a **t-adic Cauchy sequence** if for every i, there exists an $N \in \mathbb{N}$ such that for every $n, m \geq N$ it is $a_n - a_m \in \mathfrak{m}^i = (t^i)$.*

*Two Cauchy sequences (a_n), (b_n) are **equivalent** if for every i, there exists an $N \in \mathbb{N}$ such that for every $n \geq N$ it is $a_n - b_n \in \mathfrak{m}^i = (t^i)$. We define a sum and a multiplication of (equivalence classes of) Cauchy sequences, term by term, to define a ring $\widehat{A}$ called the **completion** of A.*

Remark 15. *Observe that, by the proof of Theorem 16, there is no non-zero element in the intersection of all powers of the maximal ideal, i.e. $\bigcap_{i=1}^{\infty} \mathfrak{m}^i = (0)$. Otherwise there would exists $0 \neq a \in \bigcap_{i=1}^{\infty}$ and the constant Cauchy sequence a would be equivalent to the constant Cauchy sequence zero.*

The elements of $\widehat{A}$ can be written as

$$a = \sum_{i=0}^{\infty} a_i t^i = a_0 + a_1 t + a_2 t^2 + \cdots + a_n t^n + \cdots$$

where $a_i \notin \mathfrak{m} = (t)$ for every i, i.e. a_i are units in A or zero. We can see that this is a local domain with principal maximal ideal $\widehat{\mathfrak{m}} = (t)$, hence a PID which is Noetherian. By Theorem 16, $\widehat{A}$ is a DVR where the valuation of a Cauchy sequence $a = \sum_{i=n}^{\infty} a_n t^n + a_{n+1} t^{n+1} \cdots$ is $v(a) = n$, the vanishing order of the series at zero, or the lowest power of $\widehat{\mathfrak{m}}$ such that $a \in \widehat{\mathfrak{m}}^n = (t^n)$. We also observe that

$$A/\mathfrak{m}^n = A/(t^n) = \widehat{A}/(t^n) = \widehat{A}/\widehat{\mathfrak{m}}^n \, .$$

Let us comment on the two main examples of completions of DVRs.

Example 56. *Let $k[X]_{(X)}$ be the localization of the affine line $\operatorname{Spec} k[X]$ at $X = 0$. This is a DVR whose maximal ideal is $\mathfrak{m} = (X) \cdot k[X]_{(X)}$ (see Example 48). Its completion is the **ring of formal power series** denoted by $k[[X]] := \widehat{k[X]_{(X)}}$ whose elements are*

$$f(x) = \sum_{i=0}^{\infty} a_i X^i = a_0 + a_1 X + a_2 X^2 + \cdots + a_n X^n + \cdots$$

where $a_i \in k$.

Example 57. *Let $\mathbb{Z}_{(p)}$ be the localization of the arithmetic line $\operatorname{Spec} \mathbb{Z}$ at the prime (p), which is a DVR whose maximal ideal is $\mathfrak{m} = (p) \cdot \mathbb{Z}_{(p)}$ (see Example 47). Its completion is the **ring of p-adic integers** denoted by $\mathbb{Z}_p := \widehat{\mathbb{Z}_{(p)}}$ whose elements are*

$$n = \sum_{i=0}^{\infty} \frac{a_i}{b_i} p^i = \frac{a_0}{b_0} + \frac{a_1}{b_1} p + \frac{a_2}{b_2} p^2 + \cdots + \frac{a_n}{b_n} p^n + \cdots$$

where $\frac{a_i}{b_i} \in \mathbb{Z}_{(p)}$, i.e. p does not divide b_i. The valuation of a series of the completion is the lowest order of the expansion in powers of p.

References

[AM] M.F. Atiyah and I.G. Macdonald. *Introduction to commutative algebra*, Addison-Wesley Publishing Co. (1969).

[Ar] E. Arrondo. *A geometric introduction to commutative algebra*, version of September 18th 2023. URL: https://docta.ucm.es/rest/api/core/bitstreams/05eec649-59b2-4c6f-8932-d418360b94d8/content.

[FG] J.F. Fernando and J.M. Gamboa. *Estructuras Algebraicas: Divisibilidad en Anillos Conmutativos*, Segunda Edición, Sanz y Torres (2017).

[Re] M. Reid. *Undergraduate Commutative Algebra*, Cambridge University Press (1995).